Computer Science & Information Technology 98

Dhinaharan Nagamalai
Jan Zizka (Eds)

Computer Science & Information Technology

5th International Conference on Computer Science, Engineering and Information Technology (CSEIT-2018), December 22-23, 2018, Dubai, UAE

AIRCC Publishing Corporation

Volume Editors

Dhinaharan Nagamalai,
Wireilla Net Solutions, Australia
E-mail: dhinthia@yahoo.com

Jan Zizka,
Mendel University in Brno, Czech Republic
E-mail: zizka.jan@gmail.com

ISSN: 2231 - 5403
ISBN: 978-1-921987-96-0
DOI : 10.5121/csit.2018.81801 - 10.5121/csit.2018.81815

Typesetting: Camera-ready by author, data conversion by NnN Net Solutions Private Ltd., Chennai, India

Preface

The 5th International Conference on Computer Science, Engineering and Information Technology (CSEIT-2018), was held in Dubai, UAE during December 22-23, 2018. The 10th International Conference on Network and Communications Security (NCS-2018), The 5th International Conference on Signal, Image Processing and Multimedia (SPM-2018) and The 10th International Conference on Networks & Communications (NeTCoM - 2018) was collocated with The 5th International Conference on Computer Science, Engineering and Information Technology (CSEIT-2018). The conferences attracted many local and international delegates, presenting a balanced mixture of intellect from the East and from the West.

The goal of this conference series is to bring together researchers and practitioners from academia and industry to focus on understanding computer science and information technology and to establish new collaborations in these areas. Authors are invited to contribute to the conference by submitting articles that illustrate research results, projects, survey work and industrial experiences describing significant advances in all areas of computer science and information technology.

The CSEIT-2018, NCS-2018, SPM-2018, NeTCoM-2018 Committees rigorously invited submissions for many months from researchers, scientists, engineers, students and practitioners related to the relevant themes and tracks of the workshop. This effort guaranteed submissions from an unparalleled number of internationally recognized top-level researchers. All the submissions underwent a strenuous peer review process which comprised expert reviewers. These reviewers were selected from a talented pool of Technical Committee members and external reviewers on the basis of their expertise. The papers were then reviewed based on their contributions, technical content, originality and clarity. The entire process, which includes the submission, review and acceptance processes, was done electronically. All these efforts undertaken by the Organizing and Technical Committees led to an exciting, rich and a high quality technical conference program, which featured high-impact presentations for all attendees to enjoy, appreciate and expand their expertise in the latest developments in computer network and communications research.

In closing, CSEIT-2018, NCS-2018, SPM-2018, NeTCoM-2018 brought together researchers, scientists, engineers, students and practitioners to exchange and share their experiences, new ideas and research results in all aspects of the main workshop themes and tracks, and to discuss the practical challenges encountered and the solutions adopted. The book is organized as a collection of papers from the CSEIT-2018, NCS-2018, SPM-2018, NeTCoM-2018.

We would like to thank the General and Program Chairs, organization staff, the members of the Technical Program Committees and external reviewers for their excellent and tireless work. We sincerely wish that all attendees benefited scientifically from the conference and wish them every success in their research. It is the humble wish of the conference organizers that the professional dialogue among the researchers, scientists, engineers, students and educators continues beyond the event and that the friendships and collaborations forged will linger and prosper for many years to come.

Dhinaharan Nagamalai
Jan Zizka

Organization

General Chair

Natarajan Meghanathan	Jackson State University, USA
David C. Wyld	Southeastern Louisisna University, USA

Program Committee Members

Abar Shah	Zayed University, UAE
Abdalah Rababah	Jordan University of Science and Technology, Jordan
Abdulhamit Subasi	Effat University, Saudi Arabia
Adnan Mahmood	Macquarie University, Australia
Ahmad A. Saifan	Yarmouk university, Jordan
Ahmed H. Salem	Old Dominion University, USA
Ahmed J. Jameel	Ahlia University, Bahrain
Ahmad Khasawneh	Hashemite University, Jordan
Aihua Mao	South China University of Technology, China
Ajao Lukman Adewale	Federal University of Technology, Nigeria
Ali Abdrhman Mohammed Ukasha	Sebha University, Libya
Amer Sallam	University of Taiz (UoT), Yemen
Amine Laghrib	Faculté des Sciences Beni-Mellal, Marocco
Amir Rastegarnia	University of Malayer, Iran
Amizah Malip	University of Malaya, Malaysia
Andysah Putera Utama Siahaan	Universitas Pembangunan Panca Budi, Indonesia
Annamalai	Prairie View A&M University, USA
Asmaa Shaker Ashoor	Babylon University, Iraq
Barhoumi Walid	SIIVA-LIMTIC Laboratory, Tunisia
Bhuvan Modi	Senior Member of Technical Staff, AT&T, USA
Bouchra Marzak	Hassan II University, Morocco
Bouhorma Mohammed	Faculty of science and technology of Tangier, Morocco
Boukenadil Bahidja	University of Tlemcen, Algeria
Carlo Sau	University degli Studi di Cagliari, Italy
Chaker LARABI	University de Poitiers, France
Christophe Claramunt	Naval Academy Research Institute, France
Chuanzong Zhang	Aalborg University, Denmark
Cristina-Loredana Duta	University Politehnica of Bucharest, Romania
Dac-Nhuong Le	Haiphong University, Vietnam
Diego Reforgiato Recupero	University of Cagliari, Italy
Fabio Gasparetti	Roma Tre University, Italy
Fabio Silva	Federal University of Pernambuco, Brazil
Grigorios N. Beligiannis	University of Patras, Greece
Hala Abukhalaf	Palestine Polytechnic University, Palestine
Hamid Ali Abed AL-Asadi	Basra University, Iraq
Hanming Fang	Logistical Engineering University, China
Hassan Ugail	University of Bradford, UK

Technically Sponsored by

Computer Science & Information Technology Community (CSITC)

Networks & Communications Community (NCC)

Soft Computing Community (SCC)

Organized By

Academy & Industry Research Collaboration Center (AIRCC)

TABLE OF CONTENTS

5th International Conference on Computer Science, Engineering and Information Technology (CSEIT-2018)

10th International Conference on Network and Communications Security (NCS-2018)

5th International Conference on Signal, Image Processing and Multimedia (SPM-2018)

10th International Conference on Networks & Communications (NeTCoM - 2018)

ANDROID UNTRUSTED DETECTION WITH PERMISSION BASED SCORING ANALYSIS

JACKELOU SULAPAS MAPA

College of Information Technology
Saint Joseph Institute of Technology, Montilla
Boulevard, Butuan City, Philippines

ABSTRACT

Android smart phone is one of the fast growing mobile phones and because of these it the one of the most preferred target of malware developer. Malware apps can penetrate the device and gain privileges in which it can perform malicious activities such reading user contact, misusing of private information such as sending SMS and can harm user by exploiting the users private data which is stored in the device. The study is about detecting untrusted on android applications, which would be the basis of all future development regarding malware detection. The smartphone users worldwide are not aware of the permissions as the basis of all malicious activities that could possibly operate in an android system and may steal personal and private information. Android operating system is an open system in which users are allowed to install application from any unsafe sites. However permission mechanism of and android system is not enough to guarantee the invulnerability of the application that can harm the user. In this paper, the permission scoring-based analysis that will scrutinized the installed permission and allows user to increase the efficiency of Android permission to inform user about the risk of the installed Android application, in this paper, the framework that would classify the level of sensitivity of the permission access by the application. The framework uses a formula that will calculate the sensitivity level of the permission and determine if the installed application is untrusted or not. Our result show that, in a collection of 26 untrusted application, the framework is able to correct and determine the application's behavior consistently and efficiently.

KEYWORDS

Permission, permission scoring-based, malware Android phone, Security, Internet, malware.

1. INTRODUCTION

Nowadays, the advancement of technology is rapid. The new product is being introduced to the market and in a week, month later a new one surfaces with a better functionality against its predecessor. Mobile phones are not exempted in the advancement of technology. From call and text only functionality, mobile phones became smartphones (Android) that serves as pocket computers. It is informing the entire user about the risk while using the application. In order to install the application from device you need the permissions that the application request. Some of

Dhinaharan Nagamalai et al. (Eds) : CSEIT, NCS, SPM, NeTCoM - 2018
pp. 01–14, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81801

the users are not paying attention or do not fully comprehend the requested permission. In addition, these permissions permit the malware to penetrate or exploit private data stored on device and perform malicious activities such as reading users private information, track user location, log-in credentials, and web browser history. Example of this permission is the INTERNET; many of the application communicate over the internet and malware developer advantage the use of this permission and combine with other permission [19].

In 2010, some of the Android developer Hans they just simply use it just to make sure that their application works properly. Therefore, a combination and unprofessional use of permission can take the advantage of stealing users' private data [10]. The existing security permission model of android has flaws that cannot protect the users' private data effectively. Several researchers, questioned the Android security model, and stated that the current permission model [11].

In (2015). The problems encountered by smartphone users in manipulating and maintaining the android malware security are the Absence of efficient Malware detector in Android Phones and Due to increasing numbers of Android Malware applications, a fast and reliable malware detector is necessary [13]. This proposal will conduct a study to detect the behavior of the malicious apps that can manipulate information on android devices. As a solution we present a permission-based scoring detection, which will evaluate the permission of the application and identify the application if its malicious or not The researcher achieve the process of detecting the malicious applications and develop an android application that can detect Malware applications in Android Phone, extract permissions of all installed android applications and evaluate the permissions that are extracted and determine malware application by the use of malware score formula.

2. REVIEW OF RELATED LITERATURE

A. PERMISSION ANALYSIS FOR ANDROID MALWARE (2015)

Detection. If the smart phones are infected with malware, users may face the following risks: the disclosure of personal information, sent messages and read communications without permission, exploited the data with malicious intent. So the researchers PAMP, Permission Analysis for Android Malware Detection, which analyzes the Manifest file by understanding the Android Permission and by investigating malicious characteristics [1].

B. PERMISSION-BASED MALWARE DETECTION SYSTEM (2014)

PMDS System A cloud requested permissions as the main feature for detecting suspicious activities. PMDS applies a machine learning approach to categorize and determine automatically the harmful previously unseen application based on combination of permission required. In their study, they offer some discussion identifying the degree of android malware that can be detect and the prevention of malware by focusing on the permission they request. To understand the focus of the study, the set of permissions asked by the application corresponds to the behavior as either begin or malicious [4].

C. DREBIN:EFFECTIVE AND EXPLAINABLE DETECTION OF ANDROID MALWARE IN (2014).

“Malicious applications pose a threat to the security of Android malware.” Researchers proposed DREBIN, method for detecting malware that enables identifying malicious application in Android by gathering as many features of an application as possible

D. THE POSSIBILITIES OF DETECTING MALICIOUS APPLICATIONS IN ANDROIDS PERMISSION (2013)

Study attempts to explore Collected relative large number of benign, malicious applications and conducted experiments and collected information based on the sample [3].

E.PUMA: PERMISSION USAGE TO DETECT MALWARE IN ANDROID (2013)

The presence of mobile devices has increased in our lives offering almost the same functionality as a personal computer. Android devices have appeared lately and, since then, the number of applications available for this operating system has increased exponentially. Google already has its Android Market where applications are offered and, as happens with every popular media, is prone to misuse. In fact, malware writers insert malicious applications into this market, but also among other alternative markets.” Researchers presented PUMA (Permission Usage to Detect Malware in Android), method for detecting malicious Android applications by analyzing the extracted permissions from the application itself.

F. CREATING USER AWARENESS OF APPLICATION PERMISSIONS IN MOBILE SYSTEMS.

Classifies the applications based on a set of custom rules if a rule is applied by the application it will mark as suspicious. Permission Watcher provides a home screen widget that aware users for potentially harmful applications. The methodology in this context relies on the comparison of the Android security permission of each application with a set of reference models for an application that manages sensitive data. The present researchers apply the idea of permission-based analysis to analyze the applications in order to know if the android app is malicious or benign.

G. PERMISSION WATCHER (2012)

The set of custom rules provides a home screen widget those aware users for potentially harmful application; the present researcher applies the idea of permission-based to track the behavior of the applications to know if the android app is malicious or benign [5]. Permission Flow tool that can easily identified. The system classified the application as benign.

H. DROIDMAT: ANDROID MALWARE DETECTION THROUGH MANIFEST AND API CALLS TRACING (2012)

The threat of Android malware is spreading rapidly, especially those repackaged Android malwares.” Presented Droid Mat, a static feature-based mechanism to provide a static analyst paradigm for detecting the Android malware by extracting the information (Intents, permissions, etc.) from the application's manifest and regards components (Activity, Receiver, Service) as points drilling down for tracing API Calls related to permissions.

3. METHODOLOGY AND DESIGN

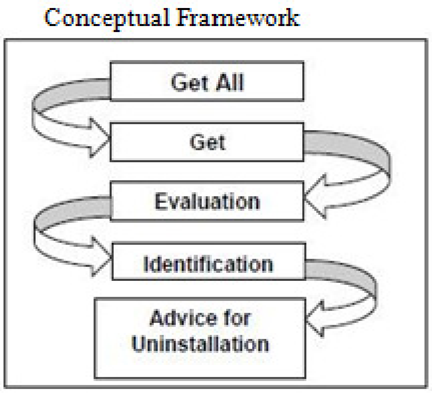


Fig. 1 Malcure Conceptual Design

This section will present the overview of the Malcure framework and the description of each phase. System frameworks illustrate the flow of each phase in working out to analyze the application during the scanning.

3.1 MALCURE

Will scan for the apps that may contain malwares that could leak sensitive information. Just after the scan button was tapped, each of the apps will processed, so that each of the app's permissions will be directly extracted, and therefore will undergo permission based scoring. The permission scoring analysis will be performed to check if the permission score has exceeded the malicious standard score or not. If yes, the application will be advised for uninstallation.

3.2 GET ALL APPLICATIONS

The process where all the applications will be process to be prepared for extraction of the permissions.

3.3 GET PERMISSIONS

The app's permissions are directly extract from the application, and there is no need for DE compilation of the base file.

3.4 EVALUATION

This is where all the permissions are evaluated based on the scores set on the sensitivity of a permission ranging from 1 to 6, making 1 as the Neutral permission, and 2 to 6 are the sensitive permissions, and all are processed base on a formula.

3.5 IDENTIFICATION

The overall malicious score is determined in this phase, and therefore will be advice for un installation if the score exceeds the malicious standard score.

3.6 ADVICE FOR UNINSTALLATION

When a particular application is judge as malicious, Malcure will open a window, where the app is advised for uninstallation

3.7 APP SCANNING FRAMEWORK

The process of Malcure scanning mechanism, at the start of this function, there will be scanning performed in a loop of user-defined and system applications that directly extracts each of the application permissions to be evaluated and process with the Permission Score Analysis and the Formula to determine the Malicious Score of a particular application. Once an application has exceeded that malicious standard score, its advice for uninstallation

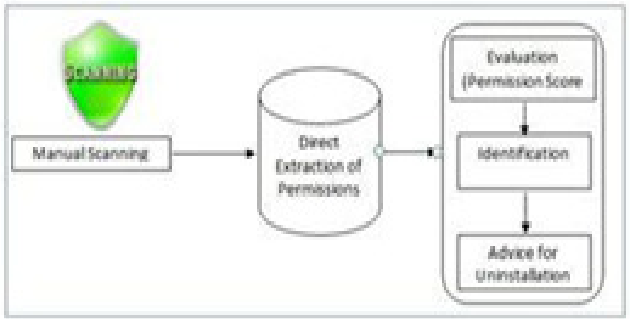
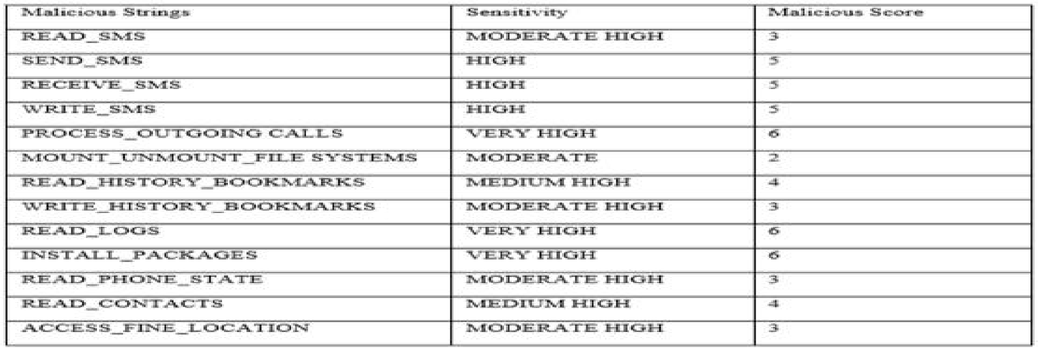

SCANNING
Manual Scanning
Direct Extraction of Permissions
Evaluation (Permission Score
Identification
Advice for Uninstallation

Fig.2 Malcure App Scanning Framework

In this section, we will briefly discuss the permissions and their sensitivity and malicious scores that will determine the capability of an app in stealing sensitive information. In addition, the table that represents the sensitive permissions and their malicious scores of a particular application. Once an application has exceeded that malicious standard score, it is then advised for uninstallation.

3.8 PERMISSIONS SENSITIVITY AND THEIR MALICIOUS SCORE



Malicious Strings	Sensitivity	Malicious Score
READ_SMS	MODERATE HIGH	3
SEND_SMS	HIGH	5
RECEIVE_SMS	HIGH	5
WRITE_SMS	HIGH	5
PROCESS_OUTGOING CALLS	VERY HIGH	6
MOUNT_UNMOUNT_FILE SYSTEMS	MODERATE	2
READ_HISTORY_BOOKMARKS	MEDIUM HIGH	4
WRITE_HISTORY_BOOKMARKS	MODERATE HIGH	3
READ_LOGS	VERY HIGH	6
INSTALL_PACKAGES	VERY HIGH	6
READ_PHONE_STATE	MODERATE HIGH	3
READ_CONTACTS	MEDIUM HIGH	4
ACCESS_FINE_LOCATION	MODERATE HIGH	3

Table 1 Permission Sensitivity and their Malicious Score

The figure shows the formula where R, is the Overall Malicious Score. M, which is the total scores of the sensitive permissions. C is the number of Neutral or Benign Permissions

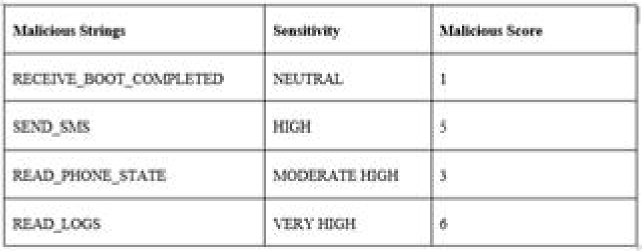
3.9 UNTRUSTED SCORING FORMULA

$$R = \frac{M}{M+C}$$

Figure 3. Untrusted Scoring Formula

The figure shows the formula where R, is the Overall Malicious Score. M, which is the total scores of the sensitive permissions. C is the number of Neutral or Benign Permissions.

3.10 UNTRUSTED SCORE EVALUATION



Malicious Strings	Sensitivity	Malicious Score
RECEIVE_BOOT_COMPLETED	NEUTRAL	1
SEND_SMS	HIGH	5
READ_PHONE_STATE	MODERATE HIGH	3
READ_LOGS	VERY HIGH	6

Table2. Sample Application with Permissions

$$R \quad \frac{14}{14+1}$$

$$= 0.93333 \text{ Overall}$$

Figure 4. Sample Result

Shows a sample application with the following permissions. Now, using the formula we will get: Figure 4. Sample Result

Figure shows the result from Table 2, which is considered to be an untrusted because of the fact that it exceeded the untrusted standard score which 0.70.

3.1.1 UNTRUSTED STANDARD SCORE

Come up with 0.70 untrusted app standard score, based on multiple mock up tests and analyzations on multiple untrusted applications, and discovered that even on applications that has only two permissions. The other is neutral and the other permission is sensitive with 2 points, it will be considered an untrusted, which is an appropriate action for anti-malware application. Any application with overall untrusted score equal or more than to 0.70 will be considered an untrusted.

The Untrusted Standard Score Basis

DeviceModelwith Built in Apps only	**Highest Score**	**Package Name**
Cherry Mobile Flare	0.69	Com.cherryplay
Acer Liquid z160	0.66	Com.backuptester
Samsung Duos	0.69	Com.hangouts
Myphone Rio	0.67	Com.facebook.orca
Sony Erikkson Curve	0.68	Com.backuptester

Total = 3.39 / 5 Average = 0.68 rounded up to 0.70

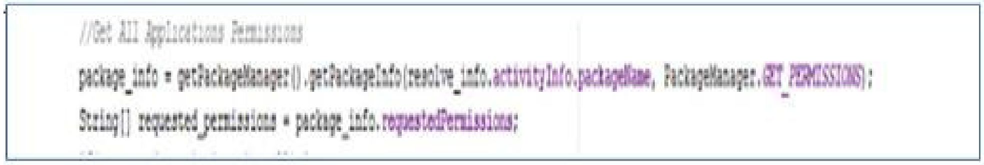
Table3. Untrusted Standard Score Basis

Table shows the basis of the untrusted detector Standard Score is by sampling some smartphones with different brands, stored with only built only applications and we've calculated the highest scores of each smartphones and get there average. Because of the fact that smartphone manufacturers do not develop built in applications with malwares, every time a user application exceeds that score, it also exceeds the basis of the manufacturer in developing clean applications. Failure to do so will result to disclosure of the license to produce Smartphones with Android OS. This standard is our basis that every time an application exceeds that standard, our study and developed system will consider it a Malware.

4. RESULTS AND DISCUSS ION

4.1 PERMISSION EXTRACTIO N

Our way of extracting the permissions of every application was successful because of the fact that Android has a predefined class of directly extracting every permission without de compiling the APK base file.



```
//Get All Applications Permissions
package_info = getPackageManager().getPackageInfo(resolve_info.activityInfo.packageName, PackageManager.GET_PERMISSIONS);
String[] requested_permissions = package_info.requestedPermissions;
```

Figure 5. Permission Extraction

The above line of codes represents the extraction of all the permissions that comes from the application, whether it is from the system or the user.

4.2 UNTRUSTED DETECTION

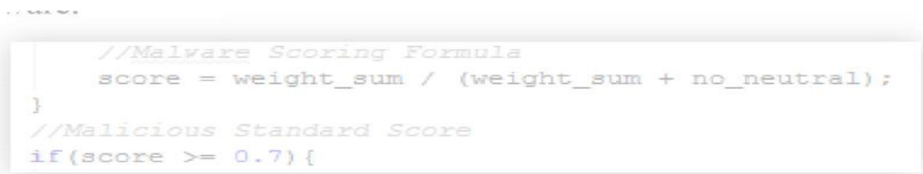
This is the process which shows on how a Malware is detected, through Evaluating the permissions extracted based on the thirteen sensitive permissions, then using the malicious scoring formula, which then states if the application is advisable for uninstallation or not.

4.3 PERMISSION VALIDATION

By comparing all of the permissions of a particular application to the sensitive per mission stated in Table 2, we were able to come up with the malicious score that are necessary for coming up with the overall malicious score. Once a permission matches with the sensitive permissions. The score matching the sensitivity of the permission is incremented, and all remaining permissions which did not match, will be considered as neutral permissions.

4.4 MALWARE SCORING FORMULA/UNTRUSTED DETECTION

Come up with untrusted scoring formula that was based on a study that we slightly modified, due to reasons that the researcher want untrusted to be fast and efficient, because on its original study, it included process and third party resource s that causes the overall process to be slow, and comprise large memory. The malware standard score on the other hand was the result of multiple mock up tests and analyzations on multiple malware applications, and discovered that even on applications that has only 2 permissions. The other is neutral and the other permission is sensitive with 2 points, it will be considered a malware, which is an appropriate action for anti-malware application. Any application with overall malware score equal or more than to 0.70 will be considered a malware.



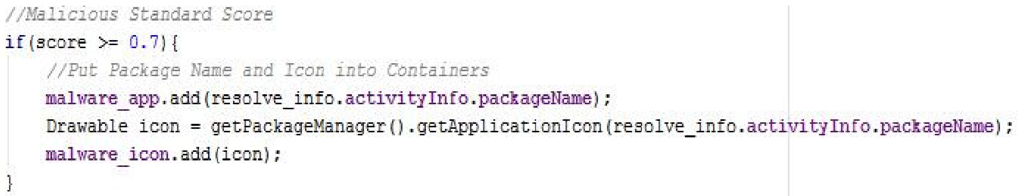
```
    //Malware Scoring Formula
    score = weight_sum / (weight_sum + no_neutral);
}
//Malicious Standard Score
if(score >= 0.7){
```

Figure 6. Untrusted Scoring Formula/Untrusted Detection

Shows the Untrusted Scoring Formula and Untrusted Standard Score.

4.5 UNINSTALL RECOMMENDATION

After the processing of all the scores of the matched sensitive permissions, a fin al and overall malicious score is generated using the formula, then a condition is formulated that when the overall malware score is equal or more than the malware standard score, that particular application will be advised for u uninstallation with the consent of the user.



```
//Malicious Standard Score
if(score >= 0.7){
    //Put Package Name and Icon into Containers
    malware_app.add(resolve_info.activityInfo.packageName);
    Drawable icon = getPackageManager().getApplicationIcon(resolve_info.activityInfo.packageName);
    malware_icon.add(icon);
}
```

Figure 7. Uninstall Recommendation

4.6 GRAPHICAL USER INTERFACE

This represents the interaction between the user and Untrusted and how the user can manipulate untrusted, from scanning to determining if the application is a malware or not, with its following process:

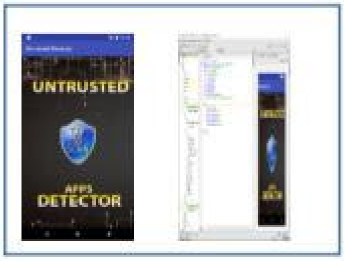
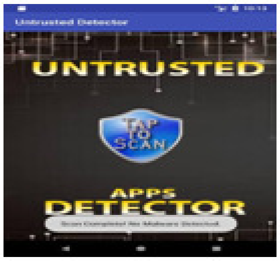


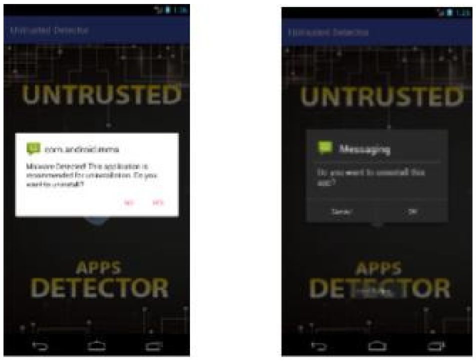
Figure 8. Tap to Scan

Whenever the user taps the shield icon, Untrusted immediately starts its scanning from the applications from the user and the system, and therefore starts the process from validation, evaluation, identification and ad vice for uninstallation.



Scan Completed! No Malware Detected

Figure 9. No Malware Detected



com.android.mms

Malware Detected! This application is recommended for uninstallation. Do you want to uninstall?

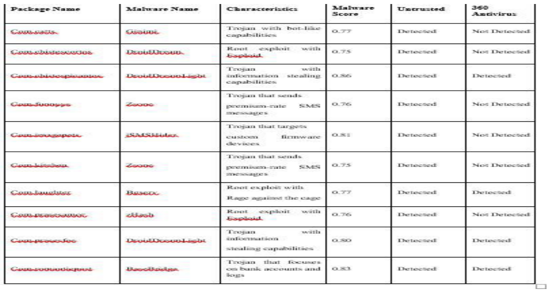
Messaging

Do you want to uninstall this app?

Figure 10. Untrusted Detected

Shows when the malware score is equal or more than the malware standard score, and therefore detects a malware, a dialog box appears advising the user to uninstall the particular application, and then after that another dialog box appears clarifying the user's decision. The researcher do this, because we observe the full right of the user to keep the application if the user wanted to. But when the user accepts, the application is uninstalled immediately. There are multiple applications detected as malware, the event that will happen is that after the first app has been take cared for, a next dialog box pertaining to the next malware detected will appear.

4.7 UNTRUSTED VS. 360 ANTIVIRUS SECURITY FIRST VERSION



Package Name	Malware Name	Characteristics	Malware Score	Untrusted	360 Antivirus
Com.cats	Gemini	Trojan with bot-like capabilities	0.77	Detected	Not Detected
Com.chistescortos	DroidDream	Root exploit with Exploid	0.75	Detected	Not Detected
Com.chistespicantes	DroidDreamLight	Trojan with information stealing capabilities	0.86	Detected	Detected
Com.fun999s	Zsone	Trojan that sends premium-rate SMS messages	0.76	Detected	Not Detected
Com.imagepets	jSMSHider	Trojan that targets custom firmware devices	0.81	Detected	Not Detected
Com.kitchen	Zsone	Trojan that sends premium-rate SMS messages	0.75	Detected	Not Detected
Com.laughter	Basebr	Root exploit with Rage against the cage	0.77	Detected	Detected
Com.prasesamor	zHash	Root exploit with Exploid	0.76	Detected	Not Detected
Com.prasesfoo	DroidDreamLight	Trojan with information stealing capabilities	0.80	Detected	Detected
Com.romanticpost	BaseBridge	Trojan that focuses on bank accounts and logs	0.83	Detected	Detected

Table 3. Untrusted vs. Other Permission Based Malware Detector

Shows that the researcher have taken 10 updated sample malwares that are likely used to attack smartphone devices and steal personal information. Out of 10 sample malware tested, 360 antivirus just detected 4, while Untrusted perfectly detected all of them. So, therefore the researcher conclude that Untrusted is more reliable than the first version of the 360 security, and with more improvement and development, it will be a remarkable malware detector for Android Operating system, with the main feature of fast, memory friendly and reliability.

SURVEYS

Disguised 10 malicious software and invited 10 individuals to try Untrusted and compare it with the first version of 360 Antivirus, with the disguised software installed, and ask their opinions and statements about the differences between the malware detector, and which is faster and more reliable for them in detecting malwares.

SURVEY RESULT

Based on the data collected from 10 participants, comprised of average users, techy geeks and researcher, come up with this graphical representation that helps us conclude on the performance, reliability, memory friendliness and usage preferability of Untrusted.

CHART PRESENTATION

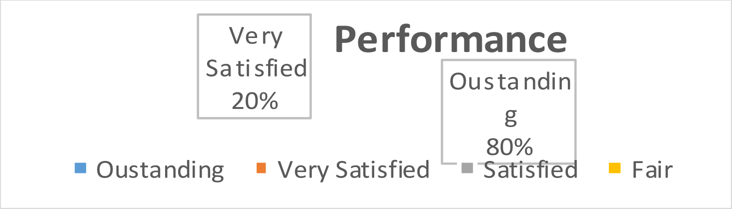


Figure 11. Performance Survey Result

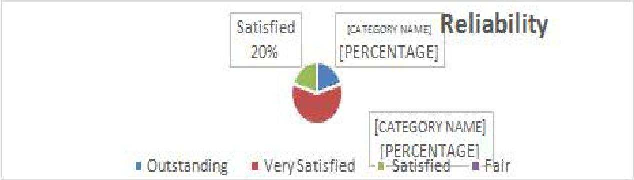


Figure 12. Reliability survey Result

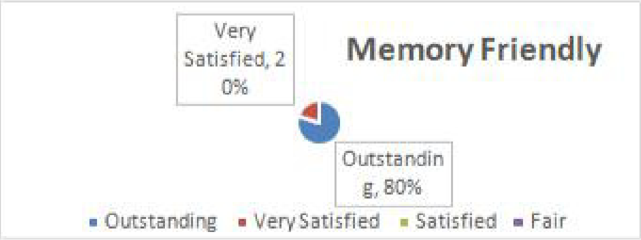


Figure 13. Memory Friendliness Survey Result

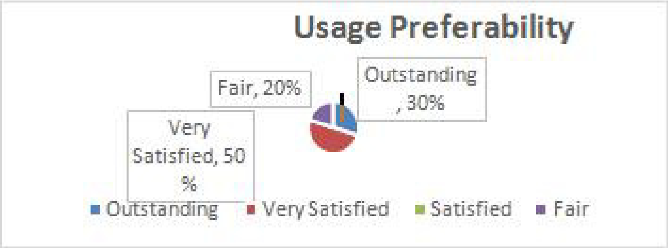


Figure 14. Usage Preferability

SURVEY CONCLUSION

Based on the survey that conducted on 10 Smartphone users, we're able to collect data that helps us prove that Untrusted is fast, reliable, memory friendly and users are going to use it. With 95% on approval on Performance, 75% percent on Reliability, 95% on Memory Friendliness and 80% percent on Usage Preferability, our study and all of its methodology are proven base on the user's experience on the developed system.

5. SUMMARY AND CONCLUSION

SUMMARY

Android Untrusted is considered as one of the problem that many android users encountered. The proposed untrusted detection for android phones that will identify the malicious application that is installed on the device. Based on the experiment that the researcher conducted it shows that untrusted is effective in detecting malicious application. Untrusted detection was effective and efficient in extracting the permission without decompiling the apk. To get the following permission use getPackageManer().getPackageInfo() to extract the permission. The researcher observed that by using the package manager it's achieve the process of extracting the permission much faster. It's also see that permission-scoring formula is effective for evaluating the level of permissions in order to decide if the application is malicious or benign.

Based on the experiment and survey that the researcher conducted it shows that untrusted is effective in capturing the malware application. It shows that the untrusted application that installed on the android device was captured by the untrusted detection.

6. CONCLUSION

The UN system is effective in providing a solution by detecting the malicious application that can penetrate the android device. The researcher presented a methodology and architecture for measuring the permission accessed by the application using permission-scoring formula, which will identify if the application was manifested with malicious permission. Using the permission scoring detection, and it's satisfies the Untrusted Detection objectives to capture the malware application. Using this anti-malware application, android user will be aware of the applications and its true behaviors.

REFERENCES

[1] NguyenVietD.etal (2015)"Permission Analysis for Android Malware Detection". Retrieved from https://www.researchgate.net/profile/Pham_Giang4/publication/296704790_Permission_Analysis_for_AndroidMalware_Detection/links/ 56d9bce708aee1aa5f8291f4.pdf

[2] Isohara, T., Takemori, et. al. (2011)."Kernel-based Behavior Analysis for Android Malware Detection". Retrieved from http://ieeexplore.ieee.org/abstract/document/6128277

[3] Huang, C. Ts ai, et. al. (2013). "Performance Evaluation on Permission- Based Detection for Android Malware". Retrieved fromhttps://www.link.springer.comchapter10.1007/978-3-642-35473-112

[4] Rovelli, P., & Vigfússon, Ý . (2014).PMDS:"Permission-Based Malware Detection System". Retrieved from https://www.link.springer.com/chapter10.1007/978-3-319-13841-1_19

[5] Struse, E., Seifert, J., Üllenbeck, S.,Rukzio, E., & Wolf, (2012). "Permission Watcher: "Creating User Awareness of Application Permissions in Mobile Systems". Retrieved from https://www.link.springer.com/chapter10.1007/978-3-642-34898-3_5

[6] Sbirlea, D. Burke, ET. Al (2013). "Automatic Detection of Inter-Application Permission Leaks in Android applications". Retrieved from http://www.ieeexplore.ieee.org/abstract/document/6665098/

[7] Wu,D.et.al.,(2012). "DroidMat: API Calls Tracing". Retrieved from http://www.ieeexplore.ieee.org/abstract/document6298136

[8] Sanz, B., Santos, et. al. (2013). "PUMA: Permission Usage to Detect Malware in Android". Retrieved from https://link.springer.com/chapter/10.1007/978-3-642-33018-6_30

[9] Arp, D., et. al. (2014). Drebin: "Effective and Explainable Detection of Android Malware in Your Pocket" Retrieved from https://www.researchgate.netprofile/264785935_DREBIN_Effective_and_Explainable_Detection_of_Android_Malware_in_Your_Pocket /links/53efd0020cf 26b9b7dcdf395.pdf

[10] Barrera, D., Kayacik, et. al., (2010). “Methodology for empirical analysis of permission-based security models and its application to android categories and subject description. In processing of 17th ACm conference on computer and communication security New York” NY, USA ACM 2010. P 73-74 http://dx.doi.org/10.1145/1866307.18663317

[11] Enck W.Gilbert, et.al., (2014).“TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smart phones”, Retrieved from http://www.dl.acm.org/citation.cfmid2619091

[12] K.Mathur et.al., “A Survey on Techniques in Detection and Analyzing Malware Executables, Int. Journal of Advanced Research in Computer Science and Software Engg.”, India, vol. 3, issue 4, pp. 422- 428, 2013.

[13] R.Sato, et.al. “Detecting Android Malware by Analyzing Manifest Files”, pp. 2331, 2013.Android Permissions Demystified. [Online] Available: https://www.truststc.org/pubs/848.html. [Accessed: 06-Nov-2015].

[14] P.Faruki, V.Ganmoor, V. Laxmi, M. S. Gaur, and A. Bharmal, Andro Similar: “Robust Statistical Feature Signature for Android Malware Detection, Proc. 6th Int. Conf. Secur. Inf. Networks”, pp. 152 159, 2013

[15] Mengyu Qiao, et. al., ”Merging Permission and API Features for Android Malware Detection”, vol. 00, no., pp. 566-571, 2016, doi:10.1109/IIAI-AAI.2016.237

[16] K.Xu, Y. Li, and R. Deng, ICC Detector: “ICC-Based Malware Detection 4 on Android, in Proc. of IEEE Transaction in Information Forensics and security”, vol. 11, no. 6, June 06, 2016

[17] R. Raveendranath, V. Rajamani, A. J. Babu, and S. K. Datta, “Android malware attacks and countermeasures: Current and future directions, 2014 Int. Conf. Control. Instrumentation Commune. Compute”. Technol., pp. 137143, 2014

[18] R. Johnson, C. Gagnon, Z. Wang, and A. Stavrou, “Analysis of Android Appss Permissions, in Proc. of 6th IEEE Int. Conference of Software Security and Reliability Companion, Maryland”, pp. 45-46, 2012

[19] “Android applications ... and more (ninja!) - Google Project Hosting”[Online].Available: https://code.google.com/p/androguard/. [Accessed: 01- Dec 2015].

[20] L.Wenjia, D. Guqian, ““An SVM Based approach”, in Proc. of IEEE 2nd Int. Conference on Cyber Security and Cloud Computing”, 2015.

[21] Android developer guide permission 9 (WWW document).Google. URL, http;//developer.android.com/guide/topics/manifest/permission-element.html#package; 2014[accessed 2512.14]

[22] Wu D J, Mao C H, Wei T E, et al. Droidmat: Android malware detection through manifest and API calls tracing. In: Proceedings of the 7th Asia Joint Conference on Information Security (Asia JCIS). Piscataway: IEEE Press, 2012. 62–69

[23] Zhou Y J, Wang Z, Zhou W, et al. Hey, you, get off of my market: detecting malicious apps in official and alternative android markets. In: Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, 2012. 25: 50–52

[24] Bläsing T, Batyuk L, Schmidt A D, et al. An android application sandbox system for suspicious software detection. In: Proceedings of the 5th International Conference on Malicious and Unwanted Software (MALWARE). Piscataway: IEEE Press, 2010. 55–62

[25] Stevens R, Ganz J, Filkov V, et al. Asking for (and about) permissions used by android apps. In: Proceedings of the 10th Working Conference on Mining Software Repositories. Piscataway: IEEE Press, 2013. 31–40

[26] Karim M Y, Kagdi H, Di Penta M. Mining android apps to recommend permissions. In: Proceedings of the 23th IEEE/ACM International Conference on Software Analysis, Evolution, and Reengineering. Piscataway: IEEE Press, 2016. 427–437

[27] M. Grace, Y. Zhou, Z. Wang, and X. Jiang. Systematic detection of capability leaks in stock Android smart phones. In Proceedings of the 19th Network and Distributed System Security Symposium (NDSS), Feb. 2012.

[28] Kim, J. I. Cho, H. W. Myeong, and D. H. Lee. A study on static analysis model of mobile application for privacy protection. In J. J. (Jong Hyuk) Park, H.-C. Chao, M. S. Obaidat, and J. Kim, editors, Computer Science and Convergence, volume 114 of Lecture Notes in Electrical Engineering, pages 529-540. Springer Netherlands, 2012. 10.1007/978-94-007-2792-2 50.

[29] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner. Android permissions demystified. In Proceedings of the 18th ACM conference on Computer and communications security, CCS '11, pages 627-638, New York, NY, USA, 2011. ACM.

[30] Sina science and technology, http://tech.sina.com.cn/it/20130510/07478325514.shtml[EB/OL].May 2013.

[31] DoNews.http://www.donews.com/net/201305/1495781. shtm[EB/OL]. May 2013.

AUTHOR

Engr. Jackelou S. Mapa, MIT
Information Technology Education Program Head
Saint Joseph Institute of Technology,
Montilla Boulevard, 8600 Butuan City, Philippines

AN ONTOLOGY-BASED HIERARCHICAL BAYESIAN NETWORK CLASSIFICATION MODEL TO PREDICT THE EFFECT OF DNA REPAIRS GENES IN HUMAN AGEING PROCESS

Hasanein Alharbi

Department of Computer Engineering Techniques,
Al-Mustaqbal University College, Babylon, Iraq

ABSTRACT

Conventional Data Mining (DM) algorithms treated data simply as numbers ignoring the semantic relationships among them. Consequently, recent researches claimed that ontology is the best option to represent the domain knowledge for data mining use because of its structural format. Additionally, it is reported that ontology can facilitate different steps in the Bayesian Network (BN) construction task. To this end, this paper investigates the advantages of consolidating the Gene Ontology (GO) and the Hierarchical Bayesian Network (HBN) classifier in a flexible framework, which preserves the advantages of both, ontology and Bayesian theory. The proposed Semantically Aware Hierarchical Bayesian Network (SAHBN) is tested using data set in the biomedical domain. DNA repair genes are classified as either ageing-related or non-ageing-related based on their GO biological process terms. Furthermore, the performance of SAHBN was compared against eight conventional classification algorithms. Overall, SAHBN has outperformed existing algorithms in eight experiments out of eleven.

KEYWORDS

Semantic Data Mining, Hierarchical Bayesian Network, Gene Ontology, DNA Repair Gene, Human Ageing Process

1. INTRODUCTION

The ultimate aim of Data Mining (DM) algorithms is to extract useful knowledge from data. Fayyad et al. have defined these methods as the non-trivial process of identifying valid, novel, potentially useful, and ultimately understandable patterns in databases [1],[2]. However, existing mining algorithms treated data as meaningless numbers disregarding their semantic context [3],[4], Hence, the data mining philosophy has faced a paradigm shift from being a data-centered process to knowledge-centered process that aims to cater for domain knowledge and its integration in the mining process. The process of integrating domain knowledge with DM task is known as Semantic Data Mining [4] ,[5],[6].

Domain knowledge can be represented using various techniques. However, recent researches indicated that ontology are playing significant role in the process of knowledge acquisition and representation [7], [8]. In fact, the formal structure of ontology makes it a strong candidate for knowledge integration in the DM algorithms. Ontology could be intertwined with DM algorithms

Dhinaharan Nagamalai et al. (Eds) : CSEIT, NCS, SPM, NeTCoM - 2018
pp. 15–26, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81802

to bridge the semantic gap, to provide prior knowledge and constraints, and formally represent the mining results [9], [10]. Likewise, ontology can be used to facilitate different steps in the Bayesian Network (BN) construction process. It can assist in the identification of the BN structure and supports the calculation of the Conditional Probability Tables (CPT's) [11].

Hence, the process of developing a framework which systematically consolidates ontology and the Bayesian mining algorithm is investigated in this paper. The aim of this paper is to explore the potential advantage obtained from coupling the domain knowledge in the form of Gene Ontology (GO) and the Hierarchical Bayesian Network (HBN) classifier and then utilizing the developed model to predict the DNA repair gene effect in the human ageing process.

The structure of this paper is organized as follows. Section 2 explains the proposed model. Section 3 presents the experimental results and the evaluation process. Finally, section 4 draws conclusions and discusses possible future research directions.

2. PROPOSED MODEL

GO was used in this research because of its high quality and comprehensive nature in biomedical domain [12]. Meanwhile, the structure of the HBN implicitly provides more knowledge about the targeted domain [13]. As a results, the integration of these two concepts, GO and HBN, generate a classification model which seamlessly reflects the domain knowledge.

The proposed SAHBN classification model shares some initial steps with the standard classification algorithms such as data pre-processing and feature selections. However, the essential steps related to BN structure construction and variables probability estimation are designed in such a way that exploits the semantic nature of the GO. Figure1 compares the process sequence of standard classification algorithms and the proposed SAHBN model.

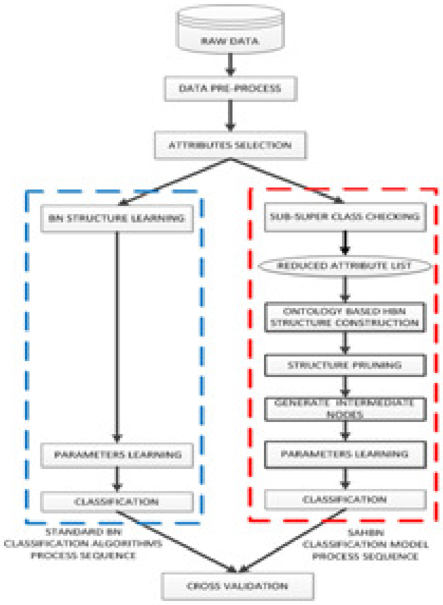


Figure 1 SAHBN Classification Model versus Standard Classification Algorithms Process Sequence

Figure1 shows that the selected prediction attributes have been further processed based on the semantic knowledge extracted from the GO. This can be seen in the steps surrounded by the red dotted line in the same figure. The new steps introduced by SAHBN model are summarized in the following subsections.

2.1. SUB-SUPER CLASS CHECKING

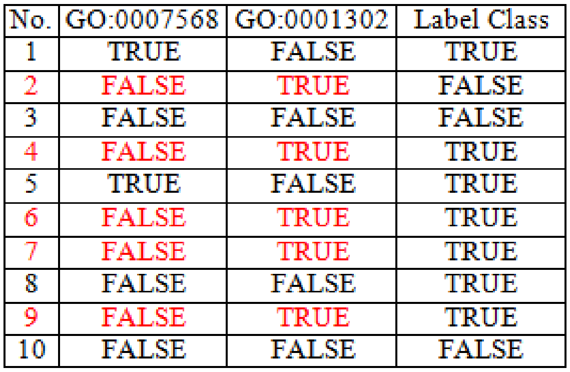
The first step which follows the attributes selection task is to check whether there is a semantic relation between the selected attributes. This is done by matching the selected attributes to the GO concepts. The data sets covered in this paper used the GO biological process (GOBP) terms as a prediction attributes. Hence, one-to-one matching between the selected attributes and the GO concepts was implemented. Consequently, the GO structure was exploited to extract the semantic relation between these attributes.

The relation that was targeted in this research is the parent-child ("is-a") class relation. GO used the "is-a" relation to represents the subtype relation between concepts. For example, "Replicative Cell Aging" is a subtype of and less general that the "Cell Aging" process. Likewise, the intermediate nodes in the HBN structure represent an aggregation of simpler nodes. Hence, the "is-a" relation was selected to identify the structure of the HBN.

The "is-a" relation not only facilitates the construction of the HBN structure, but also achieves the following objectives.

Maintain data consistency: The GO "is-a" relation follows the True Path Rule (TPR) which states that if an instance of GO node is proved to be true, so it's ancestors all the way to the root must be true. Otherwise, if an instance found to be false, so all its descendants to the leaf nodes must be false [14], [15], [16]. Thus, any two GO terms connected via the "is-a" relation and used as prediction attributes must follow the TPR. Otherwise, an inconsistent data set can be used to train the classification model, which may lead to inaccurate results.

Table 1 shows some records from the DNA repair gene-PPI data set (discussed in the 3rd section), which highlights the inconsistency in the training data set.



No.	GO:0007568	GO:0001302	Label Class
1	TRUE	FALSE	TRUE
2	FALSE	TRUE	FALSE
3	FALSE	FALSE	FALSE
4	FALSE	TRUE	TRUE
5	TRUE	FALSE	TRUE
6	FALSE	TRUE	TRUE
7	FALSE	TRUE	TRUE
8	FALSE	FALSE	TRUE
9	FALSE	TRUE	TRUE
10	FALSE	FALSE	FALSE

Table 1 Sample of Inconsistent Training Data Set

According to the GO structure, the GO:0001302 attribute is a child class of the GO:0007568. While the former refers to the replicative cell ageing, the latter refers to the ageing biological process, and there is an indirect "is-a" relationship between them. Hence, it can be seen that records 2,4,6,7 and 9 (highlighted in red in Table 1) are inconsistent because the value of the parent class is false, while the value of its child class is true and this violates the TPR.

Thus, this paper proposed the use of the Chi-squared to break the conflict between the contradicted prediction terms and eliminate data inconsistency. This is done in four steps, as follows:

a. Identify the contradictory GO prediction terms, which connected via the "is-a" relationship.

b. Calculate the Chi-squared value between each term and the label class.

c. Delete the GO term, which has the lowest dependency with the label class.

d. Repeat steps 1 throw 3 until all contradiction is removed.

Reduce prediction attributes list dimension: removing the contradicted attributes using GO "is-a" relation not only eliminates the inconsistency in the training data set but also reduces the dimension of the prediction attribute list. High dimensional data poses a serious challenge for data mining techniques, especially in medical domain.

2.2. ONTOLOGY-BASED HBN STRUCTURE CONSTRUCTION

The second step, which follows the parent-child class checking, is HBN structure construction. The structure construction task is implemented based on the reduced attributes list and the structure of the GO. The steps involved in this process are summarized in the following points.

a) Match each attribute in the reduced list generated after the parent-child class checking step to node in the GO.

b) Extract the path for each matched node (i.e. attribute node) using the "is-a" relation and the GO structure. The path is extracted from the matched node all the way to the root node. We began by extracting the parent class of the attribute node, and then the extracted parent class was considered as an attribute node and its parent class extracted. This process was repeated until the root node was reached.

c) Combine the extracted path to form a tree-like hierarchical structure.

Figure 2 depicts a sample of ontology-based HBN structure for attributes list consists of five GO terms {GO1, GO2, GO3, GO4, and GO5}. The predication attributes form the terminal nodes in the HBN structure and their parent classes shape the rest of the structure.

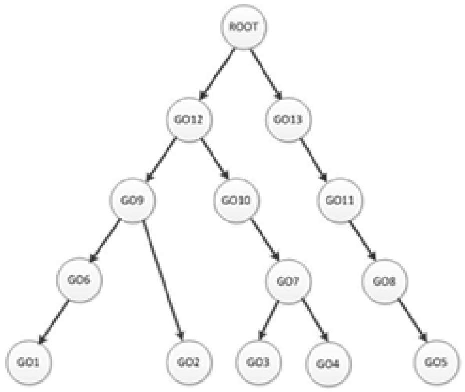


Figure 2 Ontology-based HBN structure

2.3. STRUCTURE PRUNING

The structure pruning step exploits the transitive nature of the "is-a" relationship in the GO. The "is-a" relation is transitive which mean that if "A is-a B", and "B is-a C", we can infer that "A is-a C". Hence, it is save to aggregate terms connected by the "is-a" relationship [17]. Figure 3 illustrates the structure pruning process.

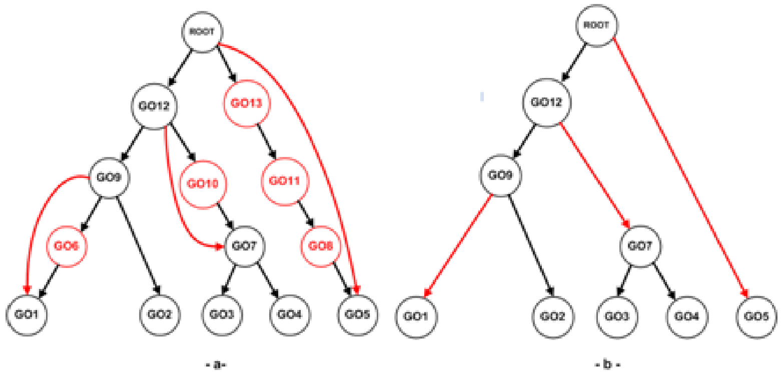


Figure 3 SAHBN Structure pruning process

The aim of this step is to remove redundant nodes that do not affect the principles of the HBN structure and maintain the semantic consistency of the targeted domain. There are two main basic principles underpinning the structure of the HBN. These principles can be summarized in the following points.

- Aggregation: each node in the HBN structure represents an aggregation of simpler nodes.
- Independency: each node in the HBN structure is conditionally independent of its non-descendant node given the value of its direct parent.

  Consequently, and in order to prune the created HBN structure without violating the above principles, the following steps were followed:

1. Delete all intermediate nodes that have only one child class.
2. The child class of the deleted node will be a child class of the deleted node parent class.

To demonstrate the pruning process, the above steps were applied to the structure of the HBN depicted in Figure 3 (a), which was constructed in the previous step. As a result GO6, GO8, GO10, GO11and GO13 terms, and the associated arcs, were deleted. The steps of the pruning process are summarized in Figure 3(b).

2.4. GENERATE INTERMEDIATE NODES

Figure 3 (b) shows that three intermediate nodes have been added to the structure of the HBN, namely, GO7, GO9, and GO12. Unlike the observed prediction attributes (i.e., terminal nodes), the value of the added intermediate nodes are unknown. However, as previously explained, the GO "is-a" relation is subject to the TPR. Consequently, the TPR principle was exploited to define the values of the intermediate nodes. This is done by implementing the following rule: "the value of any intermediate node is equal to true if and only if the value of any of its child classes is equal to true. Otherwise, its value is equal to false". Consequently, semantically consistent and complete training data set was generated.

2.5. PARAMETERS LEARNING

Having filled the intermediate nodes with values, the next step is to learn the SAHBN variables probability. There are two main approaches for estimating the probability values in the BN for complete dataset, namely, Maximum Likelihood Estimation (MLE) and Bayesian Estimation [18]–[21].

Despite its various advantages, the MLE method has the following limitation [19].

1. The size of the observed data set has no effect on the estimation process.

2. MLE does not consider the prior knowledge. Therefore, it entirely relies on the observed data set.

Hence, this paper has used a Bayesian-based approach, namely, Maximum a Posterior Estimation (MAP) method to estimate the probability values of the SAHBN variables.

3. EXPERIMENTAL RESULTS

This section discusses the experimental implementation and the obtained results. The first subsection gives an introduction on the human ageing case study. The second subsection explains the creation process of the DNA repair gene data set. Finally, the implementation of SAHBN model and the obtained results are analyzed in the third subsections.

3.1. HUMAN AGEING CASE STUDY

Human aging is defined as the gradual failure of the physiological function in various cells, tissues and organs in the human body, which ultimately leads to the fragility of body functionalities within the time growth and increases the probability of death [22]–[24].

Human ageing is an extremely complex, mysterious, controversial, and puzzling process that requires more investigation. Furthermore, studying the ageing process has led to challenges, such as ethical factors associated with doing experiments on human data, time form implementing the experiments on human data, and the comprehensive elements that must be considered when analyzing the ageing process. Thus, researchers have alternatively used the gene/protein databases of short living organism models to implement their experiments. Consequently, data mining techniques have been recently applied to analyze large amount of open access gene/protein databases to gain some insight into the human ageing process [25]–[28].

Human genome preserves its integrity by protecting the cellular DNA from both internal and external attacks. Thus, the cellular DNA is steadily monitored by the repair enzymes to correct damages resulting from these attacks. Accordingly, DNA damage is an essential element in the human ageing process, the modification of DNA repair process will result in advance understanding of the cellular ageing phenomena [27][29]. Hence the proposed SAHBN classification model applied to the DNA repair genes database to classify their effect as either an ageing-related or non-ageing-related gene.

3.2. DNA REPAIR GENE DATA SET CREATION

The data set used in this research has been created using the DNA repair gene [30], GenAge [31], Human Protein Reference [32], and UniPort [33] databases. The data set creation process can be summarized in the following steps.

1. Download the DNA repair gene database from the Human DNA repair genes website [30].

2. Classify the downloaded DNA repair genes into two categories, ageing-related and non-ageing related. The DNA repair genes appearing in the GenAge [31] database are classified as ageing-related, while the DNA repair genes that do not appear in the GenAge database are classified as non-ageing-related.

3. Represent the downloaded DNA repair genes in the form of proteins. This is done using the following steps.

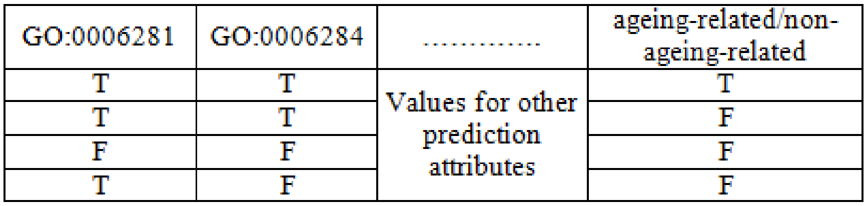
    a. Download the protein-protein interactions (PPI) from the human protein reference database [32].

    b. Select the interaction that at least one of the proteins is located in the DNA repair gene which generated in step 2.

    c. The type of evidence for the interactions is obtained from either in vitro or in vivo experiments.

4. Since the DNA repair genes are represented in form of PPI. Hence, they can be annotated in form of GO biological process (GO BP) terms using the UniProt [33] database.

Eventually, each DNA repair gene was represented in the form of a sequence of GO BP terms. The selected GO BP terms are associated with proteins that represent the DNA repair genes. The value of the GO BP terms was equal to "T" if it appears in the protein associated the DNA repair gene; otherwise, it was equal to "F". Table 2 presents sample of the DNA Repair Data Set.



GO:0006281	GO:0006284	....	ageing-related/non-ageing-related
T	T	Values for other prediction attributes	T
T	T		F
F	F		F
T	F		F

Table 2 Sample of the DNA Repair Data Set

3.3. RESULTS ANALYSIS

This subsection gives a detailed description of the experimental implementation and the obtained results. It discusses the proposed SAHBN model implementation, comparison with classical classification algorithms and results analysis.

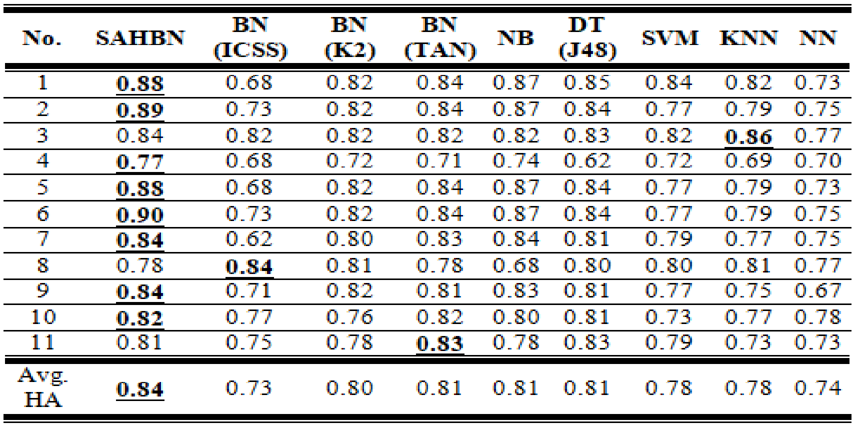
Eleven attributes selection methods were used to reduce the dimensions of the created data set. Consequently, the performance of the proposed SAHBN classification model was compared against the performance of different standard classification algorithms, such as Bayesian Network

(BN), Naïve Bayes (NB), Decision Tree (J48), Support Vector Machine (SVM), K Nearest Neighbor (KNN) and Neural Network (NN).

Classification accuracy is the most commonly used criteria to estimate the performance of the classification model. However, it has been argued that the classification accuracy can misjudge the model performance if the tested data set is imbalanced. Hence, this research used the harmonic mean of the average class accuracy as proposed by [34]. Equation (1) presents the formula of the harmonic mean for the average class accuracy.

$$average\ class\ accuracy_{HM} = \frac{1}{\frac{1}{|levels(t)|}\sum_{l\in levels(t)}\frac{1}{recall_l}} \qquad (1)$$

The harmonic mean of the average class accuracy was calculated for the proposed SAHBN model and the other 8 classification algorithms against which SAHBN was compared. This process is repeated for all 11 combinations of attribute selection methods. Consequently, the obtained results are summarized in Table 3.

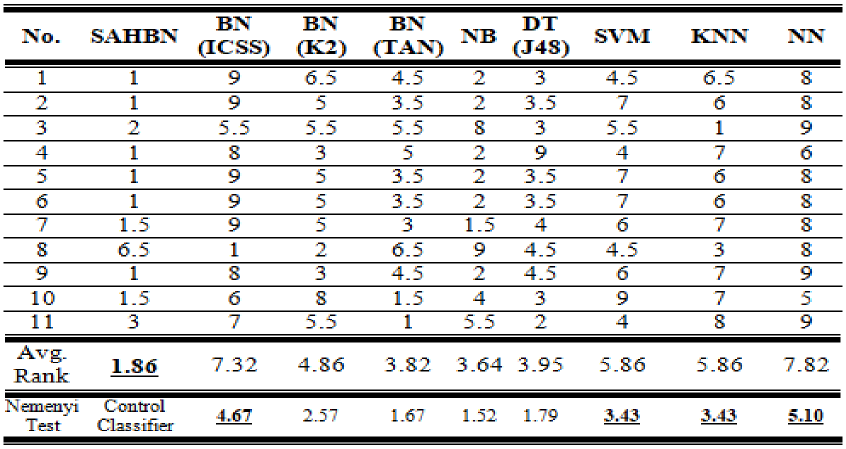


No.	SAHBN	BN (ICSS)	BN (K2)	BN (TAN)	NB	DT (J48)	SVM	KNN	NN
1	**0.88**	0.68	0.82	0.84	0.87	0.85	0.84	0.82	0.73
2	**0.89**	0.73	0.82	0.84	0.87	0.84	0.77	0.79	0.75
3	0.84	0.82	0.82	0.82	0.82	0.83	0.82	**0.86**	0.77
4	**0.77**	0.68	0.72	0.71	0.74	0.62	0.72	0.69	0.70
5	**0.88**	0.68	0.82	0.84	0.87	0.84	0.77	0.79	0.73
6	**0.90**	0.73	0.82	0.84	0.87	0.84	0.77	0.79	0.75
7	**0.84**	0.62	0.80	0.83	0.84	0.81	0.79	0.77	0.75
8	0.78	**0.84**	0.81	0.78	0.68	0.80	0.80	0.81	0.77
9	**0.84**	0.71	0.82	0.81	0.83	0.81	0.77	0.75	0.67
10	**0.82**	0.77	0.76	0.82	0.80	0.81	0.73	0.77	0.78
11	0.81	0.75	0.78	**0.83**	0.78	0.83	0.79	0.73	0.73
Avg. HA	**0.84**	0.73	0.80	0.81	0.81	0.81	0.78	0.78	0.74

Table 3 Ten-Folds Cross Validation Test Results in Terms of the Harmonic Mean of the Average Class Accuracy

Table 3 shows that the proposed SAHBN classification model outperformed conventional classification algorithms in eight experiments. Furthermore, SAHBN scored the highest average harmonic class accuracy among all classifiers.

The performance of SAHBN model was further analyzed using more sophisticated non-parametric statistical test. Precisely, Friedman test followed by Nemenyi Post-Hoc evaluation are implemented for all 11 data set combinations. SAHBN was used as a control classifier against which all other 8 conventional classifiers were compared. Consequently the results are presented in Table 4.



No.	SAHBN	BN (ICSS)	BN (K2)	BN (TAN)	NB	DT (J48)	SVM	KNN	NN
1	1	9	6.5	4.5	2	3	4.5	6.5	8
2	1	9	5	3.5	2	3.5	7	6	8
3	2	5.5	5.5	5.5	8	3	5.5	1	9
4	1	8	3	5	2	9	4	7	6
5	1	9	5	3.5	2	3.5	7	6	8
6	1	9	5	3.5	2	3.5	7	6	8
7	1.5	9	5	3	1.5	4	6	7	8
8	6.5	1	2	6.5	9	4.5	4.5	3	8
9	1	8	3	4.5	2	4.5	6	7	9
10	1.5	6	8	1.5	4	3	9	7	5
11	3	7	5.5	1	5.5	2	4	8	9
Avg. Rank	**1.86**	7.32	4.86	3.82	3.64	3.95	5.86	5.86	7.82
Nemenyi Test	Control Classifier	**4.67**	2.57	1.67	1.52	1.79	**3.43**	**3.43**	**5.10**

Table 4 Classification algorithms ranking (Friedman Test)

Table 4 reports that SAHBN model was significantly outperformed NN, BN (ICSS), SVM, and KNN. Additionally, it shows that SAHBN perform much better that the K2 search-based Bayesian Network classifier. Furthermore, the performance of DT (J48), TAN search-based Bayesian Network and NB were slightly lower than SAHBN.

Finally, the results are depicted using the Critical Difference (CD) significant diagram proposed by [35]. Figure 4 plots the compared classifiers in Y axis, and their corresponding mean ranks in the X axis. The line to the right of each classifier's mean rank represents the critical difference associated with the classifier. That is, other classifiers mean ranks located to the right of the critical difference line are significantly outperformed by the correspond classifier.

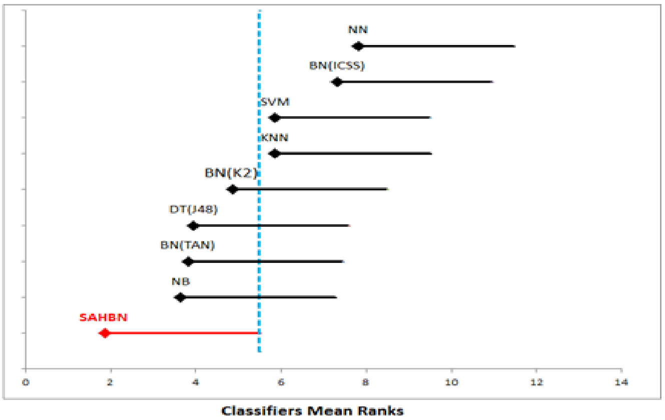


Figure 4 Pairwise comparisions of all classifiers

4. Discussion and Conclusions

This paper investigated the potential advantages of integrating the domain knowledge in the form of GO and the HBN classifier. Accordingly, the proposed Semantically Aware Hierarchical Bayesian Network (SAHBN) classification model was tested using data set in the biomedical domain. Consequently, the findings extracted from analyzing the obtained results indicated that SAHBN model demonstrated a very competitive performance in comparison with conventional classification algorithms. SAHBN model outperformed existing algorithms in eight experiments out of eleven. Furthermore, it scored the highest average performance rank among all other classifiers.

SAHBN model exploited the ontological knowledge to construct a consistent training data set and eliminate contradictions between prediction attributes. Additionally, SAHBN structure implicitly reflects the background knowledge of the targeted domain. Hence, it is a self-explanatory structure that can be readily be maintained.

SAHBN model not only highlighted the advantages of integrating ontology with the HBN classifier but also laid out the foundations to consider amore semantic relations between prediction attributes, such as equivalent, disjoint union and intersection. Future works, will investigate the advantages of integrating more ontological knowledge with the SAHBN classification model.

In summary, the SAHBN model consolidated the GO and the HBN classification algorithms in flexible framework that preserves the advantage of ontology and Bayesian theory. Initial results revealed very promising findings that establish a solid foundation for future research.

REFERENCES

[1] U. Fayyad, G. Piatetsky-Shapiro, And P. Smyth, “From Data Mining To Knowledge Discovery In Databases,” Ai Mag., Vol. 17, No. 3, Pp. 37–54, 1996.

[2] C. Zhang And S. Zhang, Association Rule Mining: Models And Algorithms. Springer-Verlag Berlin Heidelberg. Xii, 244., 2002.

[3] P. K. Novak, A. Vavpetic, I. Trajkovski, And N. Lavrac, “Towards Semantic Data Mining With G-Segs,” In Proceedings Of The 11th International Multiconference Information Society, Is, 2009.

[4] F. Benites And E. Sapozhnikova, “Using Semantic Data Mining For Classification Improvement And Knowledge Extraction,” In Ceur Workshop Proceedings, 2014, Vol. 1226, Pp. 150–155.

[5] L. Cao, “Domain-Driven Data Mining: Challenges And Prospects,” Ieee Trans. Knowl. Data Eng., Vol. 22, No. 6, Pp. 755–769, 2010.

[6] C. Antunes And A. Silva, “New Trends In Knowledge Driven Data Mining A Position Paper,” Proc. 16th Int. Conf. Enterp. Inf. Syst., Pp. 346–351, 2014.

[7] S. Staab And R. Studer, Hand Book On Ontologies. Springer Science & Business Media, 2013.

[8] G. Mansingh And L. Rao, “The Role Of Ontologies In Developing Knowledge Technologies,” Knowl. Manag. Dev. Springer Us, Pp. 145–156, 2014.

[9] H. Liu, “Towards Semantic Data Mining,” In Proc. Of The 9th International Semantic Web Conference (Iswc2010). 2010.

[10] D. Dou, H. Wang, And H. Liu, “Semantic Data Mining: A Survey Of Ontology-Based Approaches,” In Proceedings Of The 2015 Ieee 9th International Conference On Semantic Computing, Ieee Icsc 2015, 2015, Pp. 244–251.

[11] S. Fenz, “An Ontology-Based Approach For Constructing Bayesian Networks,” Data Knowl. Eng., Vol. 73, Pp. 73–88, 2012.

[12] J. A. Blake, “Ten Quick Tips For Using The Gene Ontology,” Plos Comput Biol, Vol. 9, No. 11, P. E1003343, 2013.

[13] E. Gyftodimos And P. A Flach, "Hierarchical Bayesian Networks : An Approach To Classification And Learning For Structured Data," Proceedings Of The Ecml/Pkdd - 2003 Workshop On Probablistic Graphical Models For Classification, Vol. 3025. Pp. 291–300, 2004.

[14] J. A. Blake And M. A. Harris, "The Gene Ontology (Go) Project: Structured Vocabularies For Molecular Biology And Their Application To Genome And Expression Analysis," Current Protocols In Bioinformatics, No. Suppl. 23. 2008.

[15] S. Götz And A. Conesa, Visual Gene Ontology Based Knowledge Discovery In Functional Genomics. Intech Open Access Publisher, 2011.

[16] R. P. Huntley, T. Sawford, M. J. Martin, And C. O'donovan, "Understanding How And Why The Gene Ontology And Its Annotations Evolve: The Go Within Uniprot.," Gigascience, Vol. 3, No. 1, P. 4, 2014.

[17] "Gene Ontology Consortium | Gene Ontology Consortium." [Online]. Available: Http://Www.Geneontology.Org/. [Accessed: 21-Dec-2016].

[18] T. D. Nielsen And F. V. Jensen, Bayesian Network And Decision Graph. Springer Science & Business Media, 2009.

[19] D. Koller And N. Friedman, Probabilistic Graphical Models: Principles And Techniques. Mit Press, 2009.

[20] R. G. Almond, R. J. Mislevy, L. S. Steinberg, D. Yan, And D. M. Williamson, "Learning In Models With Fixed Structure," Bayesian Networks Educ. Assessment. Springer New York, Pp. 279–330, 2015.

[21] Z. Ji, Q. Xia, And G. Meng, "A Review Of Parameter Learning Methods In Bayesian Network," In Advanced Intelligent Computing Theories And Applications: 11th International Conference, Icic 2015, Fuzhou, China, August 20-23, 2015. Proceedings, Part Iii, D.-S. Huang And K. Han, Eds. Cham: Springer International Publishing, 2015, Pp. 3–12.

[22] H. E. Wheeler And S. K. Kim, "Genetics And Genomics Of Human Ageing.," Philos. Trans. R. Soc. Lond. B. Biol. Sci., Vol. 366, No. 1561, Pp. 43–50, 2011.

[23] H. Lees, H. Walters, And L. S. Cox, "Animal And Human Models To Understand Ageing," Maturitas, 2016.

[24] T. B. Kirkwood, "The Origins Of Human Ageing.," Philos. Trans. R. Soc. Lond. B. Biol. Sci., Vol. 352, No. 1363, Pp. 1765–72, 1997.

[25] C. Wan, A. A. Freitas, And J. P. De Magalhaes, "Predicting The Pro-Longevity Or Anti-Longevity Effect Of Model Organism Genes With New Hierarchical Feature Selection Methods," Ieee/Acm Trans. Comput. Biol. Bioinforma., Vol. 12, No. 2, Pp. 262–275, 2015.

[26] J. P. De Magalhães Et Al., "The Human Ageing Genomic Resources: Online Databases And Tools For Biogerontologists," Aging Cell, Vol. 8, No. 1. Pp. 65–72, 2009.

[27] A. A Freitas, O. Vasieva, And J. P. De Magalhães, "A Data Mining Approach For Classifying Dna Repair Genes Into Ageing-Related Or Non-Ageing-Related.," Bmc Genomics, Vol. 12, No. 1, P. 27, 2011.

[28] C. Wan And A. Freitas, "Prediction Of The Pro-Longevity Or Anti-Longevity Effect Of Caenorhabditis Elegans Genes Based On Bayesian Classification Methods," In Bioinformatics And Biomedicine (Bibm), 2013 Ieee International Conference On, 2013, Pp. 373–380.

[29] R. D. Wood, M. Mitchell, J. Sgouros, And T. Lindahl, "Human Dna Repair Genes.," Science, Vol. 291, No. 5507, Pp. 1284–9, 2001.

[30] "Human Dna Repair Genes." [Online]. Available: Http://Sciencepark.Mdanderson.Org/Labs/Wood/Dna_Repair_Genes.Html. [Accessed: 08-Dec-2016].

[31] "Genage: The Ageing Gene Database." [Online]. Available: Http://Genomics.Senescence.Info/Genes/. [Accessed: 08-Dec-2016].

[32] "Human Protein Reference Database." [Online]. Available: Http://Www.Hprd.Org/Index_Html. [Accessed: 08-Dec-2016].

[33] "Uniprot." [Online]. Available: Http://Www.Uniprot.Org/. [Accessed: 08-Dec-2016].

[34] J. D. Kelleher, B. Mac Namee, And A. D'arcy, "Fundamentals Of Machine Learning For Predictive Data Analytics." Mit Pr, 2015.

[35] S. Lessmann, B. Baesens, C. Mues, And S. Pietsch, "Benchmarking Classification Models For Software Defect Prediction: A Proposed Framework And Novel Findings," In Ieee Transactions On Software Engineering, 2008, Vol. 34, No. 4, Pp. 485–496.

AUTHORS

Hasanein Alharbi received his PhD from the School of Computing, Science and Engineering at the University of Salford-Manchester. He holds a master's degree in Computer Application (MCA) from Sardar Patel University in India and a BSc in Computer Science from the University of Babylon, Iraq. Hasanein particular research interests are in the area of semantic data mining, integrating ontology with mining algorithms and mining the linked open data.

FUZZY BOOLEAN REASONING FOR DIAGNOSIS OF DIABETES

Mohamed Benamina, Baghdad Atmani and Sofia Benbelkacem

Laboratoire d'Informatique d'Oran (LIO)
University of Oran 1 Ahmed Ben Bella
BP 1524, El M'Naouer Es Senia, 31 000 Oran, Algeria

ABSTRACT

The classification by inductive learning finds its originality in the fact that humans often use it to resolve and to handle very complex situations in their daily lives. However, the induction in humans is often approximate rather than exact. Indeed, the human brain is able to handle imprecise, vague, uncertain and incomplete information. Also, the human brain is able to learn and to operate in a context where uncertainty management is indispensable. In this paper, we propose a Boolean model of fuzzy reasoning for indexing the monitoring sub-plans, based on characteristics of the classification by inductive learning. Several competing motivations have led us to define a Boolean model for CBR knowledge base systems. Indeed, we have not only desired experiment with a new approach to indexing of cases by fuzzy decision tree, but we also wanted to improve modelling of the vague and uncertain of the natural language concepts, optimize response time and the storage complexity.

KEYWORDS

Boolean Modelling, Cellular Machine, Case-Based Reasoning, Diabetes Diagnosis, Fuzzy Reasoning, Planning.

1. INTRODUCTION

The problem of planning and scheduling of tasks is one of the most complex problems in the field of Artificial Intelligence. The best-known situations include crisis management, production management, project management, robotics, medical, etc. The goal of planning is to provide a system (robotics, computer, human, ...) the capacity to reason to interact with its environment in an autonomous manner, in order to achieve the objectives that have been assigned.

Scheduling is organized in time a set of tasks. Historically, scheduling problems were discussed initially in the field of operational research (graph dynamic programming, linear programming, methods of combinatorial optimization theory), but quickly showed their limits in terms of expressiveness. Artificial intelligence and knowledge-based systems are then addressed the problem, renewing techniques through a richer representation of the domain knowledge (problems of satisfaction of constraints, constraints propagation algorithms, constraint programming languages). Among knowledge-based systems we looked on the reasoning from case (CBR). The CBR based on artificial intelligence techniques is an approach to problem solving that uses past experiences to solve new problems by finding similar cases in its knowledge base and adapting them to the particular case. All the experiences form a case basis. Each case is represented by a knowledge experience. This experience is a lesson for the CBR system to solve problems of various kinds. The CBR consists of five phases: (1) Elaboration of

Dhinaharan Nagamalai et al. (Eds) : CSEIT, NCS, SPM, NeTCoM - 2018
pp. 27–44, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81803

the case; (2) Retrieval; (3) Adaptation; (4) Review; (5) Memory. For our project we are interested in the second phase: retrieval.

Therefore our contribution in this area is double, on the one hand it offers a reactive planning module based on a CBR for the optimization of the scheduling, and on the other hand it offers a classification induction graph [1] for the acceleration of the indexing of cases: remembering. The classification issue is to assign the various observations to categories or predefined classes [2] [3]. In general classification methods consist in several stages. The most important step is to develop the rules of classification from a priori knowledge; it is the learning phase [4]. The classification by inductive learning finds its originality in the fact that humans often use it to resolve and to handle very complex situations in their daily lives [5]. However, the induction in humans is often approximate rather than exact. Indeed, the human brain is able to handle imprecise, vague, uncertain and incomplete information [6]. Also, the human brain is able to learn and to operate in a context where uncertainty management is indispensable. In this paper, we propose a Boolean model of fuzzy reasoning for indexing the sub-plans [13], based on characteristics of the classification by inductive learning in humans [7].

This article is structured as follows. Section 2 presents a state of the art about the use of fuzzy decision tree in the retrieval step of CBR, and also work about cellular automaton and Boolean modelling. Section 3 is devoted to the proposed approach Fuzzy-BML-CBR. Section 4 presents results of experimentation. Finally, we present the guidance of our contribution and experimentation and we conclude in section 5.

2. LITERATURE REVIEW

We present the state of the art in two ways. First, we quote work which combine fuzzy reasoning with decision tree in the retrieval step of CBR. Then, we give works about cellular automaton and Boolean modeling.

2.1. FUZZY DECISION TREE FOR RETRIEVAL

Fuzzy decision tree have been applied in various areas and specifically in medicine. Boyen and Wehenkel [8] describe a new algorithm able to infer fuzzy decision trees in domains where most of the input variables are numerical and output information is best characterized as a fuzzy set. It comprises three complementary steps: growing for selecting relevant attributes and fuzzy thresholds; pruning for determining the appropriate tree complexity; refitting for tuning the tree parameters in a global fashion. Begum et al. [9] presented a case-based decision support system to assist clinicians in stress diagnosis. Case-based reasoning is applied as the main methodology to facilitate experience reuse and decision explanation by retrieving previous similar temperature profiles. Further fuzzy techniques are also employed and incorporated into the case-based reasoning system to handle vagueness, uncertainty inherently existing in clinicians reasoning as well as imprecision of feature values. The work of Barrientos and Sainz [10] provides support for decision making about resource planning of an emergency call center in order to reach its mandatory quality of service. This is carried out by the extraction of interpretable knowledge from the activity data collected by an emergency call center. A linguistic prediction, categorization and description of the days based on the call center activity and information permits the workload for each category of day to be known. This has been generated by a fuzzy version of an unsupervised decision tree, merging decision trees and clustering. Levashenko and Zaitseva [11] proposed a decision making support system based on fuzzy logic for oncology disease diagnosis. The decision making procedure corresponds to the classification of the new case by analyzing a set of instances for which classes are known. Solved cases are defined as fuzzy classification rules that are formed by different fuzzy decision trees. Three types of fuzzy decision trees are considered in the paper: non-ordered, ordered and stable. Induction of these fuzzy decision trees is based on cumulative information estimates. Adidela [12] proposed a Hybrid Classification System to predict the occurrence of diabetes. The system adopts three phases. In the first phase, clustering of the data using EM-algorithm is performed. The second phase carries out the classification of the obtained individual clusters using fuzzy ID3. As of the second phase of the process, adaptation rules are obtained. These rules are essential in the prediction of diabetes. In the third phase the test tuple is supplied to the rules to predict the class label. Benamina et al [13] combined fuzzy logic and decision tree to improve the response time and the accuracy of the retrieval of similar cases. The proposed Fuzzy case-based reasoning is composed of two complementary parts, a classification by fuzzy decision tree and a CBR part. The aim of this approach was to reduce the complexity of calculating similarity degree between diabetic patients.

2.2. CELLULAR AUTOMATON AND BOOLEAN MODELLING

The objective of our approach is double: first, it provides a reactive planning module based on CBR for scheduling optimization; secondly it generates a classification decision tree to accelerate the indexing of sub-plans. The second step uses the Boolean modeling. So, the cellular machine allows to reduce the size of decision tree and to optimize automatically the generation of symbolic rules [3].

Amrani et al. [14] proposed an approach based on cellular automata for regulation and reconfiguration of urban transportation systems. Barigou et al. [15] proposed a Boolean modeling approach which uses a boolean inference engine based on a cellular automaton to do extraction. Atmani et al. [16] proposed a boolean modeling of the fuzzy reasoning and used the characteristics of induction graph classification. The retrieval phase of CBR was modeled in the form of a database with membership functions of fuzzy rules. Brahami et al. [17] exploited different data sources for improving the process of acquisition of explicit knowledge on an organization by producing inductive Boolean rules. Benfriha et al. [18] proposed a new text categorization framework based on a cellular automaton for Symbolic Induction. Aissani et al. [19] exploited a Job Shop scheduling log and simulations to extract knowledge enabling to create rules for the selection of priority rules. These rules are implemented in a CASI cellular automaton. First, symbolic modeling of the scheduling process is exploited to generate a decision tree. Then, decision rules are extracted to select priority rules. Finally, the rules are integrated in CASI which implements the decisional module of agents in a distributed manufacturing control system.

3. PROPOSED APPROACH FUZZY-BML-CBR

The architecture of the proposed Fuzzy-BML-CBR for diabetes application is given in figure 1. The main aim of the proposed framework is on improving the accuracy of Diabetes classification. The followings are the main contributions of this paper:

- The proposed framework is a novel combination of different techniques that perform classification to Diabetes patients using Fuzzy data mining, Boolean modeling and CBR;
- Fuzzy decision tree classifier is used to generate a crisp set of rules;
- Fuzzy modeling is used to deal with the uncertainty related to the medical reasoning;
- Boolean modeling is used for fuzzy rules optimization and inference;
- Case based reasoning.

It is composed of two complementary parts, the fuzzy boolean modeling part using Fispro and the case based reasoning part using JColibri platform. FisPro has been used for various modeling projects [20], and we hope that the approach presented in this paper will help in new modeling tasks. JColibri [21] is an object-oriented tool dedicated to the development of case-based reasoning applications. It is an open source tool that allows the user to customize the classes and methods of the platform according to specific needs.

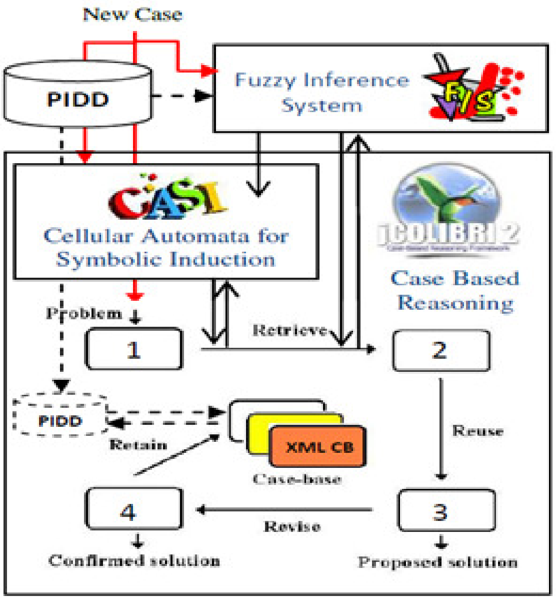


Figure 1. Fuzzy-BML-CBR for diabetes application

The main steps of the proposed framework are :

- Construction by Fispro of the fuzzy decision tree and extraction of the fuzzy rule base;
- From the fuzzy decision tree CASI begin the boolean modelling for the construction of the boolean fuzzy decision tree.
- Finally, JColibri combine the fuzzy inference system and CASI to improve the response time and the accuracy of the retrieval of similar cases.

3.1. CELLULAR AUTOMATON AND BOOLEAN MODELING

3.1.1. PIMA INDIANS DIABETES DATABASE

The Pima Indian Diabetes Dataset (PIDD) has been taken from the UCI Machine Learning repository. The input variable are Plasma glucose concentration in 2-hours OGTT(Glucose), 2-hour serum insulin(INS), Body mass index(BMI), Diabetes pedigree function(DPF), Age(Age) and the output variable are Diabetes Mellitus(DM) (Table 1). The data with the age group from 25-30 are taken to test the Fuzzy Inference Mechanism Framework [22].

Table 1. Attributes of PIDD.

Abbreviation	Full name	UoM
Pregnant	Number of times pregnant	-
Glucose	Plasma glucose concentration in 2-hours OGTT	mg/dl
DBP	Diastolic blood pressure	mmHg
TSFT	Triceps skin fold thickness	mm
INS	2-hour serum insulin	mu U/ml
BMI	Body mass index	Kg/m2
DPF	Diabetes pedigree function	-
Age	Age	-
DM	Diabetes Mellitus where 1 is interpreted as tested positive for diabetes	

3.1.2. FUZZY MODELING USING FISPRO

Figure 2 illustrates the fuzzy inference system. Firstly, a crisp set of input data are gathered and converted to a fuzzy set using fuzzy linguistic variables, fuzzy linguistic terms and membership functions. This step is known as fuzzification. Afterwards, an inference is made based on a set of rules. Lastly, the resulting fuzzy output is mapped to a crisp output using the membership functions, in the defuzzification step.

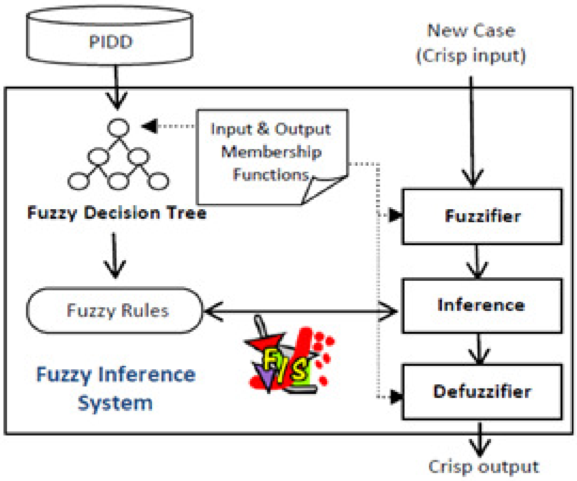


Figure 2. Fuzzy Inference System

The process of fuzzy inference mechanism is explained in Algorithm 1.
Algorithm 1 Fuzzy logic algorithm [13]:

1. Define the linguistic variables and terms (initialization).
2. Construct the membership functions (initialization).
3. Construct the fuzzy decision tree and the fuzzy rule base (initialization).
4. Convert crisp input data to fuzzy values using the membership functions (fuzzification).
5. Evaluate the rules in the fuzzy rule base (inference).
6. Combine the results of each rule (inference).
7. Convert the output data to non-fuzzy values (defuzzification).

Fuzzification : The conversion from crisp to fuzzy input is known as fuzzification [23]. Each crisp input is converted to its fuzzy equivalent using a family of membership function. Additionally, an interface is offered to tune and validate the parameters of the built fuzzy numbers. The parameter is fixed with Minimum value, Mean, Standard Deviation, Maximum value for each variable. Then the membership function μ (x) of the triangular fuzzy number is given by :

$$\mu(x) = \begin{Bmatrix} 0, x \le a \\ (x - a)/(b - a), a < x \le b) \\ (c - x)/(c - b), b < x \le c \\ 0, x > c \end{Bmatrix}$$

The parameters of fuzzy numbers are listed in Table 2.

Table 2. Parameters of triangular membership functions [22].

Fuzzy variables	Fuzzy Numbers	Fuzzy Triangular numbers
Glucose (Plas)	Low	[0, 88.335, 121.408]
	Medium	[88.335, 121.408, 166.335]
	High	[121.408, 166.335 ,199]
INS (Insu)	Low	[0 ,17.276, 173.175]
	Medium	[17.276, 173.175, 497]
	High	[173.175,497, 846]
BMI (Mass)	Low	[0, 0, 27.792]
	Medium	[0, 27.792, 38.864]
	High	[27.792, 38.864, 67.1]
DPF (Pedi)	Low	[0.078, 0.272, 0.682]
	Medium	[0.272, 0.682, 1.386]
	High	[0.62, 1.386, 2.42]
Age (Age)	Young	[21, 25.475, 40.537]
	Medium	[25.475, 40.537, 57.798]
	Old	[40.537, 57.798, 81]
DM (Class)	Very low	[0, 0, 0.25]
	Low	[0, 0.25, 0.5]
	Medium	[0.25, 0.5, 0.75]
	High	[0.5, 0.75, 1]
	Very high	[0.75, 1, 1]

Fuzzy inference engine : In our study, we make use of the Fuzzy Decision Trees (FDT), which are an extension of classical decision trees [1] [24] and constitute a popular elaborate application of region based methods. The FDT proposed in FisPro are based on the algorithm presented in [25]. The FisPro implementation relies on a predefined fuzzy partition of the input variables, which is left untouched by the tree growing algorithm.

FisPro is an open source tool for creating fuzzy inference systems (FIS) to be used for reasoning purposes, especially for simulating a physical or biological system [20]. It includes many algorithms (most of them implemented as C programs) for generating fuzzy partitions and rules directly from experimental data. In addition, it offers data and FIS visualization methods with a java-based user-friendly interface. We make use of the Fuzzy Decision Trees (FDT) [26] algorithm provided by FisPro.

Defuzzification : Defuzzification process is conducted to convert aggregation result into a crisp value for DM output. In this process a single number represents the outcome of the fuzzy set. The final combined fuzzy conclusion is converted into a crisp value by using the centroid method [13].

3.2. CELLULAR AUTOMATA FOR SYMBOLIC INDUCTION

3.2.1. CLASSIFICATION BY INDUCTIVE LEARNING

In a context of diabetic patients monitoring [27], setting up tools for accident detection is not possible without considering the necessary role that the physician must have. The aim is to design a system for assisted monitoring and diagnosis that will provide specialists with the necessary information for identifying the diabetes type of patients.

Let $\Omega = \{\omega_1, \omega_2, ..., \omega_n\}$ be the population of diabetic patients taken into account for the training. An attribute is associated with this population, called endogenous variable (also called explicative variable or class attribute), denoted *C*.

A class $C(\omega)$ can be associated with every individual ω. The endogenous variable *C* takes its values in the set *IC* of class identifiers.

$$C\text{:}\ \ \Omega \rightarrow IC = \{c_1, c_2,...,c_m\}$$

$$\omega_i \rightarrow C(\omega_i) = c_j$$

The data are taken from PIDD, the input variable are Plasma glucose concentration in 2-hours OGTT(Glucose), 2-hour serum insulin(INS), Body mass index(BMI), Diabetes pedigree function (DPF), Age (Age) and the output variable are Diabetes Mellitus (DM). This will be designated by an endogenous variable.

$$C\text{: } \Omega \rightarrow IC = \{c_1, c_2\}.$$

The objective is to define a function φ for predicting the class C, thus the diagnosis of diabetes. The determination of the prediction model φ, which is the goal of the training, is bound to the hypothesis that the values taken by the endogenous variable *C* are not at random, but depend upon certain individual situations, called exogenous variables that are determined by the expert.
The exogenous variables concerning an individual constitute a tuple of attributes:

$$X = \{X_1, X_2,...,X_p\}$$

The exogenous variables take their values in a set *IM* of mode identifiers:

$$X\text{:}\ \ \Omega \rightarrow IM = \{c_1, c_2,...,c_m\}$$
$$X(\omega) = \{X_1(\omega), X_2(\omega),...,X_p(\omega)\}$$

The value taken by $X_j(\omega)$ is called the modality of the attribute X_j for ω. In our case the exogenous variables are summarized in Table 3.

Table 3. Exogenous variables, semantics and possible modality.

Exogenous Var.	**Semantics**	**Modality**
X1	Glucose	low, medium, high
X2	DBP	low, medium, high
X3	TSFT	low, medium, high
X4	INS	low, medium, high
X5	BMI	low, medium, high
X6	DPF	low, medium, high
X7	Age	young, medium, old
Y	DM	very low, low, medium, high, very high

Updating φ requires two samples denoted Ωa and Ωt, which are subsets of Ω. The first one, Ωa, used for training, will serve for the construction of φ. The second one, Ωt, used for test, will serve for testing the validity of φ. For all patients ω∈(Ωa ∪ Ωt) we assume that both the values $X(\omega)$ and the class $C(\omega_i)$ are known. We also define Ωe, the set of individuals in Ωt (patients) not correctly classified during the test of the symbolic training. The data with the age group from 25-30 are taken to test the Fuzzy Decision Tree [22].

3.2.2. General Process of Training

The general process of training followed by our cellular system CASI (Cellular Automaton for Symbolic Inference) is organized in three stages :

1. Boolean generation and optimization of the decision tree by the cellular automaton (BOG-CASI);

2. Fuzzy conjunctive rules inference by the cellular automaton (BIE-CASI);

3. Validation by the cellular automaton (BV-CASI).

Figure 3 summarizes the general diagram of our system CASI.

Boolean Generation and Optimization (BOG) of the Decision Tree : In this section, we present the principles of construction, by boolean modelling [15] [23] [28] [29] [30] of induction decision tree in the problems of discrimination and classification [3] [28]: we want to explain the class taken by one variable to predict categorical Y, attribute class or endogenous variable; from a series of p variables $X = \{X_1, X_2,...,X_p\}$ denoted variable predictive (descriptors) or exogenous, discrete or continuous. According to the terminology of machine learning, we are therefore in the context of supervised learning.

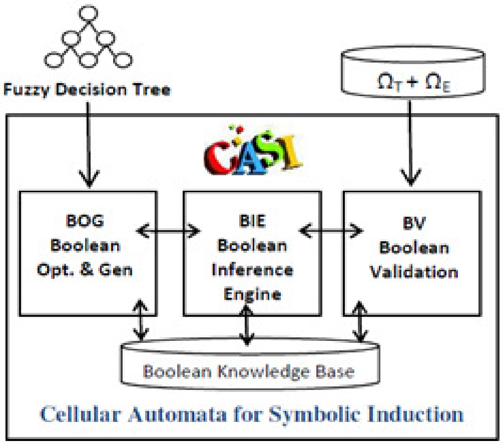


Figure 3. Cellular Automaton for Symbolic Inference (CASI)

From the sample Ω_a we begin the symbolic treatment for the construction of the decision tree (method ID3).

1. Initialize the parameters and the initial partition S_0 *;*

2. Use the ID3 method to pass of partition S_i to S_{i+1} and generate the decision tree.

3. Finally, generation of prediction rules.

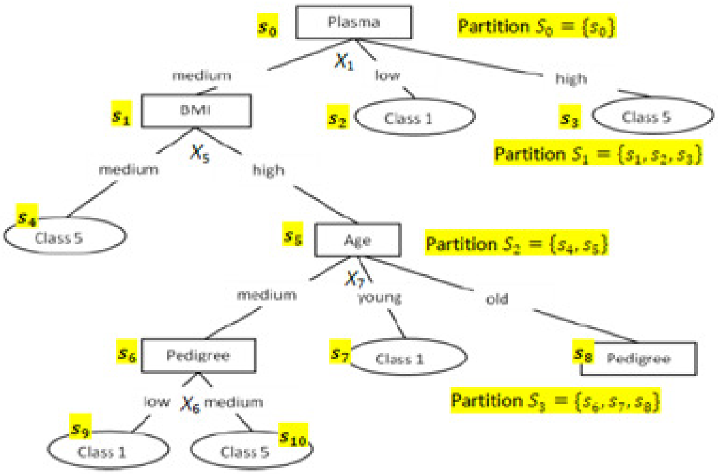
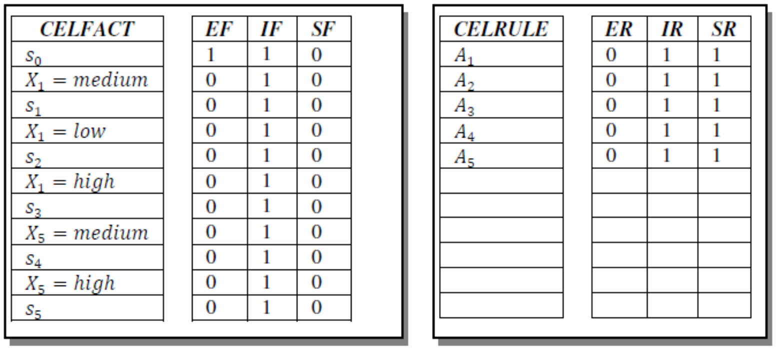


Figure 4. Example of a fuzzy decision tree

The initial partition S_0 has one noted s_0 element, which includes the entire sample learning. The next partition S_1 is generated by the variable X_1 after fuzzification and individuals in each node s_j are defined as follows: s_1 ={ω∈Ωa / $X_1(\omega)$ = medium} ; s_2 ={ω∈Ωa / $X_1(\omega)$ = low} and s_3 ={ω∈Ωa / $X_1(\omega)$ = high}.

As well as in the s_0 node, there are in s_1, s_2 and s_3, individuals of the classes{c_1, c_2}. The figure 5 summarizes the steps of construction of s_0, s_1, s_2 and s_3. The S_1 partition, the process is repeated looking for a S_2 score which would be better. We use the three arcs A_1, A_2 and A_3 to reach the vertices s_1, s_2 and s_3. Similarly A_4 and A_5 to reach the vertices s_4 and s_5.

To illustrate the architecture and the operating principle of the BOG module, we consider figure 4 with the S_0={s_0} partitions and S_1={s_1, s_2, s_3}. Figure 5 shows how the knowledge extracted from this graph database is represented by the *CELFACT* and *CELRULE* layers.



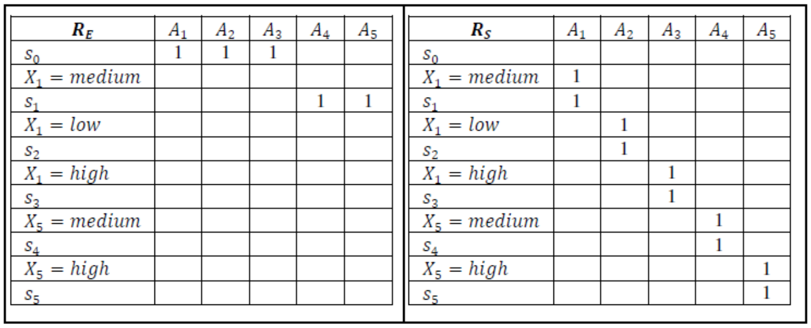
CELFACT	*EF*	*IF*	*SF*
s_0	1	1	0
$X_1 = medium$	0	1	0
s_1	0	1	0
$X_1 = low$	0	1	0
s_2	0	1	0
$X_1 = high$	0	1	0
s_3	0	1	0
$X_5 = medium$	0	1	0
s_4	0	1	0
$X_5 = high$	0	1	0
s_5	0	1	0

CELRULE	*ER*	*IR*	*SR*
A_1	0	1	1
A_2	0	1	1
A_3	0	1	1
A_4	0	1	1
A_5	0	1	1

Figure 5. Boolean partitions modeling S_0 and S_1

Initially, all entries in cells in the *CELFACT* layer are passive (*EF* = 0), except for those who represent the initial basis of facts (EF= 1). In the case of an induction decision tree, *IF* = 0 corresponds to a Fact of the type node (*si*), *IF*=1 corresponds to a Fact of the type attribute = *value* (X_1=*medium*, for example).

In figure 6 are, respectively, represented the impact of input matrices R_E and exit R_S the Boolean model.



R_E	A_1	A_2	A_3	A_4	A_5
s_0	1	1	1		
$X_1 = medium$					
s_1				1	1
$X_1 = low$					
s_2					
$X_1 = high$					
s_3					
$X_5 = medium$					
s_4					
$X_5 = high$					
s_5					

R_S	A_1	A_2	A_3	A_4	A_5
s_0					
$X_1 = medium$	1				
s_1	1				
$X_1 = low$		1			
s_2		1			
$X_1 = high$			1		
s_3			1		
$X_5 = medium$				1	
s_4				1	
$X_5 = high$					1
s_5					1

Figure 6. Input/Output incidences matrices

The relationship entry, denoted $iR_E\,j$, is formulated as follows [28][30]:

$\forall i$={1,...,l}, ∀j={1,...,r}, if (the fact $i \in$ to the premise of the rule j) then $R_E\,(i,j) \leftarrow 1$.

The relationship of output, denoted $i\ R_S j$, is formulated as follows:

$\forall i$={1,...,l}, ∀j={1,...,r}, if (the fact $i \in$ to the conclusion of the rule j) then $R_S\,(i,j) \leftarrow 1$.

Incidence matrices R_E and R_S represent the relationship input/output of the facts and are used in forward-chaining [23] [28]. You can also use R_S as relationship of input and R_E as relationship of output to run a rear chaining inference. Note that no cell in the vicinity of a cell that belongs to CELFACT (at CELRULE) does not belong to the layer CELFACT (at CELRULE).

The dynamics of the cellular automaton CASI [28][30], to simulate the operation of an Inference engine uses two functions of transitions δ_{fact} and δ_{rule}, where δ_{fact} corresponds to the phase of assessment, selection and filtering, and δ_{rule} corresponds to the execution phase [15] [28]. To set the two functions of transition we will adopt the following notation: *EF*, *IF* and *SF* to designate CELFACT: *E*, *I* and *S*; Respectively *ER*, *IR* and *SR* to designate CELRULE: *E*, *I* and *S*.
The transition function δ_{fact}:

$$(EF, IF, SF, ER, IR, SR) \xrightarrow{\delta_{fact}} \left(EF, IF, \boldsymbol{EF}, \boldsymbol{ER} + \left(\boldsymbol{R_E^T} \cdot \boldsymbol{EF}\right), IR, SR\right)$$

The transition function δ_{rule} :

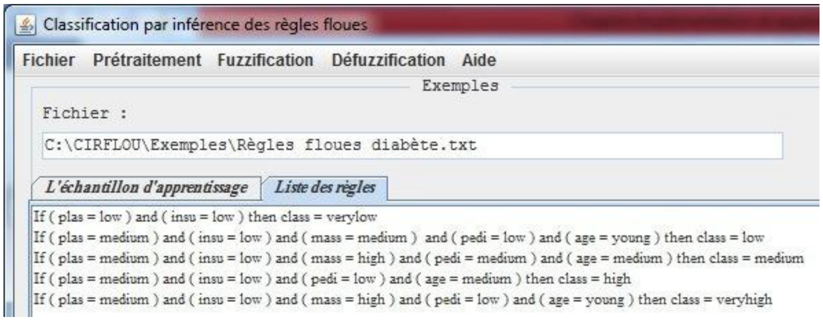
$$(EF, IF, SF, ER, IR, SR) \xrightarrow{\delta_{rule}} (\boldsymbol{EF} + (\boldsymbol{R_S} \cdot \boldsymbol{ER}), IF, SF, ER, IR, \overline{\boldsymbol{ER}})$$

In order to illustrate decision tree optimization and rules generation by the cellular method using BOG, Figure 4 shows some possible useless splitting cases. The majority class is associated with each terminal node in the decision tree. We obtain as many rules as there are terminal nodes and, in each rule, as many conjunctions as there are branches back to the root.

In knowledge discovery from database, the rules are generated from a training sample and have a double objective of characterizing the classes of concepts, and assigning a class to an example whose class is unknown. In the production rules which we wish to generate, the condition is a conjunction of elementary propositions made of an attribute, an operator (=, ≥, ≠, ...) and an attribute value. The conclusion consists of a particular proposition where the attribute relates to the class (for example diabetic or not). It is possible to associate with each rule a coefficient which defines the certainty, or probability, with which a class is predicted. After data exploration, the cellular automaton assists the Fuzzy ID3 method to generate a decision tree. This graph is represented using only R_E because, for such a type of graph, the output matrix R_S is elementary and does not even require an internal representation.

Boolean Inference Engine (BIE) : To automatically generate conjunctive rules we use same δ_{fact} and δ_{rule} transition functions with the permutation of input matrices R_E and exit R_S. We suppose that all the facts of the form X_1=*value* are established (EF=1). Going from the terminal nodes back to the root, s_0, and launching the cellular inference engine (BIE) in back chaining with a depth asynchronous mode imposed by the form of R_S. At the end of the symbolic training by the Fuzzy ID3 method (Fispro), we can generate the fuzzy rules coming from the fuzzy decision tree. Let us consider the figure 7 as if it was a final rules base. At that point, we can deduce five prediction rules R_1, R_2, R_3, R_4 and R_5 that have the form if condition then conclusion, where condition is a logical expression in conjunctive form and conclusion is the majority class in the node reached by the condition. For example, in figure 4, the majority class of s_2 is *very low* (class 1), but the majority class of s_3 is *very high* (class 5).

Generation of Conjunctive Rules : We proceed in the same way with the decision tree generated by Fispro and we obtain the following conjunctive rules (Figure 7):

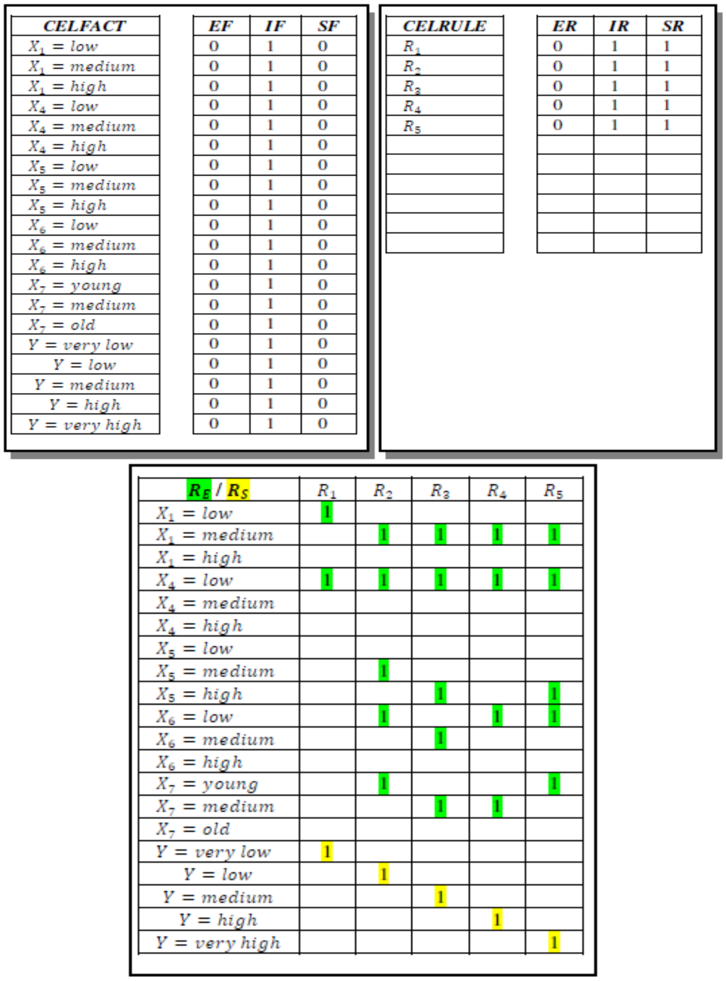


Fichier : C:\CIRFLOU\Exemples\Règles floues diabète.txt

If (plas = low) and (insu = low) then class = verylow
If (plas = medium) and (insu = low) and (mass = medium) and (pedi = low) and (age = young) then class = low
If (plas = medium) and (insu = low) and (mass = high) and (pedi = medium) and (age = medium) then class = medium
If (plas = medium) and (insu = low) and (pedi = low) and (age = medium) then class = high
If (plas = medium) and (insu = low) and (mass = high) and (pedi = low) and (age = young) then class = veryhigh

Figure 7. Generation of conjunctive rules

The representation of this knowledge base by the cellular machine is illustrated in figure 8.



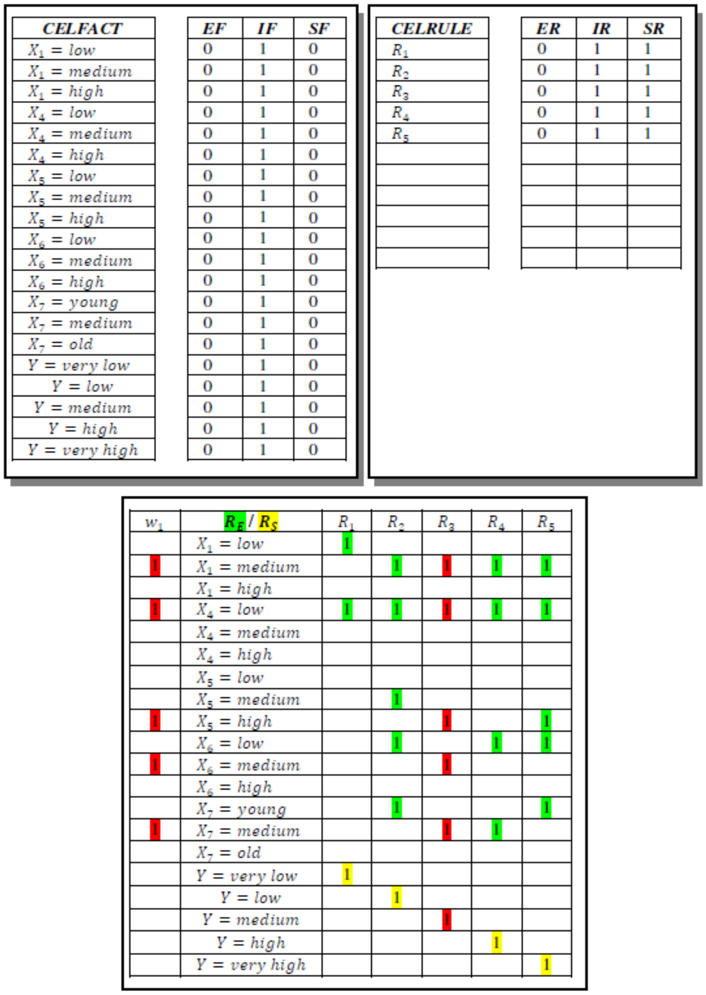
CELFACT	EF	IF	SF
$X_1 = low$	0	1	0
$X_1 = medium$	0	1	0
$X_1 = high$	0	1	0
$X_4 = low$	0	1	0
$X_4 = medium$	0	1	0
$X_4 = high$	0	1	0
$X_5 = low$	0	1	0
$X_5 = medium$	0	1	0
$X_5 = high$	0	1	0
$X_6 = low$	0	1	0
$X_6 = medium$	0	1	0
$X_6 = high$	0	1	0
$X_7 = young$	0	1	0
$X_7 = medium$	0	1	0
$X_7 = old$	0	1	0
$Y = very\ low$	0	1	0
$Y = low$	0	1	0
$Y = medium$	0	1	0
$Y = high$	0	1	0
$Y = very\ high$	0	1	0

CELRULE	ER	IR	SR
R_1	0	1	1
R_2	0	1	1
R_3	0	1	1
R_4	0	1	1
R_5	0	1	1

R_E / R_S	R_1	R_2	R_3	R_4	R_5
$X_1 = low$	1				
$X_1 = medium$		1	1	1	1
$X_1 = high$					
$X_4 = low$	1	1	1	1	1
$X_4 = medium$					
$X_4 = high$					
$X_5 = low$					
$X_5 = medium$		1			
$X_5 = high$			1		1
$X_6 = low$		1		1	1
$X_6 = medium$			1		
$X_6 = high$					
$X_7 = young$		1			1
$X_7 = medium$			1	1	
$X_7 = old$					
$Y = very\ low$	1				
$Y = low$		1			
$Y = medium$			1		
$Y = high$				1	
$Y = very\ high$					1

Figure 8. Boolean knowledge base of the figure 7

Boolean Validation (BV) : Upon completion of this process, the cellular machine is ready to launch the validation phase. By using the same guiding principle of an inference engine and the same δ_{fact} and δ_{rule} transition functions (figure 9), the cellular automaton advances from a configuration to the next, for finally generating the set Ωe [3].



CELFACT	EF	IF	SF
X_1 = *low*	0	1	0
X_1 = *medium*	0	1	0
X_1 = *high*	0	1	0
X_4 = *low*	0	1	0
X_4 = *medium*	0	1	0
X_4 = *high*	0	1	0
X_5 = *low*	0	1	0
X_5 = *medium*	0	1	0
X_5 = *high*	0	1	0
X_6 = *low*	0	1	0
X_6 = *medium*	0	1	0
X_6 = *high*	0	1	0
X_7 = *young*	0	1	0
X_7 = *medium*	0	1	0
X_7 = *old*	0	1	0
Y = *very low*	0	1	0
Y = *low*	0	1	0
Y = *medium*	0	1	0
Y = *high*	0	1	0
Y = *very high*	0	1	0

CELRULE	ER	IR	SR
R_1	0	1	1
R_2	0	1	1
R_3	0	1	1
R_4	0	1	1
R_5	0	1	1

w_1	R_E / R_S	R_1	R_2	R_3	R_4	R_5
	X_1 = *low*	1				
1	X_1 = *medium*		1	1	1	1
	X_1 = *high*					
1	X_4 = *low*	1	1	1	1	1
	X_4 = *medium*					
	X_4 = *high*					
	X_5 = *low*					
	X_5 = *medium*		1			
1	X_5 = *high*			1		1
	X_6 = *low*		1		1	1
1	X_6 = *medium*			1		
	X_6 = *high*					
	X_7 = *young*		1			1
1	X_7 = *medium*			1	1	
	X_7 = *old*					
	Y = *very low*	1				
	Y = *low*		1			
	Y = *medium*			1		
	Y = *high*				1	
	Y = *very high*					1

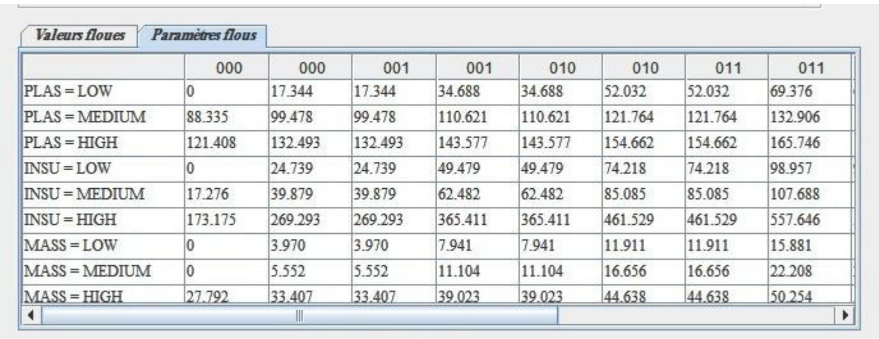
Figure 9. Boolean validation

3.3. FUZZY BOOLEAN MODELING

According to [5], founder of fuzzy logic, the limits of the classical theories applied in artificial intelligence come because they require and manipulate only accurate information. Fuzzy logic provides approximate reasoning modes rather than accurate. It is mainly the mode of reasoning used in most cases in humans.

3.3.1. BOOLEAN FUZZIFICATION OF EXOGENOUS VARIABLES

Fuzzy-BML modelling deals with the fuzzy input variables and provides results on output variables themselves blurred. Fuzzification, illustrated by the following example, is the step that consists of fuzzy quantification of actual values of a language variable. Fuzzifier to: the universe of discourse, i.e. a range of possible variations of the corresponding entry. A partition interval fuzzy from this universe, for the identification of the cost we partitioned space of variables to 7 with a Boolean modeling on 3 bits of 000 to 110 (Figure 10), finally, the duties of membership classes.



	000	000	001	001	010	010	011	011
PLAS = LOW	0	17.344	17.344	34.688	34.688	52.032	52.032	69.376
PLAS = MEDIUM	88.335	99.478	99.478	110.621	110.621	121.764	121.764	132.906
PLAS = HIGH	121.408	132.493	132.493	143.577	143.577	154.662	154.662	165.746
INSU = LOW	0	24.739	24.739	49.479	49.479	74.218	74.218	98.957
INSU = MEDIUM	17.276	39.879	39.879	62.482	62.482	85.085	85.085	107.688
INSU = HIGH	173.175	269.293	269.293	365.411	365.411	461.529	461.529	557.646
MASS = LOW	0	3.970	3.970	7.941	7.941	11.911	11.911	15.881
MASS = MEDIUM	0	5.552	5.552	11.104	11.104	16.656	16.656	22.208
MASS = HIGH	27.792	33.407	33.407	39.023	39.023	44.638	44.638	50.254

Figure 10. Boolean modeling of the fuzzy triangular numbers.

3.3.2. BOOLEAN DEFUZZIFICATION

Output the Fuzzy-BML modeling cannot communicate to the user of the fuzzy values. The role of the defuzzification is therefore to provide accurate values.

During this step, the system will perform tests to define the range of proven goal. This test will depend on the number of rules candidates and the de facto number of each rule that participated in the inference according to the following principle illustrated by figure 11 :

- Cases for a single rule and a single fact:
  if (*fact*) then (*conclusion*).
  $CELFACT_{IF}(conclusion) = Minimum(CELFACT_{IF}(fact), CELRULE_{IR}(rule))$

- Cases for a single rule with several facts:
  if ($fact_1$) and ($fact_2$) and ($fact_3$) ... then (*conclusion*).
  $CELFACT_{IF}(conclusion) = Minimum(CELFACT_{IF}(fact_1), CELFACT_{IF}(fact_2),...)$
  The *'Minimum'* operator in Boolean logic represents the logical AND.

- Several rules :
  $CELFACT_{IF}(goal) = Maximum(CELRULE_{IR}(rule_1), CELRULE_{IR}(rule_2),...)$
  The *'Maximum'* operator in Boolean logic represents the logical OR.

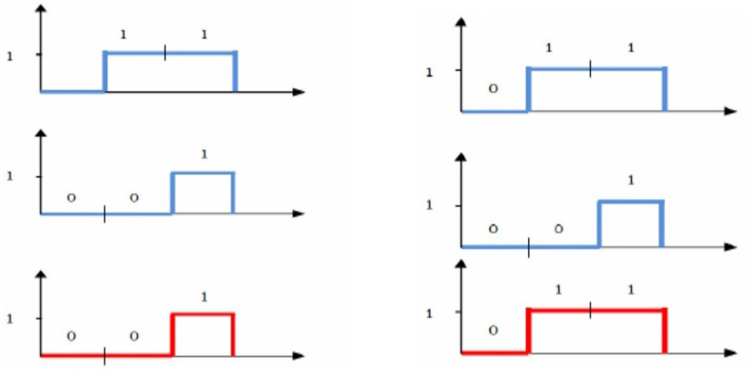


Figure 11. Boolean operator for the defuzzification

4. EXPERIMENTATION

We have evaluated our approach on a case basis of Diabetes. Diabetes is a disease in which the body does not properly process glucose or sugar. We exploited the Pima Indians Diabetes dataset of the UCI database library. This dataset consists of 768 instances characterized by 8 descriptors: During this step, the system will perform tests to define the range of proven goal. This test will depend on the number of rules candidates and the de facto number of each rule that participated in the inference according to the following principle:

X_1*: Number of times pregnant;*
X_2*: Plasma glucose concentration a 2 hours in an oral glucose tolerance test;*
X_3*: Diastolic blood pressure;*
X_4*: Triceps skin fold thickness;*
X_5*: 2-Hour serum insulin;*
X_6*: Body mass index;*
X_7*: Diabetes pedigree function;*
X_8*: Age.*

We compare the proposed approach Fuzzy-BML with k-NN [31] and decision tree on the same case base. We show in Table 4 the rate of correctly classified instances with each method using the supervised mode of discretization.

Table 4. Results of experimentation.

k-NN	Decision tree	Fispro Fuzzy-DT [13]	Fuzzy-BML
66%	73%	81%	81%

The rate of correctly classified instances is 66% with k-NN, 73% with decision tree, 81% with Fuzzy-DT and Fuzzy-BML-CBR. From the obtained results, we note that the Fuzzy-BML-CBR method has provided better results with a rate of 81% of well classified instances. In this paper Fuzzy BML approach has been applied to optimize response time and the storage complexity.

5. CONCLUSIONS AND PERSPECTIVES

Several competing motivations have led us to define a Boolean model for CBR knowledge base systems. Indeed, we have not only desired experiment with a new approach to indexing of cases by decision tree, but we also wanted to improve modeling of the vague and uncertain of the natural language concepts, optimize response time and the storage complexity.

For the calculation of the similarity in the retrieval (cases indexing) phase, typically used k-nearest neighbours. So we compared our Fuzzy Boolean Model with k-nearest neighbours (k-NN) and decision tree. We noticed that the indexing of cases for the choice of a plan is significantly better with Fuzzy-BML. Finally, we can say that the structure of the cases that we have used is quite simple. We have described the part problem of cases by age, weight and an antecedent. By adding other constraints could subsequently used a slightly more complex representation.

As a future perspective of this work, we propose to improve the other steps of the CBR process for the proposed approach.

REFERENCES

[1] Breiman, L., Friedman, J.H., Olshen, R.A. & Stone, C.J. (1984) ‘Classification and regression and trees’, Technical report, Wadsworth International, Monterey, CA.

[2] Kodratoff, Y. (1997) ‘The extraction of knowledge from data, a new topic for the scientific research’, Magazine electronic READ.

[3] Atmani, B. & Beldjilali, B. (2007) ‘Neuro-IG: A Hybrid System for Selection and Elimination of Predictor Variables and non Relevant Individuals’, Informatica, Vol. 18, No. 2, pp163-186.

[4] Fayyad, U., Shapiro, G.P. & Smyth, P. (1996) ‘The KDD process for extraction useful knowledge from volumes data’, Communication of the ACM.

[5] Zadeh, L.A. (1997) ‘Some reflections on the relationship between AI and fuzzy logic: A heretical view’, Workshop on Fuzzy Logic in Artificial Intelligence, pp1-8.

[6] Zadeh, L.A. (1968) ‘Probability measures of fuzzy events’, Journal of Mathematical Analysis and Applications, Vol. 23, pp421-427.

[7] Zighed, D.A. & Rakotomalala, R. (2000) Graphs of induction, Training and Data Mining, Hermes Science Publication, pp21-23.

[8] Boyen, X. & Wehenkel, L. (1999) ‘Automatic induction of fuzzy decision trees and its application to power system security assessment’, Fuzzy Sets and Systems, Vol. 102, pp3-19.

[9] Begum, S., Ahmed, M.U., Funk, P., Xiong, N. &Von Schéele, B. (2009) ‘A case-based decision support system for individual stress diagnosis using fuzzy similarity matching’, Computational Intelligence, Vol. 25, pp180-195.

[10] Barrientos, F. & Sainz, G. (2012) ‘Interpretable knowledge extraction from emergency call data based on fuzzy unsupervised decision tree’, Knowledge-Based Systems, Vol. 25, pp77-87.

[11] Levashenko, V. & Zaitseva, E. (2012) ‘Fuzzy decision trees in medical decision making support system’, Proceedings of the Federated Conference on Computer Science and Information Systems, pp213-219.

[12] Adidela, D.R., Devi, L., Suma, J. & Allam, A.R. (2012) ‘Application of fuzzy Id3 to predict diabetes’, International Journal of Advanced Computer and Mathematical Sciences, Vol. 3, No. 4, pp541-545.

[13] Benamina, M., Atmani, B., & Benbelkacem, S. (2018) ‘Diabetes Diagnosis by Case-Based Reasoning and Fuzzy Logic’. International Journal of Interactive Multimedia and Artificial Intelligence, (In Press).

[14] Amrani, F., Bouamrane, K., Atmani, B., & Hamdadou, D. (2011). Une nouvelle approche pour la régulation et la reconfiguration spatiale d’un réseau de transport urbain collectif. Journal of decision systems, 20(2), 207-239.

[15] Barigou, F., Atmani, B. & Beldjilali, B. (2012) ‘Using a cellular automaton to extract medical information from clinical reports’, Journal of Information Processing Systems, Vol. 8, No. 1, pp67-84.

[16] Atmani, B., Benbelkacem, S. & Benamina, M. (2013) ‘Planning by case-based reasoning based on fuzzy logic’, First International Conference on Computational Science and Engineering, Dubai, UAE, pp53-64.

[17] Brahami, M., Atmani, B. & Matta, N. (2013) ‘Using rules to enhance evolution of knowledge mapping: Application on Healthcare’, International Journal of Computer Science Issues, Vol. 10, No. 3, pp261-270.

[18] Benfriha, H., Barigou, F. & Atmani, B. (2013) ‘Lattice-cell: Hybrid approach for text categorization’, Second International Conference on Software Engineering and Applications, Dubai, UAE.

[19] Aissani, N., Atmani, B., Trentesaux, D. & Beldjilali, B. (2014) 'Extraction of priority rules for boolean induction in distributed manufacturing control', In Borangiu, T, Trentesaux, D. and Thomas, A. (Ed.), 'Service orientation in holonic and multi-agent manufacturing and robotics', Studies in computational intelligence, Vol. 544, Springer, pp127-144.

[20] Guillaume, S. & Charnomoridc B. (2011) 'Learning interpretable fuzzy inference systems with FisPro', Information Sciences, Elsevier, Vol. 181, No. 20, pp4409-4427.

[21] Bello-Tomas, J., Gonzalez-Calero, P. & Diaz-Agudo, B. (2004) 'Jcolibri: An object oriented framework for building CBR systems', Advances in Case-Based Reasoning, 7th European Conference on Case-Based Reasoning, pp32–46.

[22] Kalpana, M. & Kumar A. (2011) 'Fuzzy expert system for diabetes using fuzzy verdict mechanism', International Journal of Advanced Networking and Applications, Vol. 3, No. 2, pp1128-1134.

[23] Beldjilali, A. & Atmani, B. (2009) 'Identification du type de diabète par une approche cellulo-floue', Quatrième atelier sur les systèmes décisionnels, Jijel, Algeria, pp203-218.

[24] Quinlan, J.R. (1986) 'Induction of decision trees', Machine Learning, Vol. 1, pp81-106.

[25] Weber, R. (1992) 'Fuzzy-Id3: A class of methods for automatic knowledge acquisition', 2nd International conference on fuzzy logic and neural networks, pp265-268.

[26] Alonso, J.M., Cordon, O., Quirin, A. & Magdalena, L. (2011) 'Analyzing interpretability of fuzzy rule-based systems by means of fuzzy inference-grams', World Conference on Soft Computing, San Francisco, USA.

[27] Zulj, S., Seketa, G., Dzaja, D., Sklebar, F., Drobnjak, S., Celic, L. & Magjarevic R. (2017) 'Supporting diabetic patients with a remote patient monitoring systems', In: Torres I., Bustamante J. and Sierra D. (Ed.) VII Latin American Congress on Biomedical Engineering CLAIB 2016, Bucaramanga, Santander, Colombia, October 26th -28th, 2016, IFMBE Proceedings, Vol. 60, Springer, Singapore.

[28] Atmani, B. & Beldjilali, B. (2007) 'Knowledge discovery in database: Induction graph and cellular automaton', Computing and Informatics Journal, Vol. 26, No. 2, pp171-197.

[29] Benamina, M. & Atmani, B. (2008) 'WCSS: un système cellulaire d'extraction et de gestion des connaissances', Troisième atelier sur les systèmes décisionnels, Mohammadia, Morocco, pp223-234.

[30] Brahami, M., Atmani, B. & Matta, N. (2013) 'Dynamic knowledge mapping guided by data mining: Application on healthcare', Journal of Information Processing Systems, Vol. 9, No. 1, pp01-30.

[31] Guo, G., Wang, H., Bell, D., Bi, Y. & Greer, K. (2003) 'Knn model-based approach in classification', International Conference on Ontologies, Databases and Applications of Semantics, pp986– 996.

AUTHORS

Mohamed Benamina is currently a PhD candidat at the University of Oran 1 Ahmed Ben Bella and affiliated researcher in Laboratoire d'Informatique d'Oran, Algeria. He received his Master degree in Computer Science in 2010 from University of Oran, Algeria. His research interests include data mining algorithms, expert systems and decision support systems.

Baghdad Atmani received his PhD in computer science from the University of Oran (Algeria) in 2007. He is currently a full professor in computer sciences. His interest field is artificial intelligence and machine learning. His research is based on knowledge representation, knowledge-based systems, CBR, data mining, expert systems, decision support systems and fuzzy logic. His research are guided and evaluated through various applications in the field of control systems, scheduling, production, maintenance, information retrieval, simulation, data integration and spatial data mining.

Sofia Benbelkacem is currently a PhD candidate at the University of Oran 1 Ahmed Ben Bella and affiliated researcher in Laboratoire d’Informatique d’Oran, Algeria. Her research interests include data mining, planning, case-based reasoning, medical decision support systems, machine learning.

VIRTUAL AIS GENERATION MANAGEMENT SYSTEM FOR WATERWAY RISK ASSESSMENT

Jun Sik Kim[1], Seung Wook Hong[2] and Suhyun Park[3]

[1]Division of Computer Engineering, Dongseo University, Busan, Korea
[2]ONE Data Technology, Sasang-gu, Busan, Korea
[3]Division of Computer Engineering, Dongseo University, Busan, Korea

ABSTRACT

The virtual Automatic Identification System (AIS) generation management system is a system for analysing waterway risk by generating virtual AIS data which contains location information of a specific area. The system uses the data as an input data of the IALA Waterway Risk Assessment (IWRAP).

KEYWORDS

AIS, Shipwreck, waterway risk assessment

1. INTRODUCTION

The virtual AIS generation management system for waterway risk assessment generates the virtual AIS data which is input data of the program for analyzing risks (running aground, a head-on collision) that may occur during navigation of a ship. The generated virtual AIS data includes the position information, and it is possible to assessment the risk at a desired position in the sea. Increasing the number of vessels and expanding the size of vessels may cause the elevation of vessel accidents and because of this human and property damage are becoming serious. Moreover, due to lack of interest in safety consciousness of ship workers (non-compliance with navigation, improper operation of equipment, etc.), the marine safety tribunal ruled out 199 cases (85% of 233 cases).

Despite the development of marine technology, marine accidents tend to continue to increase around the world. So, we are making efforts to prevent marine accidents by using various technologies throughout the world. Among them, we are developing a system that uses AIS (Automatic Identification System) data to confirm the situation at the time of the accident. The AIS data can be used to know the type of ship and where the accident occurred, including location information, using the ship's information (ship's size, ship's speed, ship's unique number, MMSI (Maritime Mobile Service Identity) number). Therefore, AIS data can be used to find the place where many ship accidents occur considering the volume and time of shipment, and it can be used to calculate the risk of the shore.

AIS data can be generated by virtually creating data that is based on data assuming accidents that may occur in the territorial waters and enhancing the safety consciousness of the workers. When pioneering a new port waterway, you can create virtual AIS data and perform various simulations of the accident. It can

Dhinaharan Nagamalai et al. (Eds) : CSEIT, NCS, SPM, NeTCoM - 2018
pp. 45–51, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81804

predict and prevent marine accidents that may occur in advance. It also uses virtual AIS data in places where it is difficult for the vessel to collect data on a path that does not travel frequently. And if you do not have frequent voyages but want to analyze the risk in your area, you need virtual AIS data generation module.

Virtual AIS can be used as basic data for creating a Korean risk assessment system when the virtual AIS data generation module and the basis data of the risk assessment due to the occurrence of the actual marine accident are provided. The AIS data, which can be used as the basis for prevention of marine accidents, helps to analyse the factors that threaten accidents in the ocean. The virtual AIS data generating management system can collect accident data which is likely to occur in the ocean by virtually creating AIS data used as input data to analyse the waterway risk. The virtual AIS generation management system for waterway risk assessment can analyse the risk beforehand through the virtual AIS data in the case of pioneering a new waterway and to find the location of the new waterway in a high risk area and it can be the foundation of activity.

2. RELATED RESEARCH

2.1. RELATED RESEARCH AIS

The Automatic Identification System (AIS) is a system adopted by the International Maritime Organization and provides information on ship operations to prevent marine accidents by using two-way data communication between ship-ship, ship-ship and land. The domestic ship automatic identification system is operated in 41 base stations and 13 operating stations. The base station receives the dynamic information, the static information, and the navigation information, which is transmitted from the ship, and transmits the received information to the operating station.

AIS is diverse in equipment depending on the size of the ship, it transmits information every 6 minutes for static information, and time for transmission according to the speed of the ship in case of dynamic information.[2] There are Class A and Class B marine AIS types and SOTDMA (Self-Organized Time Division Multiple Access) methods.[3] SOTDMA is a time division multiple access communication schemes for efficient use of limited communication technologies in the ocean. The operator is able to ask each ship, AtoN, to send information[4].

AIS data consists of 27 message types in total. There are security processing messages, location report messages, control messages, and so on. Virtual AIS data messages that can be used in IWRAP should include location information. The location report of the vessel should be classified into Class A equipment and Class B equipment, and Class A equipment must be installed in the international vessel (300tons or more). Class A equipment location reporting message ID is 1, 2 and 3 and the Class B equipment location reporting message ID is 18. In order to generate a virtual message including the ship information and the location information, the message ID 1, 2, 3 and 18 are generated. The location of the ship can be changed through the virtual AIS message and the virtual AtoN can be installed in the dangerous area by generating the message ID 21 as the virtual AIS message.

2.2. RISK ASSESSMENT PROGRAM IWRAP

The IALA Waterway Risk Assessment Program (IWRAP) is a model to analyze waterway risks (ship collision, stranding, etc.)[4]. The International Association of Lighthouse Authorities (IALA) was established in July 1957 to provide ship safety and navigation assistance. The IWRAP program can analyse risks such as head-on collision, cross-over collision, stranding and uses decoded AIS data. The IWRAP program shows the probability which the ship collision and stranding frequency information will occur annually[5].

The Virtual AIS generation management system for waterway risk assessment is make virtual AIS data. In IWRAP program MK2 is quantitative evaluation model. The MK2 program can be used to quantitatively assess the risk and analyse the risk of a desired area using virtual AIS data. By creating virtual AIS data in areas where area capable of causing marine accidents, marine accidents can be predicted and prevented in advance[6].

3. VIRTUAL AIS GENERATION SYSTEM

The virtual AIS generation management system flow for the waterway risk assessment determines the position where the risk analysis is required or assumes the accident, and inputs the information for generating the virtual AIS data information at the corresponding position to generate the virtual AIS. The generated virtual AIS data is input data of the IWRAP program, which is an accident risk analysis program, and analyses the risk of the corresponding location through the location information in the AIS data. In case of high-risk areas, install the virtual AtoN to display the risk and terminate the analysis. If the risk is low, analyse the location of the surrounding area or other area and record the results. The figure1 below is the flow chart of this system.

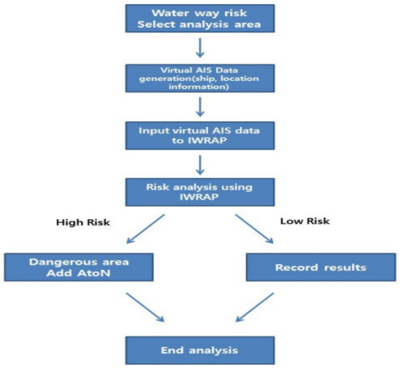

Water way risk
Select analysis area
Virtual AIS Data generation(ship, location information)
Input virtual AIS data to IWRAP
Risk analysis using IWRAP
High Risk
Low Risk
Dangerous area
Add AtoN
Record results
End analysis

Figure 1. Virtual AIS flow chart.

The Figure 1 to show the flow chart, If you want to analyse the risk in a particular area. First generate some virtual AIS using Virtual AIS generation management System. First, input the ship information (ship type, ship name, MMSI number, latitude longitude). And save AIS data (it is created as a text document). You can input this data to IWRAP program. IWRAP program can check ship traffic. You can analyse the risks based on that.

3.1. VIRTUAL AIS GENERATION

The system configuration consists of loading and saving text files through the Files menu, Main, Class A, Class B, AtoN, and Total AIS tabs. The file retrieval function can retrieve a text file, including a separator, a field name, and a space elimination function, and can fetch only a desired portion of various types of text documents by designating a message field sequence number. The import part of the table can be checked in advance before importing the file. Message field specified by the sequence number, it can be confirmed on the Main tab when Open button is pressed. The Main tab identifies the AIS Message Sentence and the ID of the message, and indicates whether the Time Stamp is used or not. When the desired message is clicked, detailed information decoded from the AIS message sentence can be confirmed in the right table.

The detailed information table differs depending on the message ID. Depending on the size of the vessel, the equipment of the AIS unit is diverse. For ships equipped with Class A equipment, information on specific vessels can be collected based on the desired message ID and Maritime Mobile Service Identity (MMSI) Number in the Class A tab. The position of the vessel can be confirmed by the occurrence of the message according to the time interval, and it can be confirmed through the map. In addition, it is possible to change the marker position information on the map and convert the changed information into AIS data. The Class B tab is a ship equipped with Class B equipment that transmits message IDs 18 and 19, and the contents are the same.

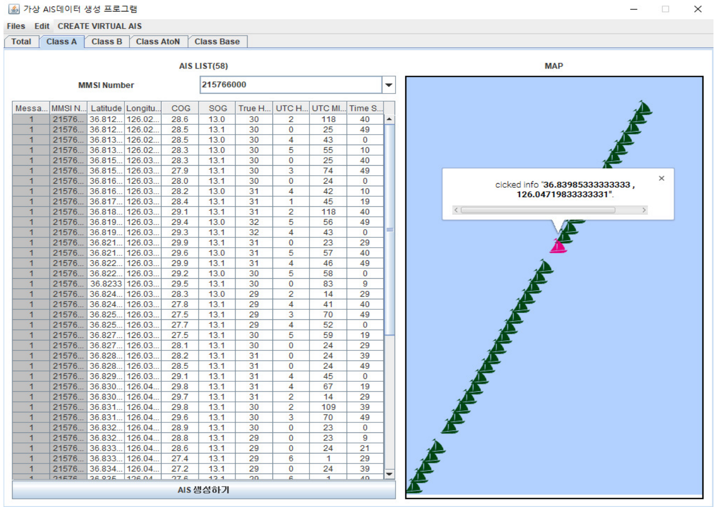
AtoN is a navigational sign that uses light, fluorescence, color, etc. to aid navigation. In the AtoN tab, AIS message ID 21 can be used. It can be displayed when the actual route marking facility is in place, but it is not actual through the Virtual AtoN flag, or in dangerous areas. You can install the AtoN in the corresponding location by checking the hazardous area measured through the Class A and Class B tabs. The installed location is indicated on the map. The Total AIS tab is a tab that allows you to see at a glance which models are culled in Class A, Class B, and AtoN.

3.2. HOW TO USE SYSTEM MODULE

The existing AIS data is composed of binary numbers that users cannot recognize. The virtual AIS generation management system can obtain desired information by decoding AIS data composed of binary numbers. The decoded information has a message ID for classifying the AIS message, an MMSI Number for knowing the information of the ship, and the location information including latitude and longitude. It can be used when you want to collect information on existing AIS data before creating a virtual module. In Class A, Class B, and AtoN tabs, you can filter the MMSI number of the vessel you want, and you can see at a glance what signals the vessel is sending. The information of the filtered MMSI Number is displayed on the map and it is easy to know where the signal is transmitted. When you want to create new virtual AIS data, you can display the marker on the map by clicking the desired position on the map.

Since the AIS data that is input data of IWRAP is encoded information, it can generate AIS data through collecting position information on the map by clicking and inputting information such as MMSI Number. By creating AIS data that can send signals to the desired location, you can create virtual AIS data that can analyze the risk through mouse clicks on the map when opening a new route or analyzing the risk in a specific area has. Class A tab can be classified based on message ID numbers 1, 2, and 3, and in the case of Class B tab, based on message IDs 18 and 19, you can easily specify the message ID number and analyze through the AtoN tab. In the case of high risk-areas, users can identify dangerous areas. In the Total AIS tab, the virtual AIS data generated from the existing Class A or Class B vessels and the AtoN information generated from the AtoN tab can be displayed on the map to easily locate the dangerous area and the desired area.

When importing existed AIS data, only necessary parts of AIS data can be filtered and recalled, and various types of character encodings can exist, and characters encoded as needed such as UTF-8 and EUC-KR can be analysed. In addition, if new virtual AIS data is generated by clicking on the map, the AIS data generated through the data storage function can be stored in a text form. You can import new AIS data via Files Button. With the AIS data information imported, you can find the detail information of the ship at total tab. On the Class A tab, the ship's location information is displayed on the map. The position information of the vessel indicated by the marker can be moved anywhere. If you moved markers, it changed location information and make new AIS data. All tabs have 'generate AIS' button on the left down side. You can input the information virtual MMSI number, message ID, SOG, Longitude, Latitude, UTC Hour, UTC Minute, Time stamp and so on. The generate AIS button creates the first new AIS data. Create new AIS data by clicking on the map, based on the generated AIS data. If you want to know the location information by vessel, it will be displayed on the map by filtering function. When you save the created data, it is provided as a text document. This text document can analyse dangerous areas with input data from the IWRAP program.



MMSI Number: 215766000

Messa...	MMSI N...	Latitude	Longitu...	COG	SOG	True H...	UTC H...	UTC MI...	Time S...
1	21576...	36.812...	126.02...	28.6	13.0	30	2	118	40
1	21576...	36.812...	126.02...	28.5	13.1	30	0	25	49
1	21576...	36.813...	126.02...	28.5	13.0	30	4	43	0
1	21576...	36.813...	126.02...	28.3	13.0	30	5	55	10
1	21576...	36.815...	126.03...	28.3	13.1	30	0	25	40
1	21576...	36.815...	126.03...	27.9	13.1	30	3	74	49
1	21576...	36.816...	126.03...	28.0	13.1	30	0	24	0
1	21576...	36.816...	126.03...	28.2	13.0	31	4	42	10
1	21576...	36.817...	126.03...	28.4	13.1	31	1	45	19
1	21576...	36.818...	126.03...	29.1	13.1	31	2	118	40
1	21576...	36.819...	126.03...	29.4	13.0	32	5	56	49
1	21576...	36.819...	126.03...	29.3	13.1	32	4	43	0
1	21576...	36.821...	126.03...	29.9	13.1	31	0	23	29
1	21576...	36.821...	126.03...	29.6	13.0	31	5	57	40
1	21576...	36.822...	126.03...	29.9	13.1	31	4	46	49
1	21576...	36.822...	126.03...	29.2	13.0	30	5	58	0
1	21576...	36.8233	126.03...	29.5	13.1	30	0	83	9
1	21576...	36.824...	126.03...	28.3	13.0	29	2	14	29
1	21576...	36.824...	126.03...	27.8	13.1	29	4	41	40
1	21576...	36.825...	126.03...	27.5	13.1	29	3	70	49
1	21576...	36.825...	126.03...	27.7	13.1	29	4	52	0
1	21576...	36.827...	126.03...	27.5	13.1	30	5	59	19
1	21576...	36.827...	126.03...	28.1	13.1	30	0	24	29
1	21576...	36.828...	126.03...	28.2	13.1	31	0	24	39
1	21576...	36.828...	126.03...	28.5	13.1	31	0	24	49
1	21576...	36.829...	126.03...	29.1	13.1	31	4	45	0
1	21576...	36.830...	126.04...	29.8	13.1	31	4	67	19
1	21576...	36.830...	126.04...	29.7	13.1	31	2	14	29
1	21576...	36.831...	126.04...	29.8	13.1	30	2	109	39
1	21576...	36.831...	126.04...	29.6	13.1	30	3	70	49
1	21576...	36.832...	126.04...	28.9	13.1	30	0	23	0
1	21576...	36.832...	126.04...	28.8	13.1	29	0	23	9
1	21576...	36.833...	126.04...	28.6	13.1	29	0	24	21
1	21576...	36.833...	126.04...	27.4	13.1	29	6	1	29
1	21576...	36.834...	126.04...	27.2	13.1	29	0	24	39

cicked info "36.83985333333333 , 126.04719833333331".

Figure 2. Input AIS data decoding & check their location

This Figure2 illustrates some information on AIS data from the map. We provide the map of AIS data location information. It can include their longitude and latitude. So we can check their location using the map. If you want make some Virtual AIS, you can create the desired region by clicking on it.

3.3. RELATIONSHIP BETWEEN VIRTUAL AIS AND IWRAP

IWRAP can measure the risk of waterways using AIS data as an input data. The Class A and Class B tabs of this system can arbitrarily modify the position and information of the ship to create AIS data and move to the desired position. It can be encoded as AIS data and used as an input data of IWRAP. So, after creating the vessel information and parking the vessel in the aimed area, the risk can be checked by measuring the risk around the radius of the located area through the IWRAP program. The system can generate the virtual AIS data which is needed to assessment the waterway risk and display the risk by virtually locating the AtoN in the dangerous area.

Through the virtual AIS data, IWRAP, which analyse the incident based on the actual ship AIS data can be analysed. When a new route is opened, there is no AIS data because there is no ship movement. Therefore, it is difficult to analyse the risk. Also, the problem can be solved by creating virtual AIS data at the corresponding position.

4. CONCLUSIONS

This system is dedicated to generate virtual AIS data in order to analyze the waterway risk. It is possible to analyze the risk at a desired location by generating virtual AIS data which can continuously send signals at the waterway location which is the movement path of the ship. AIS data is generated as input data of IWRAP which is a risk analysis program. Rather than path data, by generating virtual AIS data that includes desired location information, the risk can be measured in advance at the location. Measured data does not only indicate simple risk but also it establishes a virtual AtoN so that dangerous areas can be displayed in advance even when trying to create a new route. The virtual AIS data generated through the virtual AIS generation management system can assume the accidents that may occur in the ocean and can be used as simulation-based data for analyzing the waterway risk in advance. By creating virtual AIS data, it can play a new role in raising safety awareness of marine casualties and paving the way for new routes.

Risk assessment can be done beforehand through the IWRAP program using virtual AIS data. By measuring the risk at the desired location through the virtual AIS data, the optimal route can be virtually created. The installation of actual navigation aids requires a great deal of cost and time. Therefore, there are many difficulties in changing the route to measure the risk. By creating virtual AIS data time and money can be economized. Through creating the virtual AIS data at the desired location, it can be functioned as the base data to measure the risk in waterway. The virtual AIS data can analyse accidents that may occur on the same line as a collision accident. The AIS data also includes location data, so that it is possible to use the information that can be measured in a ship or a buoy other than an accident, so location information can be provided for observation. The currently generated AIS data is representative of Class A ships, Class B ships, and base station. It will further clarify the information generated and make it possible to collect additional information about the speed and direction of the ship, such as those generated by the actual ship. The future direction is to enable AIS messages to decode and generate a total of 27 messages.

ACKNOWLEDGEMENTS

It was funded by the ‘Ministry of Science and ICT’ and was supported by the ‘National IT Industry Promotion Agency’ (S0708-18-1021, Development of a Service Platform for Crowdsourced High Density Bathymetry). It was funded by the ‘Korea Meteorological Institute’ (AP00001992, Development of service and advance marine weather contents tailored fisheries).

REFERENCES

[1] Ministry of Maritime Affairs and Fisheries(Korea), Current status of marine accident (2013~2017).

[2] Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band ITU-R M.1371-5, February 2014, pp. 111-144.

[3] JinHo Park, (2015), Analysis Method for Maritime Accident using Automatic Identification System, Korea University, Seoul.

[4] SangHoey Lee, (2005),The SOTDMA Algorithm Development and Verification for AIS.

[5] KwangIl Kim, (2014) Analysis is of maritime traffic safety in port waterway using IWRAP.

[6] EuiJong Lee, (2018) A study on the correlation between Port waterway risk Based on IWRAP Mk2 and Marine traffic congestion.

AUTHORS

Junsik Kim received B.S. degree in computer engineering from Dongseo University, Korea, respectively. He is currently working toward the M.S Candidate degree in computer engineering at Dongseo University since March 2018. His research interest is Maritime IT research.

SeungWook Hong received B.S, M.S degree in computer engineering from Dongseo University, Korea, respectively. He is ONE Data Technology Development Team Manger. He is interest in Maritime IT convergence, Mobile application development.

Suhyun Park received PhD in department of computer science from Busan National University, Korea, respectively. She is a professor of Computer Engineering Division at Dongseo University. She is interest in Maritime IT convergence, Artificial Intelligence and Cloud Computing research.

INTENTIONAL BLANK

DATA MANAGEMENT PLATFORM SUPPORTING VOLUNTEER OCCUPATION SERVICES

Damien Nicolas, Adnan Emeri, Marie Laure Watrinet and
Djamel Khadraoui

LIST: Luxembourg Institute of Science and Technology
Maison de l'innovation - 5, Avenue des
Hauts-Fourneaux L-4362 Esch-sur-Alzettebourg

ABSTRACT

This paper deals with the Data Management Services, which acts as a link between the User Requirements, the System Requirements and the development of the core IT software components supporting the occupation services performed during the Sponsor project. This gives an overview of the main services provided by the platform, the chosen architecture model including the relationships between the different conceptual models and the data models implemented within the platform. As a result, the outcomes of this deliverable will constitute an input for the development of the platform as a services-oriented platform providing and publishing a complete API for managing organizations, opportunities and volunteers.

KEYWORDS

Data Model, SOA, RESTful Web Services, IT service platform, Ambient Assisted Living, Graph Database, Volunteering Services.

1. INTRODUCTION

This paper presents the different services provided by the Sponsor platform. It details the high-level key systems components and also the data model associated.

The Sponsor architecture design aspires to be scalable, flexible and open. To achieve this goal, it follows the principle of Service-Oriented Architecture (SOA) design. Thus, the system is component-based and provides some flexibility in deployment.

The structure of this paper is the following: the first section presents briefly the overall architecture of the platform and its data model associated; then the second section describes the core services providing support to the targeted entities: organizations and volunteers. Finally, the third section gives the description of common services such as registration, search or communication services.

Dhinaharan Nagamalai et al. (Eds) : CSEIT, NCS, SPM, NeTCoM - 2018
pp. 53–67, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81805

2. ARCHITECTURE AND DATA MODEL

The architecture of the Sponsor platform is based on the SOA approach, facilitating the flexibility, scalability and openness properties of the platform

A. SOA APPROACH OVERVIEW

The Sponsor platform shall satisfy the targeted requirements by interconnecting different internal components or external systems. Therefore, the most suitable architectural design seems to be a Service-Oriented Architecture (SOA) design that is a modular and open design. The Sponsor architecture is designed and implemented on basis of these principles where SOA is considered as an evolution of any distributed computing, putting the focus on the modularity and the interconnection of the systems from a Service point of view.

Further underlying and enabling ingredient is given by the metadata which are sufficient to describe not only the characteristics of these services, but also the data that implement them. XML has been used extensively in SOA to create data which are wrapped in a nearly exhaustive description container. Analogously, the services themselves are typically programmed in WSDL (Web Services Description Language), and communication protocols in SOAP, that is a protocol for exchanging XML-based messages over computer networks, by using normally HTTP/HTTPS. In the scope of the project, a different approach is adopted for specifying the communication format and the communications protocol:

- For the communication between the front-end and the back-end, the JSON language was selected, which is less verbose than XML and hence well adapted to other languages for the communication between two systems;
- For the communications protocol, a RESTful approach was chosen because of its simplicity (regarding the SOAP protocol) and the way it manages the access of resources through the HTTP/S operations such as GET, POST, DELETE or PATCH

Sponsor architecture is based on services on top of centralized system called here as a back-end, and on events that will be the main way of communication between the components.

The rationale behind the choice of a SOA design are motivated by the following:

- The ability to reuse developed components, to enable sharing modules between applications and inter application changes;
- The flexibility of enriching the Sponsor system with new components to satisfy possible new business needs;
- The openness and interoperability by design, in order to share components between platforms and environments
- The distribution enabled by the ability to deploy remotely some components and/or an associated data storage;
- Scalability by design

B. LAYERS DESCRIPTION

A system architecture is generally organized in different layers, also known as the n-tiers architecture pattern [1], a fact that enables a logical cut of the targeted architecture with specific responsibilities assigned to every layer. Each layer can be also split into sub-layers if needed. This approach offers the main advantage of facilitating on the one hand the conception and the development of the platform, whereas on the other hand it ensures a better maintainability of the system in the future. The following schema (Figure 1) provides an overview of the layers of the SpONSOR architecture.

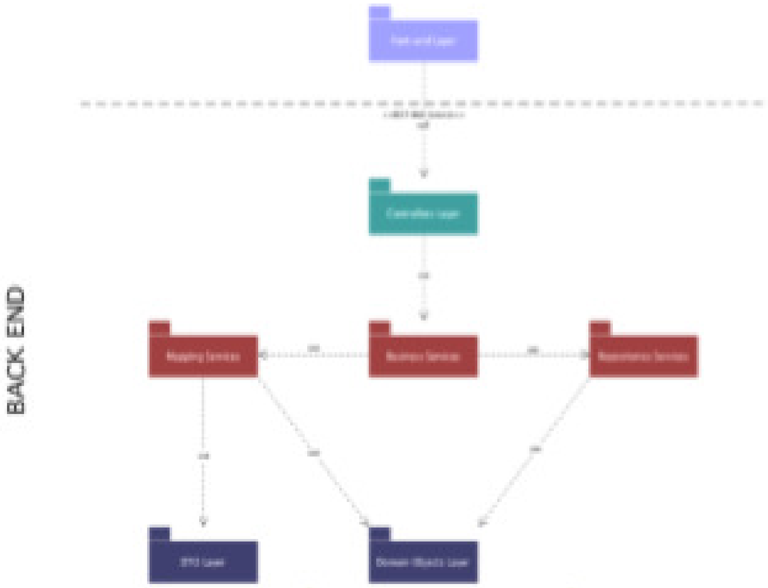


Figure 1: Architecture Layers Overview.

Each layer has a specific rationale and purpose:

- Front-end layer: this layer contains all the graphical user interface elements, such as web pages (written using the dedicated format HTML5), web-oriented languages such as Javascript, styles rules with CSS3, and some logic related to the navigation of the user and the display of the data..

- Controllers Layer: this layer contains the interfaces (endpoints) provided by the SpONSOR backend. This is the main and only entry point for accessing provided services. These entry points supports RESTful web services and uses the JSON format as the format for input and output communications between the front-end and the back-end.

- Business Services: this layer handles the business services of the SpONSOR platform. Each business service is grouped in a dedicated package, in order to facilitate the maintainability of the platform. This layer is the only layer used by the Controllers one, which enables in turn

- Mapping Services: this layer performs the mapping between the objects of the Domain layer and the objects of the Data Transfer Objects (DTO) layer. In order to ensure the encapsulation and the handling of possible changes for the services at a minimized cost, objects of the Domain are not directly exposed to the interfaces. Only the DTO layer is visible and used from the front-end layer.

- Repository Services: this layer manages the storage and the retrieval of the data from and to the database, used by the platform. This layer is based on ACID [2] transactions. This layer can also be replaced by another one if the database system should be changed, without any additional costs,

- Data Transfer Object Layer: this layer follows the well-known DTO pattern [3] to hide the real objects manipulated by the platform. A DTO is an object that aggregates some data from the data layer domain, in order to present meaningful objects to the requester, and to minimize the network connections between the requester and the provider

- Domain Objects Layer: this layer contains the core data model manipulated by the SpONSOR platform. By design, this layer has no dependencies with the other layers

The Figure 1 provides also the interactions, and therefore the dependencies, between the layers of the architecture.

C. DATA MODEL OVERVIEW

This section gives a description of the data model used by the platform. From a bird-view perspective, three concepts are mandatory for the SpONSOR platform:

- Organization;
- Volunteer;
- Opportunity

An organization is an entity comprising multiple people, such as an institution or an association, which has a collective objective and is linked to an external environment. In our case, an organization is senior-supportive and must be involved in the well-being of the senior persons with a clear mission of supporting activities of seniors

A volunteer is a person who wishes to provide services, while renouncing to any financial gain, to benefit of another person, group or association. In our case, a volunteer can be anyone who is registered, as a such, in the platform.

An opportunity is defined as a time when a particular situation makes it possible to do or achieve something. In our case, an opportunity is a task (recurrent or not) provided by an organization, that requires one or more volunteers to be achieved.

The core relations between these three concepts are the following:

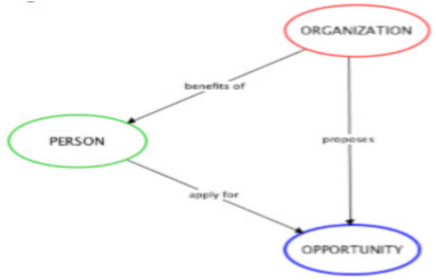


Figure 2: Core Concepts model.

An organization proposes an opportunity. A person can apply to this opportunity. If he/she fulfils all or a part of the requirements needed by this opportunity, he/she can become a volunteer if the organization agrees his/her application and then the organization can benefit of his/her skills and time

The model shown above is a simplified version of the one used by the SpONSOR platform. As shown in the Figure 4, the SpONSOR model considers additional information such as:

- Location of the opportunity (and person)
- Time constraints
- Driving Licenses
- Professional competencies
- Experience
- Type (hard, soft) and categories of skills (technical, management, organizational, etc.)
- Profiles of the eventual beneficiary of the opportunity in case of home care tasks.

The schema (Figure 3) is an excerpt of the data model of the SpONSOR platform. The data model of the SpONSOR platform is implemented through a graph-oriented database, that means a concept (such as a Person, an Opportunity, and so on) is a node and the relation "apply for" is represented by an edge between a Person and an Opportunity, and can have several properties.

This approach has several advantages:

- There is no schema for the database: the nodes and the edges (relationships) can be created at the runtime, a fact that offers a very good flexibility to handle new concepts;

- The scalability is very good, because of the nature of the graph. The graph traversal, to be performed for instance for a search, is not depending on the number of nodes;

- Some relations are naturally modeled with a graph, as for instance the relation between an organization and its volunteers

The following classes (or concepts) with theirs associated properties (that are not shown below) are implemented in the data model:

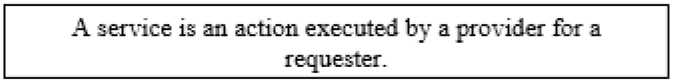
- Person: represents a human person, that can be a volunteer;

- Organization: represents a logical group of persons with the same collective goal;
- Organization type: represents the type (legal view) of an organization;
- Organization category: represents the category (humanitarian, social, etc.) of an organization;
- Opportunity: represents a time where something can be done by a person;
- Opportunity type: represents the type of the opportunity (home care, accompanying seniors, etc.)
- Availability: free time available to perform an opportunity (for a person);
- Location: GPS coordinates (in numeric format) of an address;
- Address (including zip code, street, state, city and country);
- Gender: represents the fact of being male or female for a person;
- Title: represents the status of a person to show his/her rank or profession (Mr., Miss, Dr., etc.);
- Civil status: represents the various distinct options that describe a person's relationship with a significant other person (married, single, divorced, etc.);
- Occupation: represents the job or the profession of a person;
- Professional competencies: represents the skills or competences delivered by an official institute, administration, school or university (diploma, certificate, etc.); Experience: represents a non-professional related competence that can be valorized. An example of experience can be a first activity as a helper for an association, without being validated by a diploma. This field should contain such kind of experience, while qualifying experience should be mentioned into the “professional competencies”;
- Nationality: represents the nationality of a person
- Time commitment: represents the time constraints (date and time required) of an opportunity;
- Document (such as avatar, organization logo and CV);
- Driving license: represents the driving licenses that a person can have;
- Spoken language: represents the spoken languages (with indication of the language mastering level) of a person;
- Event: represents an event organized or sponsored by an organization;
- Questionnaire: represents a list of questions that a person should answer, according to some rules defined by the organization. It is also used for representing General Condition(s) of an Organization.
- Question (including type of expected answers: binary, single or multiple answers, free text): represents a question and its possible answer type that a person should answer, according some rules defined by the organization;
- Sector of activity (for an organization): represents the sector(s) of activity of an organization;
- Recipient (also known as the beneficiary of an opportunity);
- Religion: represents the religion of the person;
- Video: a person can have one or several video sequences linked to his/her profile
- Skill: represents a skill; Skill type: represents the type of skill (soft or hard)
- Skill category: represents the category of the skill (technical, organizational, etc.);
- Interest: represents an interest for a person;
- Training: represents a set of videos that an organization can manage for a training purpose

All these concepts are implemented as a Node, and the relationships between these concepts are implemented as Edges, with specific properties when needed.

3. CORE SERVICES PROVIDED BY THE PLATFORM

This section presents the main services provided by the Sponsor platform for the two targeted entities: namely organization and volunteer. First let's give a definition of a service:



A service is an action executed by a provider for a requester.

As the communication between the front-end (also known as the Graphical User Interface) and the back-end used only web services (and specifically REST web services), an action is typically performed by executing some fragments of a program [4]. The interaction between the two actors (provider and requester) is realized through controllers that exposed specific endpoints formalized by one or several interfaces

An interface defines the supported processing in the form of an input message, an output message, and its URI to use, by providing the protocol to use (HTTP, HTTPS, FTP, etc.) for instance.

Different types of services could be found in the literature:

- Applicative service: service about a particular business domain of the company
- Functional service: service identified in the functional requirements phase
- Technical service: service that serves a specific technical process such as storage data into a database. Different levels of services can also be specified:
- High-level service: allows the access to high-level functionalities of the Business Services (high granularity)
- Low-level service: enables the access to low-level or basics functionalities of the Business Services (low granularity)

A. SPONSOR PLATFORM SERVICES

By definition, a Service-Oriented Architecture is an architecture that exposes its services in the form of independent and well-defined services. Some services are autonomous and some services can use other services (by collaboration, synchronization or composition) to provide further services with strong added value. In addition, these services are also carried out with ready-to-use interfaces

Considering the set of functional requirements, the following high-level services were developed within the Sponsor platform:

- Common Services o Registration
  - Login - Logout
  - Communication
  - Search
  - Statistics

- Organisation-related Services
  - Organisation Management
  - Profile management
  - Event management
  - Panel management
  - Opportunity Management
  - Training Management

- Volunteer-related Services o Volunteer Management
  - Profile management
  - Legal & Ethical advisor

The following schema gives an overview of the services supported by the platform:

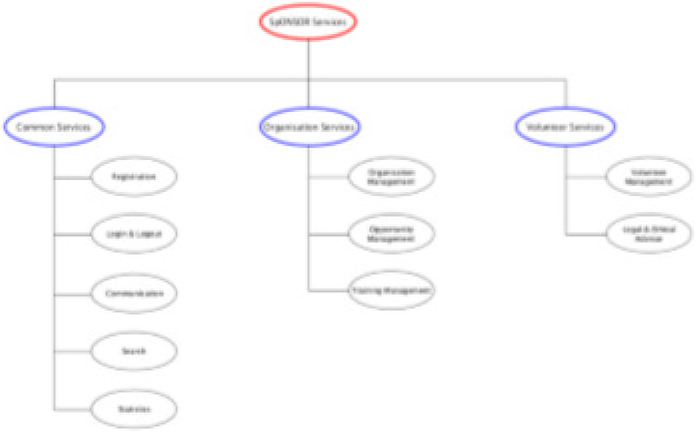


Figure 3: Sponsor Services Overview

Each service is briefly described in the following sections.

Name of service: Organization Profile Management starts always by /organization
Objective(s): this service supports all the operations related to the management of an organization, including the management of its own profile
Description: an organization needs to support some business operations such as the management of its profile, including adding, removing, updating its logo, its own documents, and its general conditions if needed.
Functionalities: Profile creation; Profile update; Profile deletion; Document addition; Document deletion; General condition addition; General condition deletion; General condition update; Logo addition/update; Logo deletion; Get the creator of an organization.

The following service manages the events proposed by a given organization

Name of service: Organization Events Management starts always by /organization/{organization ID}/event.
Objective(s): this service supports all the operations related to the management of the events proposed by an organization
Description: an organization can provide information on some events related to its business or located near the organization.
Functionalities: Event creation; Event deletion; Event update; Get an event.

The following service managed the panel of potential volunteers for a given organization:

Name of service: Organization Panel Management starts always by /organization/{organizationID}/panel
Objective(s): this service supports all the operations related to the management of the panel of an organization
Description: an organization can manage into a "virtual" panel a list of potential volunteers. These volunteers could be contacted by the organization later if needed.
Functionalities: Volunteer addition on a panel; Volunteer deletion from a panel; Organization panel deletion; Get all volunteers from a panel managed by an organization

The following services are helper services related to one or all organizations

Name of service: Organization Helper Service starts always by /organization/
Objective(s): this service provides some operations that perform basic searches on the database related to organization(s).
Description: the organization helper service frames basic searches related to information managed by organization, such as all events or all organizations
Functionalities: Get all events with criteria; Get all organizations; Get all organizations sorted by countries.

C. OPPORTUNITY RELATED SERVICES

The following section gives the services offered to manage an opportunity.

Name of service: Opportunity Service starts always by /opportunity/
Objective(s): this service provides basic operations to manage opportunities from the organization point of view
Description: this service provides support for the management of opportunity by giving the essentials functionalities
Functionalities: Opportunity creation; Opportunity deletion; Opportunity update; Get an opportunity.

Name of service: Opportunity Helper Service starts always by /opportunity
Objective(s): this service provides search functionalities on opportunities.
Description: search functionalities such as getting all opportunities or only a subset with some criteria are provided by this service.
Functionalities: Get all opportunities; Get opportunities with criteria.

D. VOLUNTEER- RELATED SERVICES

The following services provides support for the management of volunteers:

Name of service: Person Profile Management starts always by /person
Objective(s): this service supports all the operations related to the management of a person, including the management of its own profile
Description: a person needs to support some business operations such as the management of its profile, including adding, removing, updating his/her avatar, and his/her documents if needed
Functionalities: Profile creation; Profile update; Profile deletion; Get a profile; Document addition; Document deletion; Avatar addition/update; Avatar deletion

Name of service: Person Events Management Service starts always by /person/{personID}/event
Objective(s): this service supports all the operations related to the management of the events that a person could be interested in
Description: a person can register (or unregister) himself/herself for an event proposed by one or several organizations
Functionalities: Event registration; Event unregistration

Name of service: Person Helper Service starts always by /person/
Objective(s): this service provides search functionalities on volunteers or information related to the volunteers
Description: search functionalities such as getting all volunteers or only a subset with some criteria are provided by this service, setting or getting preferred organizations or opportunities for a person, etc.
Functionalities: Get all persons; Get events for which a person is registered; Get preferred organizations; Get preferred opportunities; Set/update preferred organizations; Set/update the preferred opportunities; Remove preferred organizations; Remove preferred opportunities.

E. MANAGEMENT SERVICES

Name of service: Management Service starts always by /management/
Objective(s): this service provides specific management functionalities for organization and volunteer
Description: this main service provided several services to manage the application status from the both side: volunteer and organization. A person can apply to an opportunity, withdraw an application or be interested by opportunities and organizations. An organization can set the status of the volunteer: ACCEPTED, REFUSED, STANDBY, CONVOKED INTERVIEW, CONVOKED TRAINING, QH.
Functionalities: Get opportunities posted by an organization; Get opportunities status for a volunteer; Get opportunities for a volunteer; Get organizations that posted an opportunity; Get persons with specific status related to an opportunity; Get status for a volunteer; Get volunteer status for an opportunity; Get applicants for opportunities; Set application status apply (APPLY) for an opportunity; Set application status withdraw (WITHDRAW) for an opportunity; Set the general status for an application for a volunteer; Set the status for a volunteer.

Some business rules are also implemented for some services. For example, a volunteer can only withdraw his application once the application has indeed been submitted. When a volunteer wants to withdraw his/her application, however before having filed it, an error 409 is returned by the platform with an appropriate message.

4. COMMON SERVICES

This section gives an overview of the common services provided by the platform. The term "common services" refers to services used by all the entities managed by the platform**.**

A. REGISTRATION AND LOGIN SERVICES

These services provide registration and login into the platform.

Name of service: Registration and Login Service starts by /register for registration starts by /login for login
Objective(s): this service enables the registration and the login to the platform. In addition, two services are provided: • Change the password: a user can change his/her password • Reset the password: reset the password if the user forgets it
Description: an organization can provide information on some events related to its business or located next to the organization.
Functionalities: Registration of a person; Registration of a representative of an organization; Log in into the platform; Reset the password; Change the password

B. COMMUNICATION SERVICES

This service provides communication means between the volunteers and the organizations. The communication is realized through messages, and email notifications.

Name of service: Communication Service starts by /message for communication
Objective(s): this service enables sending and receiving messages between volunteers and organizations.
Description: volunteers and organizations can communicate through an internal messaging channel. A message basically corresponds to an email including the following data: • Sender • Receiver(s): can be an email address • Subject • Content Depending on some actions, emails are also sent automatically by the platform.
Functionalities: Get all messages received or sent by an organization; Get all messages received or sent by a person; Get a message by its unique identifier; Create and post a message to one or several receivers, sent by an organization; ; Create and post a message to one or several receivers, sent by a volunteer; Delete a message, identified by its unique identifier

C. SEARCH SERVICES

The following services provides search functionalities, limited to some elements of the model such as:

- Opportunity
- Organization
- Event

Name of service: Search Service
Objective(s): this service provides search functionalities for the following elements: opportunity, organization and event
Description: volunteer and organization would search information on opportunities, organizations and events stored in the database. In order to provide such functionalities, a full-text search is made with the help of a dedicated search engine: the elastic search that provides full-text search with an indexing mechanism to speed-up the search.
Functionalities: Get all opportunities that contain a word or a list of words; Get all events that contain a word or a list of words; Get all organizations that contain a word or a list of words.

The elastic search database is populated/updated each time when an opportunity, an organization or an event is created, respectively updated. These actions are totally transparent for the user, and are made asynchronously to avoid blocking the graphical user interface. The search and matching functionalities are note very detailed in this paper.

D. STATISTICS SERVICES

Several statistics services are also provided by the platform. The statistics module makes calculations based on events and opportunities indexed for searched, and offers an additional service to index person profiles. The following statistics are available:

- Most frequent terms in opportunities
- Most searched terms in events and opportunities
- Most frequent interests and most frequent skills appearing in the profiles.

Name of service: Statistics Service
Objective(s): this service provides statistics for the following elements: opportunity, skills, interests and events
Description: it could be interesting to know the most frequent terms used in the description of opportunities for a volunteer, in order to know if one of his/her skills or interests is frequently occurring or searched, for example. This service furnishes also other useful statistical data both for an organization (regarding the most frequent terms appearing in person profiles, for example) and for a person (most frequent terms in opportunities profile)
Functionalities: Get most frequent terms in opportunities; Get searched items in events; Get searched items in opportunities; Get most frequent interests in profiles; Get most frequent skills in profiles; Get legal document(s) that contain specific words.

By default, the statistics are calculated by taking into account the data collected over the previous six months. This service is also responsible for indexing legal documents managed by the legal service. Once legal documents are indexed, it is possible to perform a full-text search on them.

E. LEGAL SERVICES

The legal service provided by the platform gives some advices to the volunteer on the legal aspects related to the opportunity he/she wants to apply for. The mechanism is based on a Legal Tree approach [5]. This service manages legal documents with the following model.

Field	Type	Description	Example value
id	String	Technical field. Automatically generated when a document is inserted.	Mf69875
Name	String	Name of the document.	Loi fédérale sur l'assurancevieillesse et survivants
Lang	String	(Optional) The language of the document.	Fr
Sections	Array of Section object	The sections that compose the document. This field is automatically managed by the system	
Pages	Integer	(Optional) The number of pages of the document, if applicable.	74
Ref	String	The file name if the document is a file, or the URL if the document is a web page.	Document 1.pdf

A section is a concept that is managed by the system when indexing the content of the legal document. The associated object has the following schema:

Field	Type	Description	Example value
Name	String	Name of the section	Article 7
cont.	String	Content of the section	Le Conseil fédéral peut fixer
Page	Int.	The page on which the section starts, if applicable	42

5. CONCLUSION

This paper presented the data management services developed in the SpONSOR platform, that are in line with the User Requirements & System requirements, the scenarios developed as well as with the legal guidance and requirements.

The main outcomes of this paper are:

- Identification and definition of the major SpONSOR services that are implemented in the platform.
- Definition of the main interactions between the different layers of the architecture.

Furthermore, this paper aimed at establishing a bridge between conceptual developments and results that were achieved in requirements phase, and the implementation phase, in which the Sponsor platform and its associated services are being developed.

We acknowledge that the work presented in this paper is composed of part of the technical contribution (Data Management Model) developed under an AAL [6] funded project (SPONSOR [7] [8]) and supported by the National Research Fund of Luxembourg

REFERENCES

[1] https://msdn.microsoft.com/enus/library/ee658117.aspx#NTier3TierStyle

[2] Haerder, T.; Reuter, A. (1983). "Principles of transaction-oriented database recovery". ACM Computing Surveys. 15 (4): 287. doi:10.1145/289.291

[3] https://martinfowler.com/eaaCatalog/dataTransferObject.html.

[4] https://www.w3.org/TR/ws-arch/#action (section Explanation).

[5] Adnan Imeri, Abdelaziz Khadraoui, Thang Le Dinh, Djamel Khadraoui: Personalization of Legal and Ethical Information in ICT Platforms: The Approach of Legal Decision Tree. Computer and Information Science 10(1): 77-88 (2017).

[6] http://www.aal-europe.eu/

[7] Amedeo Cesta, Gabriella Cortellessa, Riccardo De Benedictis, Francesca Fracasso, Daniel Baumann, Stefano Cuomo, Julie Doyle, Adnan Imeri, Djamel Khadraoui, Pierre Rossel: Personalizing Support to Older Adults who Look for a Job with the SpONSOR Platform. AI*AAL@AI*IA 2016: 105-122

[8] http://www.sponsor-aal.eu

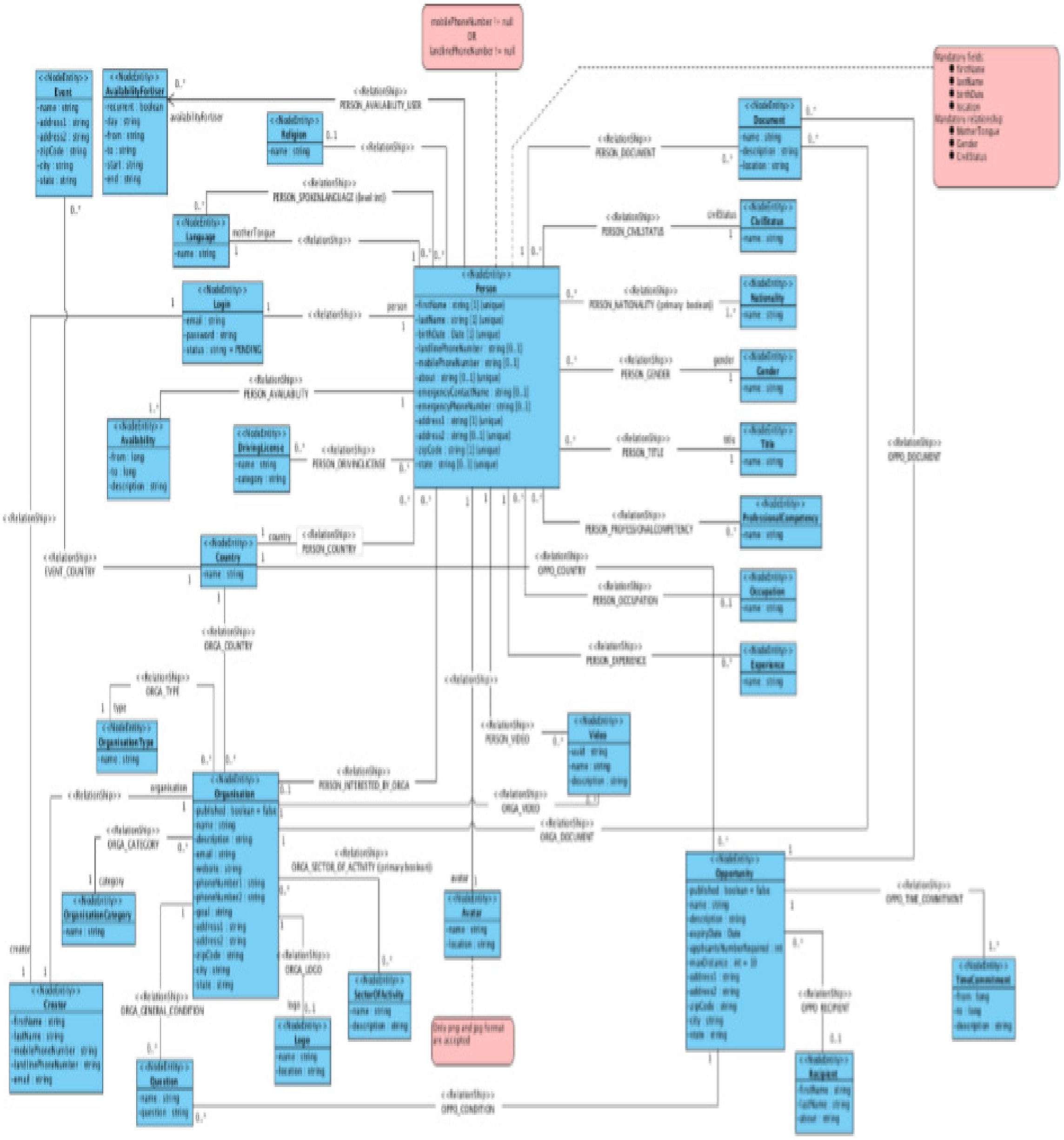

mobilePhoneNumber != null
OR
landlinePhoneNumber != null
Mandatory fields
firstName
lastName
birthDate
location
Mandatory relationship
MotherTongue
Gender
CivilStatus
<<NodeEntity>> Event
-name : string
-address1 : string
-address2 : string
-zipCode : string
-city : string
-state : string
<<NodeEntity>> AvailabilityForUser
-recurrent : boolean
-day : string
-from : string
-to : string
-start : string
-end : string
availabilityForUser
<<RelationShip>> PERSON_AVAILABILITY_USER
<<NodeEntity>> Religion
-name : string
<<RelationShip>> PERSON_SPOKENLANGUAGE (level int)
<<NodeEntity>> Language
-name : string
motherTongue
<<NodeEntity>> Login
-email : string
-password : string
-status : string = PENDING
person
<<RelationShip>> PERSON_AVAILABILITY
<<NodeEntity>> Availability
-from : long
-to : long
-description : string
<<NodeEntity>> DrivingLicense
-name : string
-category : string
<<RelationShip>> PERSON_DRIVINGLICENSE
<<NodeEntity>> Person
-firstName : string [1] {unique}
-lastName : string [1] {unique}
-birthDate : Date [1] {unique}
-landlinePhoneNumber : string [0..1]
-mobilePhoneNumber : string [0..1]
-about : string [0..1] {unique}
-emergencyContactName : string [0..1]
-emergencyPhoneNumber : string [0..1]
-address1 : string [1] {unique}
-address2 : string [0..1] {unique}
-zipCode : string [1] {unique}
-state : string [0..1] {unique}
<<RelationShip>> PERSON_DOCUMENT
<<NodeEntity>> Document
-name : string
-description : string
-location : string
<<RelationShip>> PERSON_CIVILSTATUS
civilStatus
<<NodeEntity>> CivilStatus
-name : string
<<RelationShip>> PERSON_NATIONALITY (primary boolean)
<<NodeEntity>> Nationality
-name : string
<<RelationShip>> PERSON_GENDER
gender
<<NodeEntity>> Gender
-name : string
<<RelationShip>> PERSON_TITLE
title
<<NodeEntity>> Title
-name : string
<<RelationShip>> OPPO_DOCUMENT
<<RelationShip>> PERSON_PROFESSIONALCOMPETENCY
<<NodeEntity>> ProfessionalCompetency
-name : string
country
<<RelationShip>> PERSON_COUNTRY
<<NodeEntity>> Country
-name : string
<<RelationShip>> EVENT_COUNTRY
<<RelationShip>> OPPO_COUNTRY
<<RelationShip>> PERSON_OCCUPATION
<<NodeEntity>> Occupation
-name : string
<<RelationShip>> PERSON_EXPERIENCE
<<NodeEntity>> Experience
-name : string
<<RelationShip>> ORGA_COUNTRY
<<RelationShip>> ORGA_TYPE
type
<<NodeEntity>> OrganisationType
-name : string
<<RelationShip>> PERSON_VIDEO
<<NodeEntity>> Video
-uuid : string
-name : string
-description : string
<<RelationShip>> PERSON_INTERESTED_BY_ORGA
organisation
<<NodeEntity>> Organisation
-published : boolean = false
-name : string
-description : string
-email : string
-website : string
-phoneNumber1 : string
-phoneNumber2 : string
-goal : string
-address1 : string
-address2 : string
-zipCode : string
-city : string
-state : string
<<RelationShip>> ORGA_VIDEO
<<RelationShip>> ORGA_DOCUMENT
<<RelationShip>> ORGA_CATEGORY
category
<<NodeEntity>> OrganisationCategory
-name : string
<<RelationShip>> ORGA_SECTOR_OF_ACTIVITY (primary boolean)
avatar
<<NodeEntity>> Avatar
-name : string
-location : string
<<NodeEntity>> Opportunity
-published : boolean = false
-name : string
-description : string
-expiryDate : Date
-applicantsNumberRequired : int
-maxDistance : int = 10
-address1 : string
-address2 : string
-zipCode : string
-city : string
-state : string
<<RelationShip>> OPPO_TIME_COMMITMENT
<<NodeEntity>> TimeCommitment
-from : long
-to : long
-description : string
creator
<<NodeEntity>> Creator
-firstName : string
-lastName : string
-mobilePhoneNumber : string
-landlinePhoneNumber : string
-email : string
<<RelationShip>> ORGA_GENERAL_CONDITION
<<NodeEntity>> Question
-name : string
-question : string
<<RelationShip>> ORGA_LOGO
logo
<<NodeEntity>> Logo
-name : string
-location : string
<<NodeEntity>> SectorOfActivity
-name : string
-description : string
Only png and jpg format are accepted
<<RelationShip>> OPPO_RECIPIENT
<<NodeEntity>> Recipient
-firstName : string
-lastName : string
-about : string
<<RelationShip>> OPPO_CONDITION

Figure 4: Data model (extract).

INTENTIONAL BLANK

CAMOUFLAGED WITH SIZE: A CASE STUDY OF ESPIONAGE USING ACQUIRABLE SINGLE-BOARD COMPUTERS

Kiavash Satvat[1], Mahshid Hosseini[1] and Maliheh Shirvanian[2]

[1]Department of Computer Science,
University of Illinois at Chicago, Chicago, USA
[2]Department of Computer Science,
University of Alabama at Birmingham, Alabama, USA

ABSTRACT

Single-Board Computers (SBC) refer to pocket-sized computers built on a single circuit board. A number of studies have explored the use of these highly popular devices in a variety of domains, including military, agriculture, healthcare, and more. However, no attempt was made to signify possible security risks that misuse of these devices may bring to organizations. In this study, we perform a series of experiments to validate the possibility of using SBCs as an espionage gadget. We show how an attacker can turn a Raspberry Pi device to an attacking gadget and benefit from short-term physical access to attach the gadget to the network in order to access unauthorized data or perform other malicious activities. We then provide experimental results of placing such tools in two real-world networks. Given the small size of SBCs, traditional physical security measures deployed in organizations may not be sufficient to detect and restrict the entrance of SBCs to their premises. Therefore, we reiterate possible directions for network administrators to deploy defensive mechanisms for detecting and preventing such attacks.

KEYWORDS

Espionage, Single-Board Computer (SBC), Physical Security, Network Security, Raspberry Pi.

1. INTRODUCTION

Single-Board Computer (SBC) is a pocket-sized computer that is built on a single circuit board. Using microprocessors and high density integrated circuits these small devices are able to offer almost all the functionalities of desktop computers. Small size and low-cost of SBCs have made them a strong competitor in the computing market.

The popularity of SBCs has increased with the emergence of companies that produce commercially affordable devices such as Raspberry Pi [1], BeagleBone [2], and Arduino [3]. A series of functionalities such as the embedded wireless card, USB, and Ethernet port further justified the popularity of SBCs. Moreover, mass production reduced the price of each unit and made it more affordable for general purposes. The pocket-sized Raspberry Pi (only as one example) has

Dhinaharan Nagamalai et al. (Eds) : CSEIT, NCS, SPM, NeTCoM - 2018
pp. 69–80, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81806

become the third most popular computer in less than five years [4]. Distribution of over 10 million devices shows the currency of this device [5] in recent years.

Literatures have explored the use of SBCs in different industries (e.g., IoT [6, 7], health care [8, 9], and cloud [10, 11]). As an example, size and price have made SBC a major candidate to be used as the underlying hardware for IoT devices. Recently, IBM has specifically introduced integration of Watson IoT platform with Raspberry Pi [12]. Sensly [13], a smart and portable air pollution sensor, Fridge [14], and Espresso[15], as two IoT-enabled appliances are a few examples of IoT devices using SBC.

While SBC had been the focus of researchers in several domains, less number of works have considered it in the realm of offensive security. In [16], authors have discussed possible usage of this device to launch different types of penetration tests to assess the security of a network. [17] uses Raspberry Pi as a Honeypot to detect SQL injection attacks and [18] deployed a Honeypot to simulate vulnerabilities and attract attackers. Hu et al. used this device as a distributed vulnerability assessment tool [19]. However, to the best of our knowledge, no previous research has been conducted to represent the potential misuse of SBC to threaten the security of a network.

Industrial espionage has existed long before the emergence of the Internet, however, modern technologies have facilitated theft of information. Prior to the emergence of commercially accessible SBC devices, access to spy gadgets and gears were limited. The finite number of producers and distributors available in the market made the traceability of these devices easy. For instance, there were only a limited number of companies to produce the physical key-loggers and market their devices publicly. Industrial espionage is now a major threat to the corporate world and can make long-term harm to companies. It has been reported that cyber-crime and economic espionage costs more than $445 billion annually in the world economy (almost 1 percent of global income) [20].

In this paper, we show how an attacker can deploy a full-fledged inexpensive attacking tool that can be mounted on networks if he has short-term physical access to the organization. We perform a set of experiments to demonstrate the possible harm that misemploying of SBC may cause. To show the feasibility of the attack, we use Raspberry Pi as a spying device to attack two real-world networks. We also provide possible directions for detection and prevention of such attacks.

SBC facilitates our attacks in several aspects. First, unlike the traditional form of insider attacks, the attacker does not need to plug a large computational device to the network. Large devices are more probable to be noticed while entering the organization or if left unattended for a long duration of time. In contrast, in our work, the attacker can benefit from the small size of SBC, and take them to premises and even leave them for a long period of time without grabbing the attention of security officers or employees. Second, in conventional attacks the attacker may exploit an insider machine to run a malicious software; however, such malwares may get detected by the machine's antivirus/malware tools or be noticed since they impact the performance of the local machine. SBC on the other hand, is an attacker owned device with no local anti-virus and malware tool installed and is not controlled by the system administrator. Third, using SBC, the attacker does not need to launch the attacks from outside the networks and, therefore, the possibility of detecting the attack by edge intrusion detection systems and firewalls reduces. All the mentioned points can play in favor of the attacker to smoothly perform the malicious activities without getting trapped.

Contributions: The detail contribution of our work is as follow.

1. Attack Setup: We turned a low-cost Raspberry Pi 3 (as an instance of SBC) into a spying gadget and plug it to a victim machine located in a real-world network to subliminally intercept the target machine's traffic. We installed Kali Linux on Raspberry Pi and loaded our gadget with multiple off-the-shelf malicious scripts and tools to exploit the victim. Our device is capable of launching different types of attacks including sniffing, spoofing, and man in the middle attacks.

2. Experiment and Results: We tested our gadget in two large size organization. Due to ethical considerations, we only intercepted the traffic targeted to the examiner's machine acting as the victim. We successfully launched several attacks including traffic sniffing and redirecting, and DNS service poisoning as a few examples of several possible attacks. We observed that both organizations were highly susceptible to the attacks launched from our small size spying gadget.

3. Direction for Defense: We conclude by reiterating defensive mechanisms that may be deployed to detect and prevent the suggested attacks. While threats are continually evolving and adapting to undermine protective measures, security measures as an ongoing set of practices and controls need to be updated to reduce the possible harms that new threats may cause.

Paper Outline: In Section 2, we present the potential attack scenario. Next, in Section 3, we present the experiment and its results. This is followed by Section 4, where we discuss possible defense mechanisms. Finally, we summarize our results and conclude our paper in Section 5.

2. ATTACK SETUP

In this section, we define the threat model and describe how an attacker can turn SBCs into an Espionage gadget.

2.1. Threat Model

In our study, the malicious adversary tries to launch network attacks against target victims in a large scale organization using an SBC. The attacker has short-term physical access to the organization, that is, he has access to enter the premises but is not allowed to carry advanced computational devices (e.g., laptop) into the building and leave it unattended.

In this scenario, the attacker enters the building carrying the pocket-size SBC (despite the organization's policy). After accessing the building, the attacker can plug the device in a hidden way to a computer or the network. The attacker may load the SBC with off-the-shelf tools and script to fully launch different type of attacks, including passive attacks (e.g., intercept and transfer private information to the outsiders or possibly store them locally for future offline access), or active attacks (e.g., DNS poisoning and man-in-the-middle attack) as will be discussed in Section 2.2.

Our hypothesis is that the attacker can plug the device in a subliminal way – owing to its size, and launch the attacks successfully, given poor network configuration and lack of optimal physical and network system countermeasures.

2.2. Turning Raspberry Pi into an Espionage Gadget

Hardware Specification: We selected Raspberry Pi [1] due to its popularity, affordability, and desired functionality it can provide. However, any other available SBC with network communication support can be chosen. We use the third generation of Raspberry Pi with the Quad Core 1.2GHz Broadcom BCM2837 64bit CPU, 1GB RAM, BCM43438 wireless LAN and Bluetooth Low Energy (BLE) on board, 4 USB 2 ports and Micro SD port for storing data.

Physical Setup: Several approaches may be taken to connect the Raspberry Pi device to the targeted network. If the attacker has unrestricted access to the victim's wireless network, he can connect and intercept the traffic. Similarly, the attacker may simply plug Raspberry Pi to any unattended network socket. However, commonly, administrators limit the number of available network sockets and restrict access to wireless networks and unplugged wired ones.

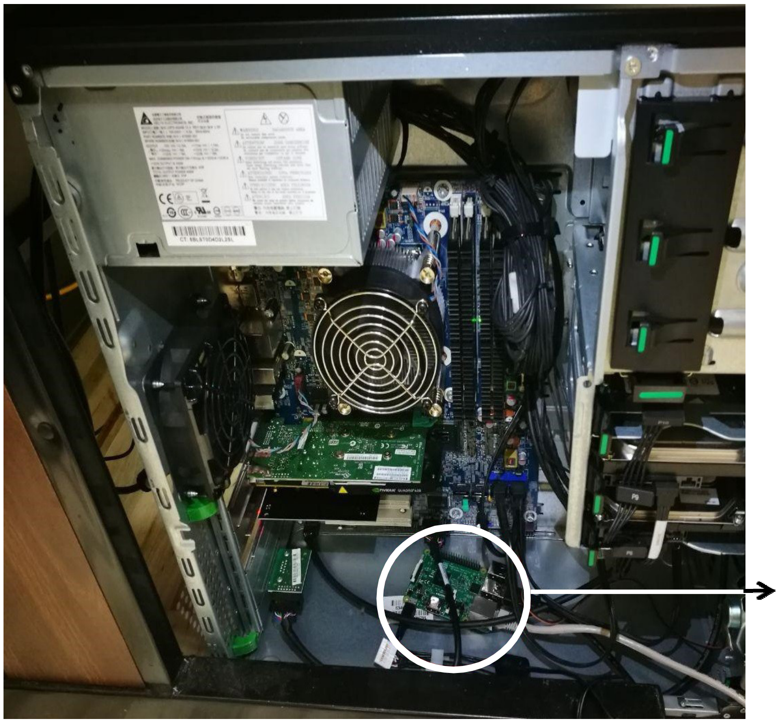


Fig. 1: Experiment Setup

Optionally, the attacker may connect the SBC to a victim machine to intercept and relay all the traffic targeted to the victim machine, while performing other network attacks. In this setting, the attacker puts the gadget between the target computer and the network (i.e., acting as a hub between the victim machine and the network). Hence, the device can use the network port primarily assigned to the target machine and intercept/relay all traffic designated to target machine. Figure 1 shows an example of such a setup used in our experiment.

Apart from the unavailability of network sockets, the main motivation behind this setup is to minimize the interception of traffic to one machine rather than the whole network due to ethical consideration (as will be fully discussed in chapter 3.1).

Operating System: We used Kali Linux [21] (A distribution of Linux for penetration testing) as an underlying platform for launching the attacks. Kali Linux offers two different pre-built versions that can be installed on Raspberry Pi: first, a light image, streamlined with the minimum tools; second, a full version that includes a Kali Linux full meta-package [22]. In this paper, we used the light version, which only encompasses some of the major Kali's application. The reason for installing the lighter version was that we found it more stable and also it helps the system to boot faster compared to the full meta-package.

Network Attacking Tools: After installing Kali Linux in Raspberry Pi, we installed a series of tools, which is needed to launch the attack. First, we installed the *Bridge-utills* package for sharing the Internet and making the Raspberry pi able to sniff the traffic somewhere between the targeted system and the network. This package lets Raspberry become a hub and accordingly helps to pass and intercept the traffic. Second, we installed the *tcpdump* packet analyzer to capture TCP/IP packets over a network. *tcpdump* provides the functionality of dumping the live packages and storing them into the dump files. Third, *Driftnet* [23], which listens to the network stream and picks images from TCP traffic. Finally, we installed *Ettercap* as a comprehensive suite for the man-in-the-middle attacks. This tool allows launching the DNS spoofing and redirecting the user to the attacker's website. Other tools can be loaded as per the attacker's requirement.

3. EXPERIMENT AND RESULT

3.1. Ethical Consideration

It has always been a dilemma whether computer network attacks are ethically correct. It is known that computer network attacks may harm an individual's and company's privacy, secrecy, reputation, and financial gains. However, if used in the correct way to aware the companies on possible vulnerabilities, it in fact, turns into a valuable tool helping to improve the security of the organizations. For more information about the ethics of computer network attacks please refer to [24].

Similar to any other network attack study, the purpose of our study and the affected target machine's defines the ethics of our work. In this research, we attempt to cast light on the fact that small SBCs have gained enough computational and communication power that they can be used as powerful attacking devices. We run several experiments to show how a real-world organization could be susceptible to attacks. In order to follow the ethical consideration, we designed our experiments so that we minimize the harm to the organizations by limiting the target of the attack to the experimenter's computer on the same network, as will be discussed in Section 3.2.

3.2. Experiment

To demonstrate the results of using the spying SBC in real world contexts, we conducted our experiments in two different organizations, an educational institution and a telecommunication company. We examined our scenario in a setting where the SBC device acts as a hub between a victim computer and the network. As mentioned in Section 3.1 the victim computer is the examiner's computer. Such a computer is a representative of other nodes in the same network with a similar setup and attack protective measures that are applied from a centralized network administration system.

Our SBC is able to capture all the traffic with the victim machine as the destination. Depending on the type of the attack, the attacker may store the traffic, transfer it to an external destination, or relay it to the victim (with or without manipulation). Note that the device is in fact capable of launching other types of active or passive attacks on the whole network, however, to eliminate the harm to the organization network, we pick attacks that only impact the victim machine. Figure 2 shows the attack

Attacker Outside the Premises

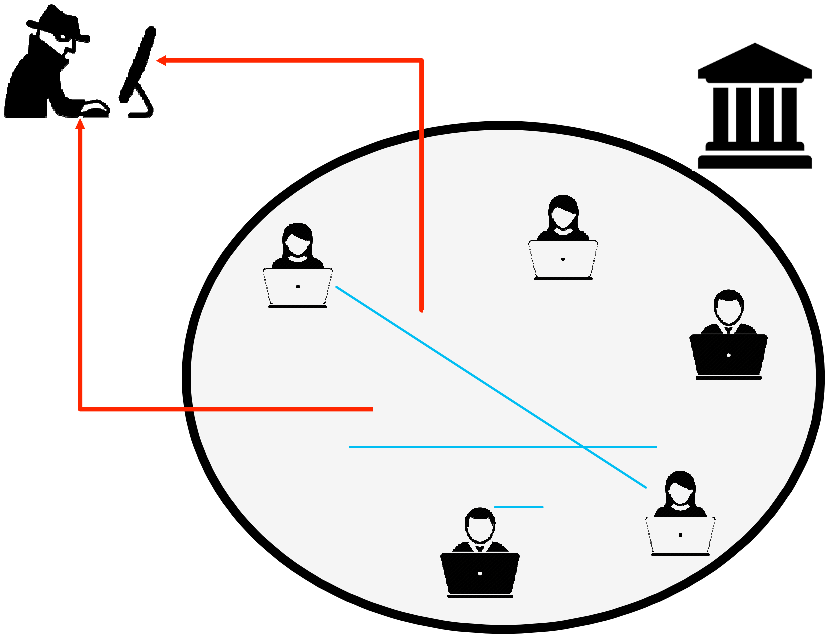
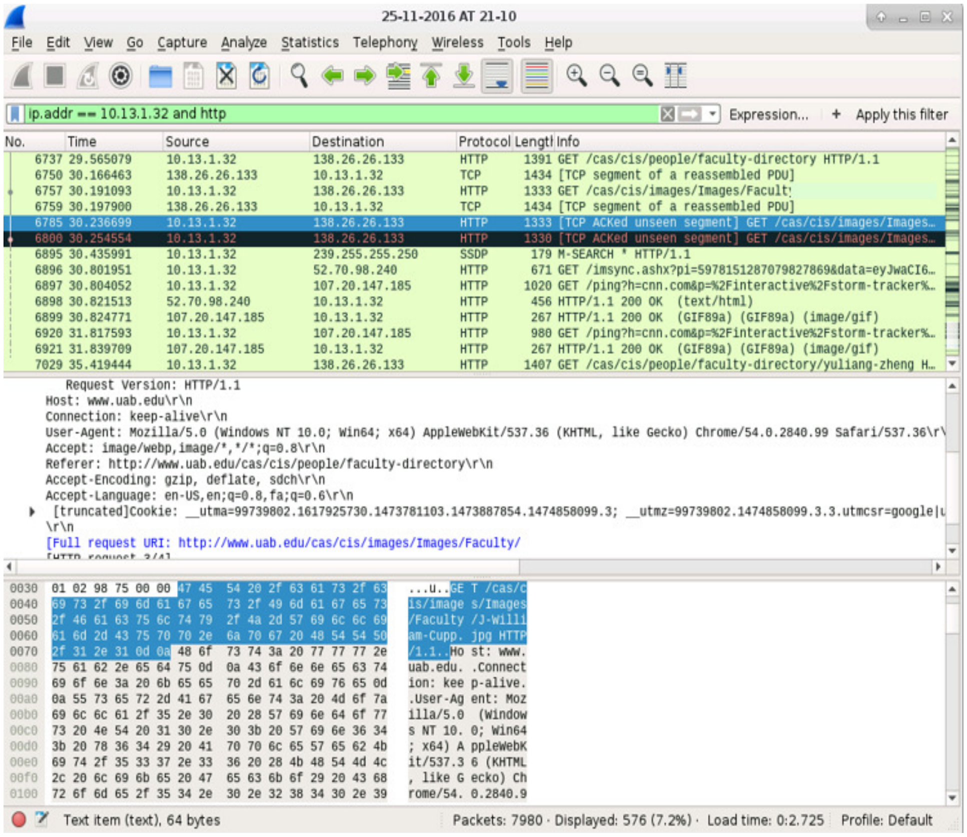


Fig. 2: Attack overview

Transferring Data to the attacker: As discussed in Section 2.1, the attacker has a limited, short-term access to the target company premises. Thereby, he needs to follow a mechanism to obtain his accumulated data. The attacker may store the data on the device and later on collect the device and analyze the stored data offline. Optionally, the attacker can use the device to access the data online by making the device to transfer the data in real-time or upon attacker's request. For the purpose of transferring the data to the attacker, we took two approaches: 1) emailing the collected data to the attacker and 2) storing the collected data on a cloud-based storage.

In the first option, we setup an email account on Gmail that is used by the attacker to receive the data stored on Raspberry Pi. We developed a Python program that creates an email with the Raspberry Pi data as a file attachment and sends it to the attacker email address every 60s (the timing is configurable). In the second option, we created a Dropbox account and a Dropbox API App under the same Dropbox account that can access files. We created a Dropbox directory to store files and gave the app access overview where the attacker can mount the spying device to one or more nodes to launch passive and active targeted or holistic attacks to this folder. We then developed a Python application that uses Dropbox library and uploads locally stored files (e.g., dump files) to Dropbox using an access token generated on Dropbox account.


25-11-2016 AT 21-10
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+ Apply this filter

ip.addr == 10.13.1.32 and http

```
No.   Time          Source           Destination       Protocol Lengtl Info
 6737 29.565079     10.13.1.32       138.26.26.133     HTTP     1391 GET /cas/cis/people/faculty-directory HTTP/1.1
 6750 30.166463     138.26.26.133    10.13.1.32        TCP      1434 [TCP segment of a reassembled PDU]
 6757 30.191093     10.13.1.32       138.26.26.133     HTTP     1333 GET /cas/cis/images/Images/Facult;
 6759 30.197900     138.26.26.133    10.13.1.32        TCP      1434 [TCP segment of a reassembled PDU]
 6785 30.236699     10.13.1.32       138.26.26.133     HTTP     1333 [TCP ACKed unseen segment] GET /cas/cis/images/Images…
 6800 30.254554     10.13.1.32       138.26.26.133     HTTP     1330 [TCP ACKed unseen segment] GET /cas/cis/images/Images…
 6895 30.435991     10.13.1.32       239.255.255.250   SSDP      179 M-SEARCH * HTTP/1.1
 6896 30.801951     10.13.1.32       52.70.98.240      HTTP      671 GET /imsync.ashx?pi=5978151287079827869&data=eyJwaCI6…
 6897 30.804052     10.13.1.32       107.20.147.185    HTTP     1020 GET /ping?h=cnn.com&p=%2Finteractive%2Fstorm-tracker%…
 6898 30.821513     52.70.98.240     10.13.1.32        HTTP      456 HTTP/1.1 200 OK  (text/html)
 6899 30.824771     107.20.147.185   10.13.1.32        HTTP      267 HTTP/1.1 200 OK  (GIF89a) (GIF89a) (image/gif)
 6920 31.817593     10.13.1.32       107.20.147.185    HTTP      980 GET /ping?h=cnn.com&p=%2Finteractive%2Fstorm-tracker%…
 6921 31.839709     107.20.147.185   10.13.1.32        HTTP      267 HTTP/1.1 200 OK  (GIF89a) (GIF89a) (image/gif)
 7029 35.419444     10.13.1.32       138.26.26.133     HTTP     1407 GET /cas/cis/people/faculty-directory/yuliang-zheng H…
```

```
    Request Version: HTTP/1.1
  Host: www.uab.edu\r\n
  Connection: keep-alive\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36\r\
  Accept: image/webp,image/*,*/*;q=0.8\r\n
  Referer: http://www.uab.edu/cas/cis/people/faculty-directory\r\n
  Accept-Encoding: gzip, deflate, sdch\r\n
  Accept-Language: en-US,en;q=0.8,fa;q=0.6\r\n
▸  [truncated]Cookie: __utma=99739802.1617925730.1473781103.1473887854.1474858099.3; __utmz=99739802.1474858099.3.3.utmcsr=google|u
  \r\n
  [Full request URI: http://www.uab.edu/cas/cis/images/Images/Faculty/
  [HTTP request 3/4]
```

```
0030  01 02 98 75 00 00 47 45  54 20 2f 63 61 73 2f 63   ...u..GE T /cas/c
0040  69 73 2f 69 6d 61 67 65  73 2f 49 6d 61 67 65 73   is/image s/Images
0050  2f 46 61 63 75 6c 74 79  2f 4a 2d 57 69 6c 6c 69   /Faculty /J-Willi
0060  61 6d 2d 43 75 70 70 2e  6a 70 67 20 48 54 54 50   am-Cupp. jpg HTTP
0070  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1..Ho st: www.
0080  75 61 62 2e 65 64 75 0d  0a 43 6f 6e 6e 65 63 74   uab.edu. .Connect
0090  69 6f 6e 3a 20 6b 65 65  70 2d 61 6c 69 76 65 0d   ion: kee p-alive.
00a0  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   .User-Ag ent: Moz
00b0  69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
00c0  73 20 4e 54 20 31 30 2e  30 3b 20 57 69 6e 36 34   s NT 10. 0; Win64
00d0  3b 20 78 36 34 29 20 41  70 70 6c 65 57 65 62 4b   ; x64) A ppleWebK
00e0  69 74 2f 35 33 37 2e 33  36 20 28 4b 48 54 4d 4c   it/537.3 6 (KHTML
00f0  2c 20 6c 69 6b 65 20 47  65 63 6b 6f 29 20 43 68   , like G ecko) Ch
0100  72 6f 6d 65 2f 35 34 2e  30 2e 32 38 34 30 2e 39   rome/54. 0.2840.9
```

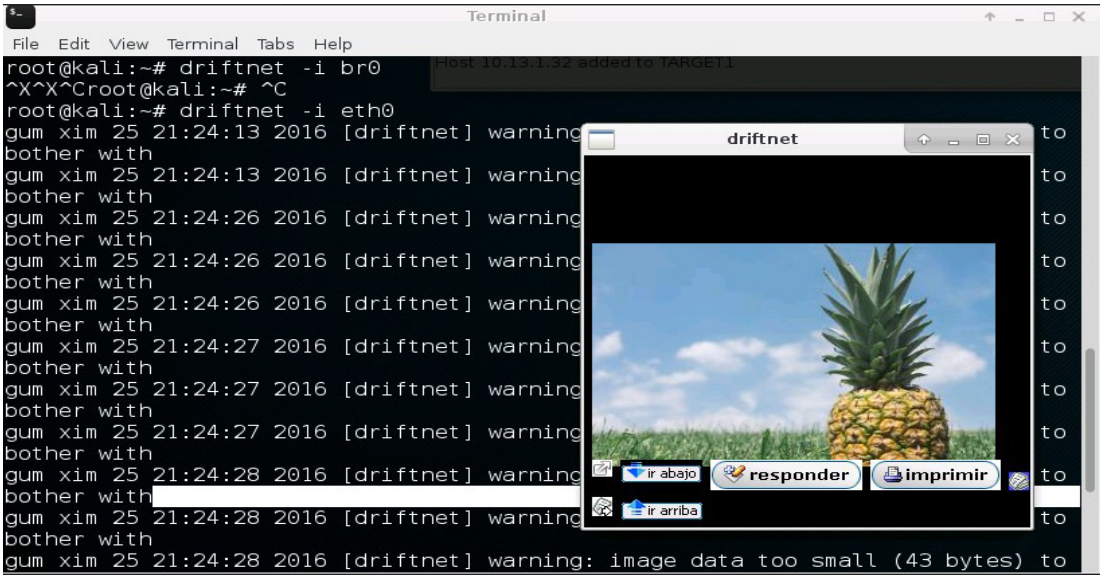
Text item (text), 64 bytes · Packets: 7980 · Displayed: 576 (7.2%) · Load time: 0:2.725 · Profile: Default

Fig. 3: Viewing intercepted traffic using Wireshark

Intercepting Network Traffic: For the purpose of sniffing network traffic, we used *tcpdump*, as a common command-line monitoring and packet analyzer tool. Using *tcpdump* network administrators are able to acquire network traffic for future debugging. *tcpdump* is a light-weight application and therefore is suitable to be loaded on Raspberry Pi.

We accessed the *tcpdump* data remotely and not from the Raspberry Pi device itself. Hence, we stored the dump data in a local file. Since the size of the file could become large, we developed a Python program that runs *tcpdump* and loads the data in one single text file in certain intervals. The stored files can be sent to the attacker using the transferring program we explained earlier in this section. The naming of the files are sequential so that the attacker can access them in the order they were generated.

Using *tcpdump* we were able to sniff and dump the data related to a user's visited website. The collected dump file can be analyzed using packet analyzers. Wireshark [25] is one of the most prominent network protocol analyzer tools. Figure 3 displays the *Wireshark* app debugging the obtained data from *tcpdump*. As can be seen in the figure the attacker can access the victim's visited website (or any other sensitive information send or received by the target machine).



```
root@kali:~# driftnet -i br0          Host 10.13.1.32 added to TARGET1
^X^X^Croot@kali:~# ^C
root@kali:~# driftnet -i eth0
gum xim 25 21:24:13 2016 [driftnet] warning                              to
bother with
gum xim 25 21:24:13 2016 [driftnet] warning                              to
bother with
gum xim 25 21:24:26 2016 [driftnet] warning                              to
bother with
gum xim 25 21:24:26 2016 [driftnet] warning                              to
bother with
gum xim 25 21:24:26 2016 [driftnet] warning                              to
bother with
gum xim 25 21:24:27 2016 [driftnet] warning                              to
bother with
gum xim 25 21:24:27 2016 [driftnet] warning                              to
bother with
gum xim 25 21:24:27 2016 [driftnet] warning                              to
bother with
gum xim 25 21:24:28 2016 [driftnet] warning                              to
bother with
gum xim 25 21:24:28 2016 [driftnet] warning                              to
bother with
gum xim 25 21:24:28 2016 [driftnet] warning: image data too small (43 bytes) to
```

Fig. 4: Intercepted image viewed by victim using Driftnet

To simulate these kinds of attacks, we used *Ettercap*. This tool allows the attacker to launch a variety of spoofing attacks to launch Man-in-the-Middle attack, and page or user redirection to a counterfeit host or service. During our attack we found both networks to be sustainable to different types of spoofing attacks. Figure 5 displays DNS spoofing attack as an example of attacked possible through Ettercap. In this experiment, we faked the DNS server for the targeted machine to redirect it to the attacker's website. We created a counterfeit website as shown in Figure 5 and by mapping the desired DNS to faked address, redirected the user to a counterfeit website (here an imitated Facebook page).

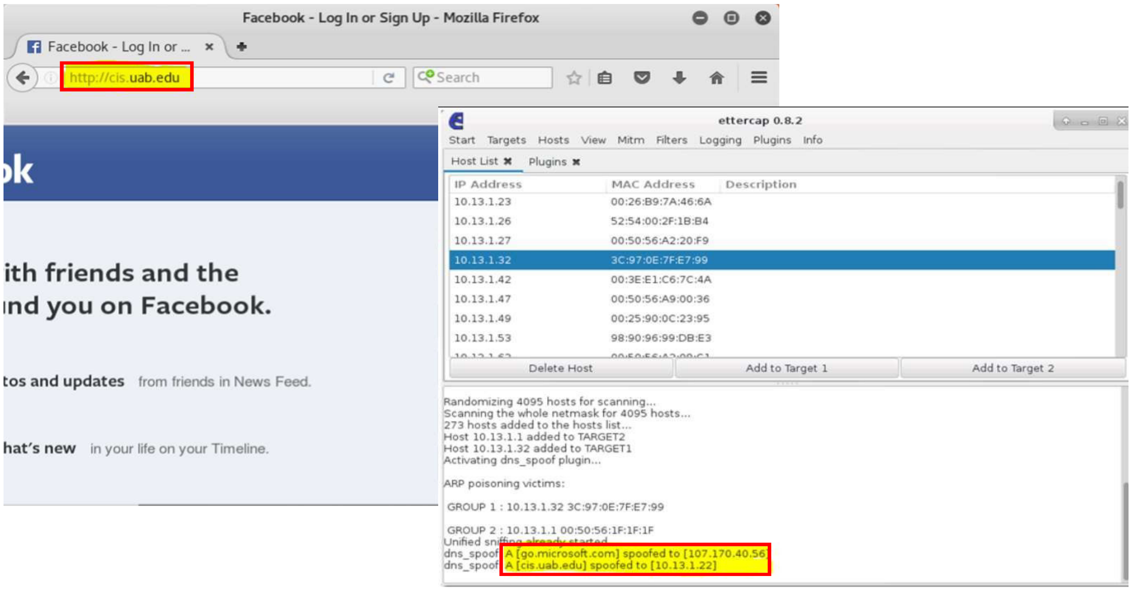
Other Attacks: In the case of illegitimate access to company premises, our gadget can potentially be used to launch a variety of attacks. Since the attacker using current implementation has turned to an insider node, the potential protective mechanisms such as firewall have already been bypassed and thereby the attack surfaces are limitless. For instance, while network foot-printing in a vast number of cases might not be viable from outside, it is more likely to work from the inside network using our

gadget. For instance, we further expanded our test to observe the reflection of our target network against a Dos attack. To run this test, we developed a simple packet generator script which randomly sends UDP packets to the random UDP ports. By adding 5 instances of our gadget to our test environment, we noticed a significant amount of load on the network. Clearly, on a larger scale with more devices attached to a network, as a distributed decentralized attack, can result in a significant UDP storm and accordingly network downtime.

4. DISCUSSION AND POSSIBLE DEFENCE MECHANISEMS

As discussed, the small size of the computationally powerful SBC allows the attacker to leave it in the network (temporarily or permanently) without getting noticed. One possible source of attack seems to be lack of enough physical security measures that permit the attacker to enter the targeted building while carrying such device. However, organizations may be reluctant to enforce policies for entering digital devices to the buildings due to the prevalence of these devices. A more feasible approach is to deploy best practices in network security to detect and perhaps prevent attacks from unmanaged devices inside the network. In this section, we discuss possible attack origins and protective mechanisms that can help to safeguard companies' digital assets, and avert such data breaches.

Fig. 5: DNS spoofing and redirecting user


Facebook - Log In or Sign Up - Mozilla Firefox
Facebook - Log In or ...
http://cis.uab.edu
Search
ok
ith friends and the
ınd you on Facebook.
tos and updates from friends in News Feed.
hat's new in your life on your Timeline.
ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List
Plugins
Delete Host
Add to Target 1
Add to Target 2

IP Address	MAC Address	Description
10.13.1.23	00:26:B9:7A:46:6A	
10.13.1.26	52:54:00:2F:1B:B4	
10.13.1.27	00:50:56:A2:20:F9	
10.13.1.32	3C:97:0E:7F:E7:99	
10.13.1.42	00:3E:E1:C6:7C:4A	
10.13.1.47	00:50:56:A9:00:36	
10.13.1.49	00:25:90:0C:23:95	
10.13.1.53	98:90:96:99:DB:E3	

```
Randomizing 4095 hosts for scanning...
Scanning the whole netmask for 4095 hosts...
273 hosts added to the hosts list...
Host 10.13.1.1 added to TARGET2
Host 10.13.1.32 added to TARGET1
Activating dns_spoof plugin...

ARP poisoning victims:

 GROUP 1 : 10.13.1.32 3C:97:0E:7F:E7:99

 GROUP 2 : 10.13.1.1 00:50:56:1F:1F:1F
Unified sniffing already started...
dns_spoof: A [go.microsoft.com] spoofed to [107.170.40.56]
dns_spoof: A [cis.uab.edu] spoofed to [10.13.1.22]
```

4.1. Physical Security

Organizations try to improve their security maturity and the resistance to attacks using different types of protective measures. Limiting accesses and using physical security is one way of deterring malicious outsiders. Physical security as one of the crucial components of security is being taught in the majority of related educational materials. A variety of researches investigated the physical security from different angle and context. Several literatures discussed the influence and effectiveness of the physical security in the industry [26, 27]. The traditional definition of the physical security was limited to protecting assets against perils such as flood, fire, and burglary. The modern definition of the term describes methods and techniques that are utilized to prevent or deter unauthorized physical accesses and thereby safeguard information.

Physical security as a barrier placed around the organization digital assets [28] provides an additional layer of security against malicious outsider and adversary insider. Many of the big (and even medium size) organizations control their doorways to avoid entrance of digital devices (e.g., laptops, cameras and networking devices) to minimize the risk associated with launching attacks and theft of information. However, the development of mobile phones and small computational devices seems to have made physical security more challenging. In this experiment, we showed that the attacker bypassed the physical security measures in the two mentioned organizations and took the Raspberry Pi device inside the network. The result of our experiments delineates the importance of revising the traditional definition of physical security and reconsidering the efficiency of it against such pocket-sized threats.

4.2. Network Security

Network Configuration. First protective mechanism lies on system configuration. At the very first step our suggested attacks were successfully launched as there was no mechanism to prevent an untrusted device to join the network. More specifically the result of this attack was promising due to the misconfiguration in upstream switch/router which allowed SBC to appear as a switch for redirecting traffic in the network. The attack can be prevented or be far less harmful if *"unauthorized switches"* configuration [29] was active in the upper layers of network. Means that the target network could be impervious to attack by activating *"unauthorized switches"*.

Attack Detection Script. While proper configuration can ideally prevent this type of attacks, depending on the environment conditions such configuration might not be applicable. This specifically can happen for the cases where a company involves considerable commuting in devices which makes the device tracking tough or even impossible to follow. Therefore in this section, we suggest use of scanning tools which can detect the presence of sniffing devices in the network.

We assume that the victim network is a switched Ethernet and traffic is not transferred on a shared media (e.g., hub, bus). In a switched network, there are several methods to sniff the network traffic. The simplest sniffer is set by configuring the network card into promiscuous mode and sniffing all traffic matching a targeted MAC address. Another type of sniffing relies on ARP poisoning, in which the attacker poisons the ARP cache and links the IP address of a legitimate user to its own MAC address, therefore, any packet intended to the IP address will reach the victim.

Several tools have already been developed to detect if a node on a network intercepts the traffic. *"Nmap"*[30] is a network security tool created to scan the network for administration purposes. *"Nmap"* sends a packet to the target host and receives the responses that can be used to assess different security parameters. *"Nmap"* has developed a script based on the method suggested in [31] to detect whether a network card is in promiscuous mode. This method creates fake ARP request packets that are sent to every node on the network. Nodes that are set in promiscuous mode respond to this ARP requests while other genuine nodes block the request. Another tool created by researchers is AntiSniff [32] that uses a variety of attacking techniques to not only recognize sniffing devices with the Ethernet cards in promiscuous mode but also to detect active attackers. Using such tools would heavily help the networks to detect and prevent attacks launch from an insider node.

5. CONCLUSION

Prior to the emergence of SBCs, to produce a spying gadget, attackers needed to have an advanced technical knowledge to build the hardware and program it according to the requirements, or to plug laptops into target networks to launch attacks, which could have been spotted. However, SBC devices made it easier for attackers to run networking attacks without getting noticed.

In this study, we have witnessed how a malicious adversary is able to launch an attack against an organization using off the shelf devices and tools. We showed how one can turn a small size SBC into a full-fledged network attacking gadget. We configured and installed the device in two organizations and showed examples of the possible network attacks. Given the popularity of SBC devices and their powerful resources we suggested deploying network monitoring schemes to detect and prevent such malicious network activities.

REFERENCES

[1] RASPBERRY PI FOUNDATION: RASPBERRY PI. Available at: https://www.raspberrypi.org/ (2017)

[2] BB Foundation: BeagleBone Black. Available at: http://beagleboard.org/BLACK/ (2017)

[3] Arduino LLC: Arduino Uno. Available at: https://www.arduino.cc/ (2017)

[4] Dave Neal: The Raspberry Pi is suddenly the third best-selling computer ever. Available at: https://www.theinquirer.net/inquirer/news/3006780/ the-raspberry-pi-is-suddenly-the-third-best-selling-computer-ever/ (2017)

[5] Eben Upton: TEN MILLIONTH RASPBERRY PI, AND A NEW KIT. Available at: https://www.raspberrypi. org/blog/ten-millionth-raspberry-pi-new-kit/ (2017)

[6] Guinard, D., Trifa, V.: Building the web of things: with examples in node. js and raspberry pi. Manning Publications Co. (2016)

[7] Zhao, C.W., Jegatheesan, J., Loon, S.C.: Exploring iot application using raspberry pi. International Journal of Computer Networks and Applications 2(1) (2015) 27–34

[8] IEEE: Healthcare based on IoT using Raspberry Pi. In: Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on, IEEE (2015)

[9] IEEE: Using of Raspberry Pi for data acquisition from biochemical analyzers. In: Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS), 2013 11th International Conference on. Volume 2., IEEE (2013)

[10] Abrahamsson, P., Helmer, S., Phaphoom, N., Nicolodi, L., Preda, N., Miori, L., Angriman, M., Rikkila, J., Wang, X., Hamily, K., et al.: Affordable and energy-efficient cloud computing clusters: the bolzano raspberry pi cloud cluster experiment. In: Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on. Volume 2., IEEE (2013) 170–175

[11] Tso, F.P., White, D.R., Jouet, S., Singer, J., Pezaros, D.P.: The glasgow raspberry pi cloud: A scale model for cloud computing infrastructures. In: Distributed Computing Systems Workshops (ICDCSW), 2013 IEEE 33rd International Conference on, IEEE (2013) 108–112

[12] IBM:IoT on Raspberry Pi. Available at: https://www.ibm.com/internet-of-things/partners/ raspberry-pi/ (2017)

[13] kickstarter: Sensly - A Smart, Portable Pollution Sensor For Your Home. Available at: https://www.kickstarter.com/projects/sensly/sensly-a-smart-portable-pollution-sensor-for-your/ (2016)

[14] Matt Richardson: Tutorial: Beer/Wine Fridge of Awesomeness. Available at: http://blog.initialstate.com/ tutorial-beerwine-fridge-of-awesomeness/ (2015)

[15] zipwhip: The world's first text enabled Raspberry Pi espresso machine. Available at: https://www.zipwhip.com/2013/06/18/zipwhip-text-enabling-of-the-delonghi-magnifica-espresso-machine/ (2013)

[16] Muniz, J., Lakhani, A.: Penetration testing with raspberry pi. Packt Publishing Ltd (2015)

[17] Djanali, S., Arunanto, F., Pratomo, B.A., Studiawan, H., Nugraha, S.G.: Sql injection detection and prevention system with raspberry pi honeypot cluster for trapping attacker. In: Technology Management and Emerging Technologies (ISTMET), 2014 International Symposium on, IEEE (2014) 163–166

[18] Mahajan, S., Adagale, A.M., Sahare, C.: Intrusion detection system using raspberry pi honeypot in network security. International Journal of Engineering Science 6(3) (2016) 2792

[19] Hu, Y., Sulek, D., Carella, A., Cox, J., Frame, A., Cipriano, K.: Employing miniaturized computers for distributed vul- nerability assessment. In: Internet Technology and Secured Transactions (ICITST), 2016 11th International Conference for, IEEE (2016) 57–61

[20] Ellen Nakashima and Andrea Peterson: Report: Cybercrime and espionage costs445 billion annually. Available at: https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html?utm_term=.8e7faf49a991 (2014)

[21] Offensive Security: Our Most Advanced Penetration Testing Distribution, Ever. Available at: https://www.kali.org/(2017)

[22] Offensive Security: Kali Linux - Raspberry Pi. Available at: https://docs.kali.org/kali-on-arm/ install-kali-linux-arm-raspberry-pi/ (2017)

[23] Chris Lightfoot: Driftnet. Available at: http://www.ex-parrot.com/~chris/driftnet/ (2017) 24.Bayles, W.J.: The ethics of computer network attack. Parameters 31(1) (2001) 44

[25] Wireshark: Wireshark. Available at: https://www.wireshark.org/ (2017) 26.Fennelly, L.: Effective physical security. Butterworth-Heinemann (2016) 27.Harris, S.: CISSP all-in-one exam guide. McGraw-Hill, Inc. (2010)

[28] Weingart, S.H.: Physical security devices for computer subsystems: A survey of attacks and defenses. In: International Workshop on Cryptographic Hardware and Embedded Systems, Springer (2000) 302–317

[29] Teare, D., Vachon, B., Graziani, R., Froom, R., Frahim, E., Ranjbar, A.: CCNP Routing and Switching Foundation Learning Guide Library:(ROUTE 300-101, SWITCH 300-115, TSHOOT 300-135). Cisco Press (2015)

[30] Gordon Lyon: NMAP. Available at: https://nmap.org/download.html/ (2017)

[31] Sanai, D.: Detection of promiscuous nodes using arp packets. A white paper from http://www. securityfriday. com Accessed in Aug (2002)

[32] Spangler, R.: Packet sniffer detection with antisniff. University of Wisconsin, Whitewater. Department of Computer and Network Administration (2003)

PREDICTING SECURITY CRITICAL CONDITIONS OF CYBER PHYSICAL SYSTEMS WITH UNOBSERVABLES AND OBSERVATION TIMES

Alessio Coletta[1, 2]

[1]Security and Trust Unit, Bruno Kessler Foundation, Trento, Italy
[2]Department of Information Engineering and Computer Science,
University of Trento, Italy

ABSTRACT

Cyber Physical Systems (CPS), like IoT and industrial control systems, are typically vulnerable to cyber threats due to a lack of cyber security measures and hard change management. Security monitoring is aimed at improving the situational awareness and the resilience to cyber attacks. Solutions tailored to CPS are required for greater effectiveness. This work proposes a monitoring framework that leverages the knowledge of the system to monitor in order to specify, check, and predict known critical conditions. This approach is particularly suitable to CPS, as they are designed for a precise purpose, well documented, and predictable to a good extent. The framework uses a formal logical language to specify quantitative critical conditions and an optimisation SMT-based engine that checks observable aspects from network traffic and logs. The framework computes a quantitative measure of the criticality of the current CPS system: checking how criticality changes in time enables to predict whether the system is approaching to a critical condition or reaching back a licit state. An important novelty of the approach is the capability of expressing conditions on the time of the observations and of dealing with unobservable variables. This work presents the formal framework, a prototype, a testbed, and first experimental results that validate the feasibility of the approach.

KEYWORDS

Security Monitoring, Detection and Prevention Systems, Critical Infrastructures, Cyber Physical Systems, SMT.

1. INTRODUCTION

Cyber Physical Systems (CPS) include Industrial Control Systems (ICS), Internet of Things, and critical infrastructures. They are composed by networked ICT devices that support the operation of physical entities and are employed in a large number of business- or safety-critical sectors. Due to their historical evolution, the progressive use of ICT technology without proper cyber security measures exposed CPS to vulnerabilities and threats typical of the ICT world [1-3]. CPS present many specific differences from standard ICT systems [4] that make general ICT security solutions seldom effective for CPS. Fortunately, the same peculiarities can also lead to better tailored solutions.

CPS are aimed at a specific purpose in a determined environment. As a consequence, the behaviour of their physical process is well designed and predictable to a good extent, and

Dhinaharan Nagamalai et al. (Eds) : CSEIT, NCS, SPM, NeTCoM - 2018
pp. 81–100, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81807

typically well documented. Also the behaviour of the cyber counterpart is predictable: a security operator may use such knowledge to specify critical conditions to be monitored. It is also possible to combine cyber and process aspects for a greater expressiveness and effectiveness.

While a number of the statistical and anomaly detection solutions are present in the literature and in the market, specification-based security monitoring approaches appear less mature. This work contributes in this regard presenting a framework that enables a security operator specifying which aspects of the CPS to observed, to express logical and quantitative critical condition about observed variables, and to detect and predict the criticality of the current state of the CPS.

The assumption that every parameter of the CPS can always be observed is not suitable to real cases. The main novelty of our approach is the ability to handle unobservable variables. Present work improves our previous results in that regard, defining a quantitative criticality notion whose changes in time predict both whether the CPS is getting closer to a critical condition and whether it is returning back to licit states. In presence of unobservable variables, the framework is capable of computing the criticality in the best and worst cases. It also computes the piece of missing information required for a more accurate result as a logical expression of unobservable values. Such information is provided to security operators as a guide for finding a refinement of the CPS state.

Present paper improves our previous works [5] and [6] in these aspects. Moreover, in this work the reasoning is untangled from observations, and it is possible to specify critical condition that depends on properties of observation times. This enables detecting illicit behaviours that depends on their time evolution properties.

As previous works, the framework does not need a full model of the CPS, which is very hard to achieve in real cases. It is based on passive observations of the CPS through the analysis of network traffic and logs, to be more suitable for the industrial sector where change management and shutdowns are nearly impossible in practice, especially when employed in critical infrastructures. The framework presents an expressive specification language and is agnostic to observation methods and attack models, thus it is suitable for detecting possible 0-days attacks. Section 2 describes related existing works and approaches. Section 3 shows an example to explain the main idea behind the cyber security monitoring framework. The same example is also used as a simulation scenario for our feasibility and performance testbed. Section 4 defines our proposed framework, while Section 5 presents our first working prototype and our first experimental results that validates the approach.

2. Related Work

One of the main source of vulnerability for CPS is the lack of security mechanisms in communication protocols, like authentication, authorisation, and confidentiality [2], [3]. Literature presents several secured version of control protocol, e.g. [7-9]. However, these security approaches rely on the possibility to redesign and replace at least some parts of the system, while for many industrial control systems downtimes and change management is not practical or affordable due to the high costs and risks related to any possible change. For this reason, redesign is often not an option and legacy components are often present. Passive and unobtrusive security measures are crucial for such CPS.

Intrusion Detection Systems (IDS) have been widely used in ICT security with good results. Signature-based IDS, like Snort [10], [11], are able to express *bad* IP packet that can be detected. Since cyber attacks are combinations of different licit-like actions and communications, signature-based IDS usually fall short in detecting complex attacks.

The *Anomaly-based* intrusion detection approach has proved effective for CPS cyber security [12-17]. [18] classifies anomaly-based IDS in two main categories:

1. *unattended techniques*, leveraging statistical models or machine learning to create a baseline representing licit behaviours that are compared with the run-time observations

2. *specification-based techniques*, for which a human ICS expert precisely defines what is licit or anomalous in a specification language, and the detection tool compares the state of the monitored system against such specifications.

The absence of human effort is a good advantage of the unattended techniques, but they suffer from high false positive rates which requires human effort to spot false alarms. Our work focuses on the specification-based approach, with the advantage that false positive rates are extremely low or even zero when enough knowledge of the system is available. The main drawback is the effort required to define the known critical conditions. However, CPS typically shows predictable and repeatable behaviours over time. Moreover, the design phase of a critical infrastructure is detailed and documented, providing valuable knowledge to be modelled. Nonetheless, some approaches to automatically derive specifications from the monitored system have proved effective, e.g. [19]. For this reason, specification-based techniques seem to be a good approach for developing security monitors for CPS.

Security monitoring has gained relevance in the Security Operation Centres (SOC) of big organizations and in the DevOps sector. Wide spread frameworks include Splunk [20], [21], Elasticsearch-Logstash-Kibana (ELK) [22-25], Grafana [26], and LogRythm [27]. Such tools continuously collect log events and time series data (e.g. cpu load, memory consumption, etc.). Security operators can customise visualisation dashboards of such information to spot anomalous vs. normal behaviours in a graphical way. Moreover, security operators can define custom alarms specifying queries on the collected data and events, for instance to detect known indicator of compromise (IoC). The possibility to define alarms is somehow similar to our notion of critical condition described in this paper. Unlike our proposed framework, such tools allow queries only on observable data and do not offer a notion of proximity / proximity range from criticality.

Nai et al. [28-30] developed a specification-based Intrusion Detection and Prevention System methodology specific for SCADA systems that is not based on specific attack models and can detect 0-day attacks. The methodology allows combining the knowledge of the physical process with the cyber behaviour to be monitored, and is further extended in [5] with a greater expressiveness and more effective computation methods. Our present work further improves the same approach. The novelty of this work consists in (1) using observation times untangled from reasoning (2) dealing with unobservable aspects of the system for a greater expressiveness and feasibility in real cases (3) using real-time knowledge refinements from human operators (4) guiding the operator towards better refinements (5) computing and monitoring a the criticality of the CPS state in the best and worst case to predict whether it is getting closer to critical conditions or returning back to licit states even in presence of unobservable variables.

3. A MOTIVATING EXAMPLE

This section presents an example of a simplified chemical process and its control system and logic. This scenario serves both to explain our proposed approach and as simulation scenario to test our prototype and validate the results. Figure 1 shows the components of the chemical process.

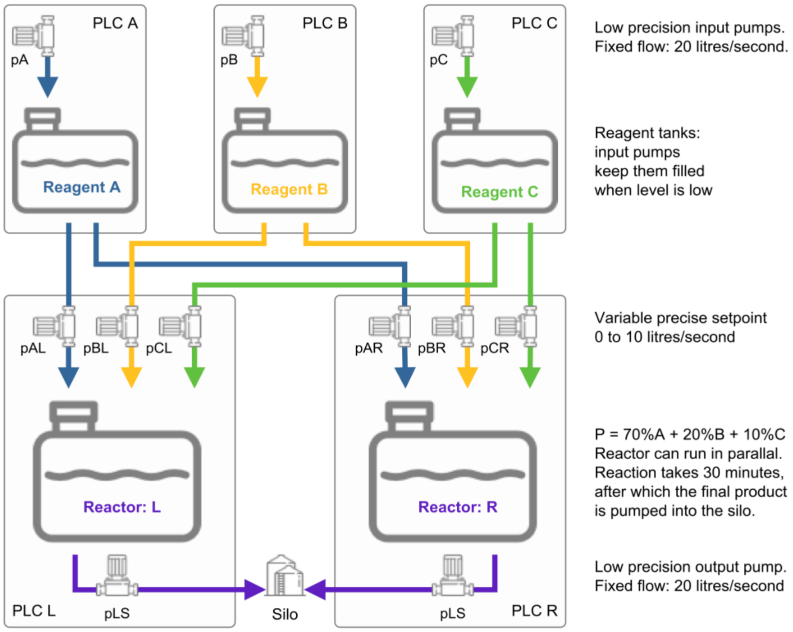


Figure 1. Simple chemical process use case.

Process overview. A pharmaceutical company produces a chemical product P from three reagents A, B, and C. All chemical reagents and products are liquids. The process begins filling a reactor with reagents A, B, and C with concentrations of respectively 70%, 20%, and 10% using precise pumps. Assume these proportions are part of a patented secret process. More than one reactor can be used in parallel: this example considers two reactors L and R. When the reactor L (or R) is filled, the chemical reaction takes 30 minutes, after which the content of the reactor is moved to the final product silo S using output pumps *pLS* (or *pRS*). Input pumps pA pB pC fill the tanks containing reagents A B C when the level of the tank is lower than a threshold. Pumps *pAL*, *pBL*, *pCL* and *pAR*, *pBR*, *pCR*, which are used to mix reagents in the correct proportions, are required to be precise: a numerical setpoint specifies the pump flow (in this example from 0 to 10 litres per second). Pumps *pA*, *pB*, *pC* and output pumps *pLS*, *pRS* do not need to be precise, the pump flow is fixed to 20 litres per second, and they can only be turned on and off.

Cyber components. The control of the process is based on the level sensors: each tank, reactor, and silo have a sensor that measures the *level of the content*. The employed actuators are: mixing pumps *pAL*, *pBL*, *pCL*, *pAR*, *pBR*, *pCR*, which can be operated setting a *variable setpoint* and can be switched *on/off*; other pumps *pA*, *pB*, *pC*, *pLS*, *pRS* which can only be turned on/off.

Sensors and actuators are wired to Programmable Logic Controllers (PLC), connected to the same TCP/IP-based Process Control Network (PCN):

- PLC A, PLC B, and PLC C read level sensors of resp. tanks A, B, C and control the on/off status of input pumps A, B, C.
- PLC L reads the level of reactor L and controls the setpoint of pumps *pAL*, *pBL*, and *pCL* and the on/off status of *pLS*. Analogously for PLC R.

A SCADA server, connected to the PCN, controls the chemical process sending read and write network command to the PLCs through an industrial control protocol like Modbus [31]:

- it constantly reads control parameters from the PLCs using active polling at a constant frequency, specified in its configuration;
- it automatically operates the process implementing a control logic, sending write commands to the PLCs when certain predefined conditions occur;
- it provides a Human Machine Interface (HMI) component, which shows the current values of the process and enables operators to manually send control commands to the PLCs.

The SCADA server is the only system that is allowed to send read and write commands to PLC, as a result of automatic or manual operations.

Specifying criticalities from the knowledge of the process. An attacker may compromise the SCADA to gather and exfiltrate secret process data off the PCN or to damage the process. While any network message not originated from the SCADA can be easily detected as illicit, read and write commands sent from a compromised SCADA are identical to the licit ones from the network signature perspective. Thus, signature-based IDS fail short to detect such attacks. Modbus-like control protocols, vastly used in existing industrial control systems, present no authentication/authorization mechanisms. Hence, the attacker can initiate Modbus TCP connections from the compromised SCADA server to any PLC to illicitly operate the process.

Suppose the attacker sends read commands and collects the response values to exfiltrate secret data, like the reaction proportions and timings. This attack can be detected comparing the total number of read messages with the one expected from the SCADA server configuration. Let RF_p be the number of read commands from the SCADA server to PLC p in the time unit, with $p \in \{A, B, C, L, R\}$. This value can be easily observed using network traffic analysis and deep packet inspection tools like Wireshark [32]. Let rf_p be the constant number of read commands per second to the PLC P in the SCADA server configuration, called polling frequency. The critical condition corresponding to the read attack is then

$$RF_A \neq rf_A \lor RF_B \neq rf_B \lor RF_C \neq rf_C \lor RF_L \neq rf_L \lor RF_R \neq rf_R \tag{1}$$

In this work RF_p are called *variables* of interest of the monitored CPS. Each variable is bound to an observation method, in this case to network packet inspection that counts read commands.

Suppose the attacker sends write commands with random setpoints to the mixing pumps to alter the proportions and to corrupt the chemical reaction. Let PS_p be the variables representing the last observed setpoint sent to the PLC controlling the pump p. Again, it is easy to observe PS_p with deep packet inspection of Modbus commands on the PCN. It is possible to detect such attack comparing those values with the expected proportions, expressed by the following critical condition:

$$(2 \cdot PS_{pAL} \neq 7 \cdot PS_{pBL} \land PS_{pBL} \neq 2 \cdot PS_{pCL}) \lor (2 \cdot PS_{pAR} \neq 7 \cdot PS_{pBR} \land PS_{pBR} \neq 2 \cdot PS_{pCR}) \tag{2}$$

Unobservable variables. The aim of industrial control systems is to automatically operate sensors and actuators to implement a specific process. In our example, automatic control rules are implemented by the SCADA server. Figure 2 shows the state-based rules for sensors and actuators that control the reaction, while Table 1 shows the rules to control the other components.

Table 1. Example of automatic operation rules.

every 500 ms	→	read *all* sensors	
if $Level_X < h_X$	→	set $pX = \mathbf{off}$	for $X \in \{A, B, C\}$
if $Level_X > l_X$	→	set $pX = \mathbf{on}$	for $X \in \{A, B, C\}$

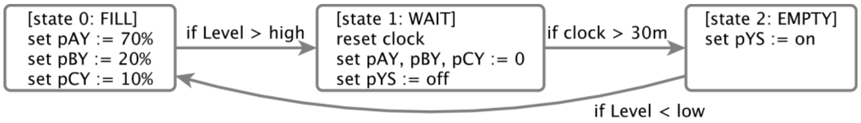


Figure 2. Automatic reactor control statechart ($Y \in \{L, R\}$).

Suppose the attacker sends on/off command to the pLS pump that does not comply with the control logic. The following critical condition detects such attack:

$$((S_L = 0 \vee S_L = 1) \wedge pLS = \text{on}) \vee (S_L = 2 \wedge pLS = \text{off}) \tag{3}$$

where variable pLS is the observed on/off payload of the write command and variable S_L is the state of the control logic of reactor L. Notice that S_L is necessary to express critical condition (3), but it is inherently unobservable because it is the hidden state of a control program implemented in the SCADA server. While S_L is always unobservable, any variable may become temporarily unobservable, e.g. when it is bound to a malfunctioning sensor. This example shows that the assumption that all the variables are always observable is not feasible with real cases, and that critical conditions of interest may need to refer to unobservable variables. Next sections show how our framework is capable of dealing with them.

Observation time in critical specifications. Some attacks can be detected observing how the CPS behaves in time. According to Figure 2, when a turn-off command and later a turn-on command are sent to pump pLS (i.e. a transition from state 1 to 2 occurs), then the two write commands must be observed with at least 30 minutes time difference, but not much more than that. Assuming 1 minute tolerance in the execution of the control logic, the following critical condition detects attacks that turn off pLS too early or too late:

$$\neg(pLSon.t < pLSoff.t \quad \rightarrow \quad 30m < pLSoff.t - pLSon.t < 31m) \tag{4}$$

where $pLSon$ and $pLSoff$ are boolean variables bound to the observation of respectively on and off write commands to pump pLS.

Refinements. Detecting if the current state of the CPS is critical w.r.t. a critical specification may be impossible in presence of unobservable variables. A human operator can provide the monitor with a refinement, i.e. a logical expression of further knowledge. For instance, a process operator who supervises the production knows whether a reaction started, i.e. if $S_L = 1$. For this reason, the operator can alternatively provide our monitor with the refinement $S_L = 1$ or the refinement $S_L = 0 \vee S_L = 2$.

Similarly, unobservable variables can express human intentions, which can be valuable knowledge to a monitoring framework. Assume an operator sends licit commands for maintenance purpose not compliant with the control logic of the CPS. Critical conditions (2) (3) (4) do not discriminate such licit commands from the attacker's ones. Each condition ϕ can be replaced with $\neg M \rightarrow \phi$, where M is an unobservable boolean variable representing that the CPS is intentionally manually operated. This way, an operator provides the refinement $M = \mathbf{true}$ when the maintenance activity begins and $M = \mathbf{false}$ when it ends, and his operations are not detected as illicit.

When it is not possible to discriminate the criticality of the current state of the CPS due to unobservable variables, our monitor is capable of computing an *assisted check*, i.e. a logical expression that a human operator can evaluate in order to provide a minimal valuable refinement. Next sections show how the monitor computes this expression using its logical reasoning core.

Predictiveness. Besides discriminating whether the current state of the CPS is critical, our monitor also predicts if the system is getting closer to a critical condition. To this aim, the monitor computes a notion of distance of the current CPS state from a critical condition. When the current state is non-critical, monitoring how the distance from the critical condition changes in time tells if the system is reaching that criticality. On the other hand, when the state is critical, it is possible to monitor the distance from the border of the criticality, i.e. how far the CPS is from returning to a non-critical state.

In our example, if the current CPS state satisfies the critical condition (1), its criticality measure represents how the observed polling differs from the expected one. On the other hand, if the current state is not critical w.r.t. (4), i.e. the observation time between on and off commands is between 30 and 31 minutes, the proximity from the criticality represent how the observation time difference is close to the critical boundaries 30 or 31.

Unobservable variables imply that the current state is not fully known, hence the criticality or the proximity can be evaluated on a range of possible values. The following sections shows how our monitor computes the criticality/proximity range in the best and worst case.

4. THE MONITORING FRAMEWORK

The proposed monitoring framework passively runs in parallel with the monitored CPS. It continuously observes the current state of the CPS and checks the specified *critical conditions*. Figure 3 depicts the main structure of the framework.

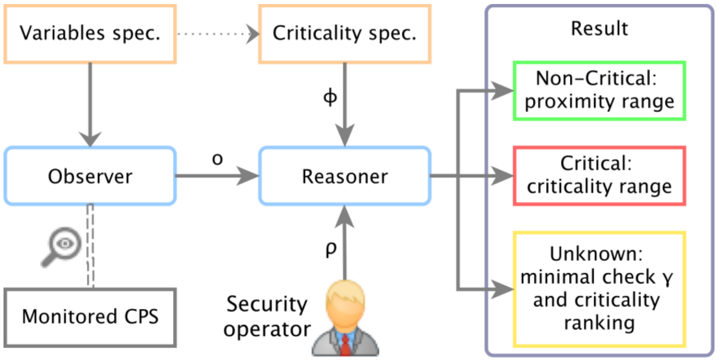

Variables spec.
Criticality spec.
Result
ϕ
Non-Critical: proximity range
Observer
o
Reasoner
Critical: criticality range
ρ
Unknown: minimal check γ and criticality ranking
Monitored CPS
Security operator

Figure 3. Structure of the real-time monitoring framework.

The first step is to identify the aspects of the CPS, called *variables*, that are necessary to express the critical conditions. In real cases, the assumption that it is always possible to retrieve the value of all the variables is too strict and unfeasible. Thus, a variable can be *observable* or *unobservable*, either temporarily or permanently. Unobservable variables complicate the framework but allow for a greater expressiveness and practical feasibility. There are three main cases in which a variable is considered unobservable:

1. a variable bound to the value of a malfunctioning sensor that cannot provide its value;
2. a variable bound to a parameter of the CPS which is required to express the critical condition but that can never be observed by design, e.g. the temperature of a gas in a point where no thermometer has been installed;
3. any aspect of the monitored system that is inherently unobservable, e.g. the intention of a human operator that acts without specifying his actions in advance.

The monitoring framework is composed by two main components: the *observer* and the *reasoner*.

The former continuously observes the CPS, e.g. analysing the traffic on the control network, in order to retrieve the value of the observable variables. The latter checks the current state of the CPS against the set of known critical conditions.

The input to the observer consists of the *specification of variables*, which enumerates the variables of interest and their properties. Precisely it defines for each variable:

1. the *name*, used as an identifier in the specification of critical conditions
2. the *type*: boolean, integer, or real
3. an optional *range constraint*, i.e. lower and upper bounds
4. an optional *observation method*: how the observer captures the value of the variable through network or log analysis. When the method fails or is not provided, the variable is considered unobservable.

Our threat model assumes the integrity of the observed values: if an attacker takes the complete control of the network it might compromise the effectiveness and correctness of our monitoring framework. However, this assumption is typical of security monitoring solutions cited in Section 2. In real cases, such approach is still valid provided that a sufficient large number of variables are observable and effective critical conditions are specified. In this way the likelihood that an attacker is able to compromise enough values to make the monitor ineffective is low.

Iteratively the reasoner receives the observation o and a critical condition ϕ and checks o against ϕ. If the critical condition only contains observable variables, the reasoner is always able to tell whether the CPS has reached the criticality or not. In presence of unobservable variables, it might be impossible to discriminate whether the CPS is in a critical state only from observations.

The reasoner is also able to take as input some further information about the CPS state in form of a logical assertion, hereafter called *refinement* and denoted by ρ. Refinements are typically provided by human operators to give the monitor additional information about unobservable variables.

When the reasoner is unable to determine whether the current state satisfies a critical condition, it computes the minimal condition of unobservable variables that is necessary to determine that the system state is not critical (γ in Figure 3). The minimal condition γ is hereafter called *assisted check*, because it helps security operators figure out the missing unobservable information. In other words, the assisted check can guide operators to provide better knowledge refinements.

4.1. Specification of Variables and Critical Conditions

Let $\mathcal{V}$ denote the set of variables, whose type can be boolean, integer, or real, and let $range(v)$ denote the range constraint of v defined in the variable specification. Boolean variables range on the set $\{0,1\}$, with both the boolean and the numeric meaning, in order to be able to use boolean and numeric variables in the same arithmetic expressions. As a consequence, all variables in $\mathcal{V}$ range on $\mathbb{R}$.

An *observation* is a partial mapping from variables to timestamped values. Formally, let $V \subseteq \mathcal{V}$ be a subset of variables. An observation is a pair of functions $o: V \to \mathbb{R}$ and $o^t: V \to \mathbb{T}$ such that $o(v) \in range(v)$ for each variable $v \in V$. The notation $dom(o)$ denotes its domain V.
When clear from the context we use o to indicate the pair (o, o^t).

A *state* s of the monitored CPS is a total observation function that maps all variables to timestamped values, i.e. an observation such that $dom(s) = \mathcal{V}$. Given an observation o, we define

$$\mathcal{S}(o) = \{s \in \mathcal{S} \mid \forall v \in dom(o): s(v) = o(v) \wedge s^t(v) = o^t(v)\}$$

as the set of states that coincide with s.

The reasoner regularly receives the most current observation o from the observer. If $v \notin dom(o)$ variable v is unobservable, otherwise the value $o(v)$ was observed at time $o^t(v)$. This allows reasoning about the actual time the value was observed, crucial to express time relationships about observations of different variables.

A *critical condition formula* is defined by the grammar:

$$\begin{array}{lll} X & ::= v \mid v.t \mid \text{now} & \text{value or timestamp of variable observation} \\ \phi & ::= a_1X_1 + \cdots + a_nX_n \bowtie b \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi & \end{array} \tag{5}$$

where $v \in \mathcal{V}$, now $\notin \mathcal{V}$ is a distinct symbol from variables, $a_i, b \in \mathbb{R}$, $\bowtie \in \{=, \neq, <, \leq, >, \geq\}$. The set of variables occurring in a formula ϕ is denoted by $var(\phi)$.

A critical condition formula is a boolean combination of linear inequalities of values and timestamps of observation of variables. It expresses a property of the most current observation of the CPS state, where both observable and unobservable variables may occur in a formula. We use the standard interpretation of formulae over assignments.

Definition 1. Given an observation o, a point in time τ, and a formula ϕ such that $var(\phi) \subseteq dom(o)$, the observation o *satisfies* (or *models*) at time τ the formula ϕ, denoted by $o, \tau \models \phi$, when recursively:

$$[\![v]\!]_{o,\tau} = o(v) \quad [\![v.t]\!]_{o,\tau} = o^t(v) \quad [\![\text{now}]\!]_{o,\tau} = \tau$$

$$\begin{array}{rll} o,\tau \models \sum_i a_i X_i \bowtie b & \text{iff} & \sum_i a_i\, [\![X_i]\!]_{o,\tau} \bowtie b \\ o,\tau \models \neg\phi & \text{iff} & o,\tau \not\models \phi \\ o,\tau \models \phi_1 \wedge \phi_2 & \text{iff} & o,\tau \models \phi_1 \; and \; o,\tau \models \phi_2 \\ o,\tau \models \phi_1 \vee \phi_2 & \text{iff} & o,\tau \models \phi_1 \; or \; o,\tau \models \phi_2 \end{array}$$

The set of states satisfying a formula ϕ is denoted by $\mathcal{S}(\phi)$.

Our framework uses state formulae to define the known critical conditions of the monitored CPS. The reasoner iteratively receives from the observer the most recent observation o, and try to evaluate if $o, \tau \vDash \phi$ for each critical condition ϕ where τ is the current time. In this way, the reasoning time can be different from the observation time, and the observation time for each variable can be different.

Notice that in the general case it is not possible to check if $o, \tau \vDash \phi$ due to unobservable variables. Formally, if $var(\phi) \subseteq dom(o)$ then $o, \tau \vDash \phi$ can be simply checked using semantics in **Definition 1** defined by induction on the syntax of the formula. Otherwise, it may not be possible to check its satisfiability. The following section describes how the reasoner handles the satisfiability of critical conditions in order to detect when critical condition occurs and to measure the criticality of the current state of the CPS (or its distance from the critical condition).

4.2. The Observer

The proposed monitoring framework is agnostic to actual observation methods. This section describes assumptions and give examples of possible methods feasible to cyber physical systems. The critical specification language defined in (5) is able to express the observed value and the observation time of variables. An observation point is timestamped value (t, x), with the meaning that value x was actually observed at that time t. Variable specifications associate each variable v with an observation method, i.e. any procedures that returns the most recent observation point. The method may fail to represent unobservable variables. In this case the Observer does not pass any observation point for that variable to the Reasoner.

The reasoning time, i.e. the time the Reasoner computes the criticality of the current state, generally does not coincide with observation time. This is typical in CPS, where the supervisor server polls PLCs to collect the process values independently from any possible analysis. Moreover, this enables passive observations using application logs and/or network traffic analysis, as in our testbed described in Section 5. For this reason, the observer and the reasoner must be untangled. Established continuous monitoring solutions, largely employed in the industry, maintain the data collection separated from the analysis using efficient storage in the middle. We use the same approach to keep the observer and the reasoner untangled, since it proved to be very effective and scalable. Observations are stored in timeseries databases, i.e. in databases that provide efficient methods to store and retrieve timestamped data with an ad-hoc query language.

In this work we assume that all the observations are stored in one or more timeseries databases that represent application logs and parsed network traffic dumps. In particular, the observations in the use case described in Section 3 are the parsed Modbus-like messages dumped from the Process Control Network of the form:

```
READ <SESSIONID> <PLC> <PARAMETER>
READ_RESPONSE <SESSIONID> <PLC> <PARAMETER> <RETURN VALUE> <RESPONSE STATUS>
WRITE <SESSIONID> <PLC> <PARAMETER> <NEW VALUE>
WRITE_RESPONSE <SESSIONID> <PLC> <PARAMETER> <RESPONSE STATUS>
```

Table 2 shows an example of data stored in the database that represents messages observed in the PCN.

Table 2. Example of observations of PCN traffic as parsed network messages stored in a timeseries DB.

Time	Msg Type	Session	PLC	Parameter	Value	Status
t1	WRITE	342	PLC_A	pump_onoff	1	null
t2	WRITE_RESPONSE	342	PLC_A	pump_onoff	null	OK
t3	READ	343	PLC_C	pump_onoff	null	null
t4	READ_RESPONSE	343	PLC_C	pump_onoff	1	OK
t5	READ	345	PLC_L	tank_level	null	null
t6	READ_RESPONSE	345	PLC_L	tank_level	null	ERROR

The observation method of variables can be implemented using a query to the timeseries database that returns at most one timestamped value. For instance, the observation method of variable $pLSon$ occurring in (4) can be implemented with the query

```
SELECT time, value FROM pcn_db
WHERE msg_type="WRITE" AND plc="PLC_L" AND parameter="pump" AND value="1"
LIMIT 1
```

which retrieves only the time and value attributes of the most recent entry (`LIMIT 1`) that refers to a write command to pLS with payload value is 1 (i.e. on) from the database containing PCN messages such that the PLC.

4.3. The Reasoner

Figure 4 depicts the behaviour of the reasoner. At each iteration it receives two inputs: an observation o from the observer and an optional information refinement ρ from the operator.

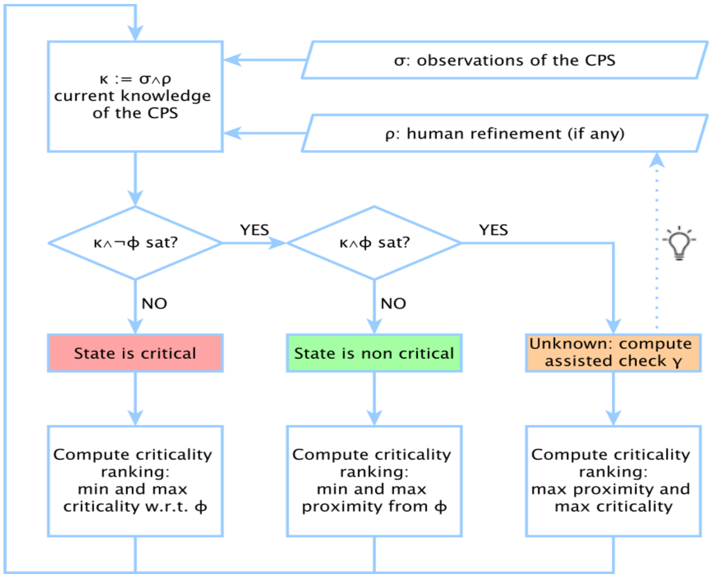


Figure 4. Reasoner flow chart given criticality ϕ.

The core of the reasoner is a Satisfiability Modulo Theory (SMT) logical engine. Thus, the reasoner computes a formula that is the equivalent of the observation in logical terms as follows:

$$\sigma_o := \bigwedge_{v \in dom(o)} v = o(v) \wedge v.t = o^t(v)$$

where v and $v.t$ are distinct symbols for the value and timestamp of variable v. Notice that unobservable variables, i.e. variables not defined in o, do not appear in σ_o. In the following we use σ to denote σ_o since the observation o is fixed for each iteration of the reasoner.

The refinement is a logical assertion that enables an operator to provide the reasoner with any further information about unobservable variables. It there is no such information then $\rho \coloneqq \mathbf{true}$. The logical expression $\kappa \coloneqq \sigma \wedge \rho$ represents all the information that the reasoner knows about the current CPS state s, i.e. that $s \in \mathcal{S}(\kappa)$.

4.3.1. Criticality Detection

To discriminate if the CPS is currently in a critical state the reasoner checks whether the formulae $\kappa \wedge \phi$ and $\kappa \wedge \neg\phi$ are *satisfiable* using an SMT solver. Three cases are possible:

1. The system *is in a critical state*, regardless unobservable values, or equivalently $\mathcal{S}(\kappa) \cap \mathcal{S}(\phi)^C = \emptyset$. This is equivalent to checking whether the formula

$$\kappa \wedge \neg\phi \text{ is unsatisfiable.} \tag{6}$$

2. The system *is not in a critical state* regardless unobservable values, or equivalently $\mathcal{S}(\kappa) \cap \mathcal{S}(\phi) = \emptyset$. Similarly, this is equivalent to checking whether formula

$$\kappa \wedge \phi \text{ is unsatisfiable.} \tag{7}$$

3. If both formulae in (6) and (7) are satisfiable, then $\mathcal{S}(\kappa) \cap \mathcal{S}(\phi) \neq \emptyset$ and $\mathcal{S}(\kappa) \setminus \mathcal{S}(\phi) \neq \emptyset$. In other words, it is not possible to establish from κ whether the actual CPS state is critical, because this depends on some unobservable values not in κ.

In the first and second cases the reasoner can compute an estimation of the criticality and proximity of the current state respectively, as explained in Section 4.3.2.

In the third case κ does not contain enough information to discriminate whether the CPS is in critical state. Since the observation σ does not contain information about unobservables by definition, the only way to obtain a more precise result is to provide a more informative refinement ρ.

In practical cases it can be hard for a human operator to understand which piece of information is missing. To this aim, the reasoner is able to calculate a condition, hereafter denoted by γ, that is sufficient to guarantee the non-criticality of the current CPS state given κ and ϕ, i.e. such that $\kappa \wedge \gamma \wedge \phi$ is not satisfiable. Our monitoring solution provides a human operator with γ as a guide for better refinements. Indeed, the operator can try verifying if γ holds, or at least if some of its sub-formulae. This way the operator may acquire some information, make educated assumptions on unobservable variables, and provide it back to the reasoner in the form of a more informative refinement. For this reason, the reasoner acts as an assistant to the human operator, and the formula γ is called *assisted check*. In practical cases, the operator must be able to handle the complexity of the assisted check, thus it is crucial that the size of γ is as small as possible.

We use the notion of interpolant, provided by most SMT solvers, to compute the minimal assisted check γ. Given two mutually unsatisfiable formulae α and β, a *Craig interpolant* (denoted by $interpolant(\alpha, \beta)$) is a formula η such that $var(\eta) \subseteq var(\alpha) \cap var(\beta)$ and formulae $\alpha \rightarrow \eta$ and $\eta \rightarrow \neg\beta$ are valid. In other words, the formula η is an explanation for the mutual unsatisfiability that uses only the variables that are common in α and β.

Our framework also uses syntactic simplification of logical expressions that most SMT solvers provide. Hereafter $simplify(\alpha)$ denotes the computation[1] of a possibly simpler expression equivalent to α. Since formulae $\kappa \wedge \neg\phi$ and $\kappa \wedge \phi$ are mutually unsatisfiable, the assisted check can be defined as

$$\gamma \coloneqq interpolant(simplify(\kappa \wedge \neg\phi), simplify(\kappa \wedge \phi))$$

4.3.2. Predictiveness: State Criticality and Proximity from Conditions

In this section we define a notion of distance from a critical condition ϕ. Given a set X, a function $d: X \times X \to \mathbb{R}$ is called *premetric* if both $d(x,y) \geq 0$ and $d(x,x) = 0$ for all $x, y \in X$. Given a set X, a premetric function $d: X \times X \to \mathbb{R}$ is called a *metric* if for all $x, y, z \in X$: (i) $d(x,y) = 0$ iff $x = y$, (ii) $d(x,y) = d(y,x)$, (iii) $d(x,y) \leq d(x,z) + d(z,y)$. The pair (X,d) is called *metric space*.

We use the following well known result. Let (X,d) be a metric space. The function $D: 2^X \times 2^X \to \mathbb{R}$ defined as

$$D(A,B) = \inf_{a\in A,\, b\in B} d(a,b)$$

is a premetric.

Provided any enumeration of the CPS variables $v \in \mathcal{V}$ and their observation times $v.t$, the set of states $\mathcal{S}$ can also be seen as a vector of $\mathbb{R}^{2n}$, where n is the number of variables. Thus, any metric d on $\mathbb{R}^{2n}$ is a metric on $\mathcal{S}$ that induces a premetric D on $2^{\mathcal{S}}$. In the following we use the premetric D to capture the notion of proximity from critical condition.

Table 3.Example of metrics.

$m_V(s,t)$	$= \sum_{v\in V} \lvert s(v) - t(v) \rvert$	Manhattan distance (i. e. L_1 metric on $\mathbb{R}^n$)
$wm_V(s,t)$	$= \sum_{v\in V} w_v \lvert s(v) - t(v) \rvert$	Weighted Manhattan distance, $w_v \geq 0$
$nm_V(s,t)$	$= \frac{1}{\#V} \sum_{v\in V} \frac{\lvert s(v)-t(v) \rvert}{v_{\max}-v_{\min}}$	Normalised Manhattan distance (defined if $v_{\min}, v_{\min} \in \mathbb{R}$)
on $h_V(s,t)$	$= \#\{v \in V \mid s(v) \neq t(v)\}$	Hamming distance
$wh_V(s,t)$	$= \sum_{\substack{v\in V \\ s(v)\neq t(v)}} w_v$	Weighted Hamming distance, $w_v \geq 0$
$nh_V(s,t)$	$= \frac{1}{\#V} h_V(s,t)$	Normalised Hamming distance

where $s, t \in \mathcal{S}$, $V \subseteq \mathcal{V}$, $v_{\min} = \min(range(v))$, $v_{\min} = \max(range(v))$.

Our framework requires to specify for each critical condition ϕ an associated metric d. Recall that at runtime the formula $\kappa \coloneqq \sigma \wedge \rho$ represents what the reasoner knowns about CPS variables. The *proximity* of the current CPS state from the critical condition ϕ is defined as

$$D(\mathcal{S}(\kappa), \mathcal{S}(\phi)) = \inf_{\substack{s\vDash\kappa \\ t\vDash\phi}} d(s,t)$$

hereafter denoted by $D(\kappa, \phi)$.

[1] As a reference, our prototype uses Z3 [33] with the tactic `(then simplify ctx-simplify ctx-solver-simplify)`.

Previous definition is parametric w.r.t. the chosen metric on the set of states $\mathcal{S}$, and the actual choice function depends on the application. Table 3 shows possible examples of metrics. For instances, the Hamming distance captures the number of variables that differs, while the Manhattan distance captures each variable variation, and this choice allows for a qualitative vs. quantitative proximity notion.

When the current CPS state is critical, i.e. $\kappa \wedge \neg\phi$ is unsatisfiable, proximity $D(\kappa, \phi) = 0$. When the CPS is in a critical state, i.e. when $\kappa \wedge \phi$ is unsatisfiable, computing the proximity from the critical condition $D(\kappa, \phi)$ is an optimisation problem on linear constraints, since critical formulae κ and ϕ represent boolean combination of linear inequalities. Our framework uses SMT-based optimisation techniques, such as the one provided by the Z3 prover [33] and by OptiMathSat [34].

Due to unobservable variables, κ does not represent one system state but a set of possible states. It is possible to evaluate the proximity from ϕ or the criticality w.r.t. ϕ in the best and worst possible cases. The *criticality range* of κ with respect to ϕ is the pair $C(\kappa, \phi) = (C_{\min}, C_{\max})$ defined as

$$\begin{aligned}
C_{\min}(\kappa, \phi) &:= \begin{cases} -D_{\max}(\kappa \wedge \neg\phi, \phi) = -\sup\limits_{s \vDash \kappa \wedge \neg\phi} \inf\limits_{t \vDash \phi} d(s,t) & \text{if } \kappa \wedge \neg\phi \text{ is satisfiable} \\ D_{\min}(\kappa \wedge \phi, \neg\phi) = \inf\limits_{s \vDash \kappa \wedge \phi} \inf\limits_{t \vDash \neg\phi} d(s,t) & \text{otherwise} \end{cases} \\
C_{\max}(\kappa, \phi) &:= \begin{cases} D_{\max}(\kappa \wedge \phi, \neg\phi) = \sup\limits_{s \vDash \kappa \wedge \phi} \inf\limits_{t \vDash \neg\phi} d(s,t) & \text{if } \kappa \wedge \phi \text{ is satisfiable} \\ -D_{\min}(\kappa \wedge \neg\phi, \phi) = -\inf\limits_{s \vDash \kappa \wedge \neg\phi} \inf\limits_{t \vDash \phi} d(s,t) & \text{otherwise} \end{cases}
\end{aligned} \tag{8}$$

The meaning of previous definition is explained in, Table 4, which summarises the possible combinations of values of $C(\kappa, \phi)$, as a result of the logic in Figure 4 and definitions (8).

Table 4. Meaning of the results of the Reasoner.

$C_{\min}$	$C_{\max}$	$\kappa \wedge \neg\phi$	$\kappa \wedge \phi$	**Meaning**
negative	negative	sat	unsat	State is non critical regardless unobservables. $-C_{\min}$ and $-C_{\max}$ are the best and worst proximity values to ϕ
negative	positive	sat	sat	State could be critical or not depending on unobservables. Assisted check returned for further refinement. $-C_{\min}$ is the proximity to ϕ in the best case and $C_{\max}$ is the criticality (i.e. proximity to $\neg\phi$) in the worst case.
positive	positive	unsat	sat	State is critical regardless unobservables, $C_{\min}$ and $-C_{\max}$ are the worst and best criticality values (i.e. proximity to $\neg\phi$)

$C_{\max}$ and $C_{\min}$ can be positive, negative, or zero. A positive value indicates a state is critical w.r.t. ϕ, and the value represents how far the state is from licit state (i.e. states that does not satisfy ϕ). A negative value indicates the state is non-critical w.r.t. ϕ, and its absolute value represents how far it is from ϕ. Zero means the state is on the border of the critical states set.

Figure 5 shows the pseudo-algorithm to compute the criticality $C(\kappa, \phi)$ of the current CPS state. Logical expressions κ_s and κ_t represent the expression κ where each variable is replaced with a symbol in fresh sets s and t respectively. Similarly for ϕ_s and ϕ_t. Moreover, δ is a fresh symbol that is bound in the SMT solver to the expression that represent the metric on $\mathbb{R}^{2n}$ of choice. This enables to handle expressions $\kappa \wedge \phi$ and $\kappa \wedge \neg\phi$ easily without variable clashes and to minimise the distance at the same time.

```
Require

  $\kappa_s$, $\phi_s$, $\kappa_t$, $\phi_t$: instances of $\kappa$ and $\phi$ with two distinct sets of fresh symbols
  $\delta$: fresh real symbol bound to distance expression on symbol sets $s$ and $t$
  $\epsilon$: error tolerance

function PROXIMITYRANGE($\kappa$, $\phi$)

 solver ← new SMT-Optimizing-Solver
  solver.minimize-goal($\delta$).assert($\neg\phi_s \wedge \phi_t$).assert($\kappa_s$)
  model ← solver.check-sat()
  if model not found then                     // $\kappa_s \wedge \neg\phi_s$ unsat: state is critical
    (Cmin, Cmax) ← (model.getvalue($\delta$), DMAX(solver))
  else                                        // $\kappa_s \wedge \neg\phi_s$ sat
    solver.remove($\kappa_s$).assert($\kappa_t$)
    model ← solver.check-sat()
    if model not found then                   // $\kappa_t \wedge \phi_t$ unsat: state is not critical
      (Cmin, Cmax) ← (-DMAX(solver), -model.getvalue($\delta$))
    else
      Cmin ← -DMAX(solver)
      solver.remove($\kappa_t$).assert($\kappa_s$)
      Cmax ← DMAX(solver)
  return (Cmin, Cmax)
function DMAX(solver)
  model ← solver.get-model()
  repeat
    dmax ← model.getvalue($\delta$)
    solver.assert($\delta >$ dmax $+ \varepsilon$)
    model ← solver.check-sat()
  until model is found
  return dmax
```

Figure 1. Proximity range pseudo-algorithm.

5. EXPERIMENTAL RESULTS

This section describes our prototype of the framework and the chemical process simulation testbed to prove the feasibility of the approach and the first performance results.

The prototype is based on Docker [35] containers with a microservice architecture made of freely available open source tools and ad-hoc software developed by the author:

- **Chemical Process Simulation**: a Node-RED [36] docker container used to simulate[2]:

  a. The physical simulation of pumps and liquid flows, developed in the Typescript language.

[2] We developed a first version based on a Redis to simulate the physical behaviour using Lua scripts and a Python simulation of PLCs based on the Pymodbus [37] library to send real Modbus messages on the network. The Observer used TShark/Wireshark [32] for traffic capturing and the same timeseries databases to store parsed messages. The real deep packet inspection for CPS, already established in literature [28], [30], was too cumbersome for our goal since the Observer that can make use of parsed messages from the simulator without loss of generality and applicability.

b. The HMI implementing the manual control of the process, developed using Typescript functions and the Node-RED visual language Figure 6 shows a screenshot.

c. The automatic control, emulating the SCADA server, developed in Typescript and Node-RED.

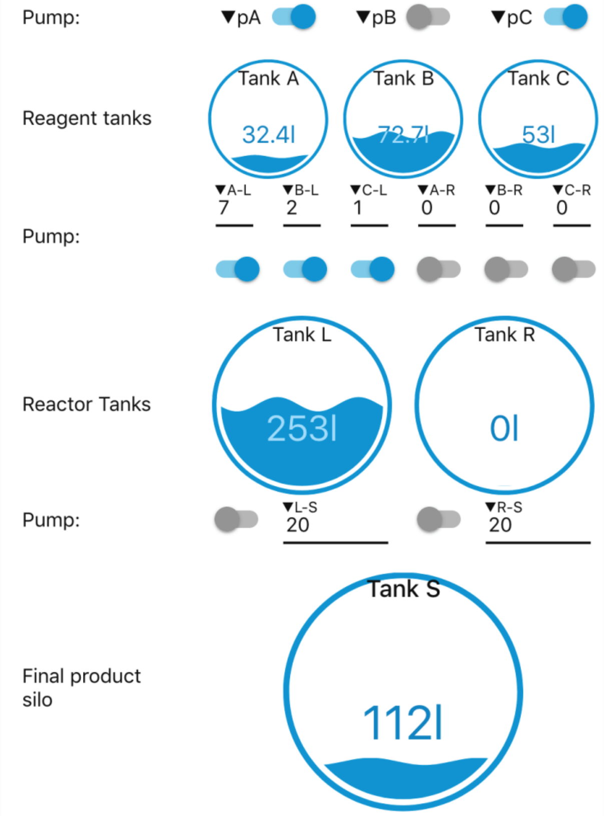
d. The attacker's read and write commands to PLCs to emulate the scenarios in Section 3.

- **The Observer**: Modbus-like network messages from the chemical process simulations are stored in timeseries database with all the required fields. Each variable occurring in critical specifications is associated with a query that returns one timestamped value or fails in case of unobservable variables. The timeseries DB of choice is InfluxDB [38] with its native query language and DataFrame files queries using the Pandas library [39], [40].

- **The Reasoner**: the prototype of the core of the proposed framework, developed in Python using Microsoft Z3, an open source SMT prover [33]. It implements the concepts described in Section 4 and provides the first performance and feasibility measurements. Results are store in timeseries databases for easy access. The reasoner is also instrumented with performance measurements using Prometheus [41].

- **Monitoring Interface**: Grafana [26] and Chronograf (part of the InfluxData suite [38]) containers that provide mature data visualisation and query interface to time series databases.

The whole prototype works on an Intel Core i7 laptop with 8 GB or RAM. Figure 7 shows the performance results of our benchmark. Each test generates random critical conditions based on a different number of variables up to 200. Then it generates a random CPS state. We performed different set of tests with different percentages of observable values: 100%, 50%, 20%. The maximum computation time is about 4 seconds, which proves the feasibility of our framework in real cases. It is worth noticing that, while the 50% and 20% cases exhibit similar computational times, the 100% one is clearly easier to compute. This was expected, since unobservable variables require optimisation computations on wider space. Notice that the overall computational time is super-linear w.r.t. the number of variables.



Pump: ▼pA ▼pB ▼pC

Reagent tanks

Tank A 32.4l

Tank B 72.7l

Tank C 53l

▼A-L 7 ▼B-L 2 ▼C-L 1 ▼A-R 0 ▼B-R 0 ▼C-R 0

Pump:

Reactor Tanks

Tank L 253l

Tank R 0l

Pump: ▼L-S 20 ▼R-S 20

Final product silo

Tank S 112l

Figure 6: Screenshot of the emulated HMI.

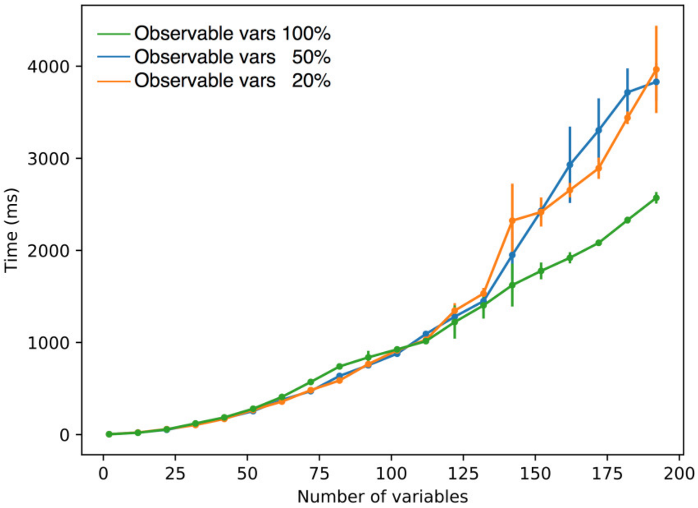


Figure 7: Computation time of $C(\kappa, \phi)$ from random benchmark.

6. Final Remarks

This work presents a specification-based predictive cyber security monitoring framework for cyber physical systems and improves previous works [5] and [6]. It enables specifying known critical conditions, through an easy but expressive formal language, that can be detected at runtime. It defines a quantitative notion of criticality of the CPS current state from the specified critical states: checking how the criticality changes in time enables security operators to predict whether the system is evolving towards critical states and how close it is from them, or similarly if it is returning to a licit state.

The novelty of the approach is to handle both observable and unobservable aspects of the CPS. This enables a security operator to express a model of criticality that is more complete and suitable for real cases. The monitor is able to continuously gather the value of all the observable variables from the analysis of the network traffic analysis, and to build a representation of this knowledge that correctly approximates the actual state of the system. Present work provides a way to specify critical conditions also in terms of constraints on the observation times, not only on their value. This provides a way to specify simple but effective temporal properties of the observed CPS behaviour.

Unobservable variables complicate the criticality detection. When the monitor cannot discriminate if the CPS is in a critical state, a human operator can provide additional knowledge about unobservable variables as a refinement. However, this can be hard in real cases due to the complexity of the CPS and the large number of variables. To this aim, the framework is capable of computing the minimal piece of information that is required to discriminate the criticality of the CPS state, and provide such information as a guide to the operator.

Unobservable variables also complicate computing the proximity from critical states. However, the framework is able to compute a min/max range of the criticality of the CPS. Our working prototype plots how the range changes in time, providing an overview of the evolution of the system w.r.t. the specified critical conditions which can be used as a criticality dashboard of support to Security Operaton Centers (SOC) and cyber incident response teams.

This work uses SMT techniques to assess the criticality of the CPS current state and to compute the minimal assisted checks. It also uses SMT-based optimisation techniques to compute proximity ranges from critical states. Preliminary results prove an expressive specification language and an efficient reasoning engine. While first results seem feasible and promising, further experiments can be performed to characterise critical conditions and will be the subject of further investigation to assess the limits of our approach.

REFERENCES

[1] V. M. Igure, S. A. Laughter, and R. D. Williams, “Security issues in SCADA networks,” Computers & Security, vol. 25, no. 7, pp. 498–506, Oct. 2006.

[2] P. Huitsing, R. Chandia, M. Papa, and S. Shenoi, “Attack taxonomies for the Modbus protocols,” International Journal of Critical Infrastructure Protection, vol. 1, pp. 37–44, Dec. 2008.

[3] S. East, J. Butts, M. Papa, and S. Shenoi, “A Taxonomy of Attacks on the DNP3 Protocol,” in Critical infrastructure protection iii, 2009, pp. 67–81.

[4] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, “Guide to Industrial Control Systems (ICS) Security,” National Institute of Standards; Technology, Gaithersburg, MD, Jun. 2015.

[5] A. Coletta and A. Armando, “Security Monitoring for Industrial Control Systems,” in Security of industrial control systems and cyber physical systems. CyberICS 2015, 2016, pp. 48–62.

[6] A. Coletta, "Predictive Detection of Known Security Criticalities in Cyber Physical Systems with Unobservable Variables," in 11th international conference on security and its applications (cnsa), 2018, pp. 61–77.

[7] I. N. Fovino, A. Carcano, M. Masera, and A. Trombetta, "Design and Implementation of a Secure Modbus Protocol," in International conference on critical infrastructure protection, 2009, pp. 83–96.

[8] M. Majdalawieh, F. Parisi-Presicce, and D. Wijesekera, "DNPSec: Distributed network protocol version 3 (DNP3) security framework," in Advances in computer, information, and systems sciences, and engineering, Springer, 2007, pp. 227–234.

[9] G. Gilchrist, "Secure authentication for DNP3," in IEEE power and energy society general meeting - conversion and delivery of electrical energy in the 21st century, 2008, pp. 1–3.

[10] M. Roesch, "Snort: Lightweight Intrusion Detection for Networks." LISA '99: 13th Systems Administration Conference, pp. 229–238, 1999.

[11] B. Caswell and J. Beale, Snort 2.1 intrusion detection. Syngress, 2004.

[12] D. Bolzoni, S. Etalle, P. Hartel, and E. Zambon, "POSEIDON: a 2-tier Anomaly-based Network Intrusion Detection System," in Fourth ieee international workshop on information assurance (iwia), 2006.

[13] W. Heimerdinger, V. Guralnik, and R. VanRiper, "Anomaly-based intrusion detection." Google Patents, 2006.

[14] C. Zimmer, B. Bhat, F. Mueller, and S. Mohan, "Time-based intrusion detection in cyber-physical systems," Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems - ICCPS '10, p. 109, 2010.

[15] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes, "Using Model-based Intrusion Detection for SCADA Networks," Science And Technology, vol. 329, pp. 1–12, 2006.

[16] R. Mitchell and I. R. Chen, "Behavior Rule Specification-Based Intrusion Detection for Safety Critical Medical Cyber Physical Systems," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 1, pp. 16–30, 2015.

[17] K. Xiao et al., "A Workflow-Based Non-intrusive Approach for Enhancing the Survivability of Critical Infrastructures in Cyber Environment," in Third international workshop on software engineering for secure systems (sess'07: ICSE workshops 2007), 2007, pp. 4–4.

[18] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," Computers & Security, vol. 28, nos. 1-2, pp. 18–28, Feb. 2009.

[19] M. Caselli et al., "Specification Mining for Intrusion Detection in Networked Control Systems Specification Mining for Intrusion Detection in Networked Control Systems," Proceedings of the 25th USENIX Security Symposium, pp. 791–806, 2016.

[20] D. Carasso, Exploring Splunk. CITO Research, 2012.

[21] J. Diakun, P. R. Johnson, and D. Mock, Splunk Operational Intelligence Cookbook. Packt Publishing Ltd, 2016.

[22] C. Gormley and Z. Tong, Elasticsearch: the Definitive Guide. O'Reilly Media, Inc., 2015.

[23] J. Turnbull, The Logstash Book. James Turnbull, 2013.

[24] Y. Gupta, Kibana Essentials. Packt Publishing Ltd, 2015.

[25] G. S. Sachdeva, Practical ELK Stack. Apress, 2017.

[26] Grafana Labs, “Grafana.” 2017.

[27] LogRhythm Inc, “LogRhythm security intelligence and analytics platform.” 2017.

[28] I. Nai Fovino, A. Coletta, A. Carcano, and M. Masera, “Critical State-Based Filtering System for Securing SCADA Network Protocols,” IEEE Transactions on Industrial Electronics, vol. 59, no. 10, pp. 3943–3950, Oct. 2012.

[29] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. Nai Fovino, and A. Trombetta, “A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems,” IEEE Transactions on Industrial Informatics, 2011.

[30] I. Nai Fovino, A. Carcano, A. Coletta, M. Guglielmi, M. Masera, and A. Trombetta, “State-based firewall for industrial protocols with critical-state prediction monitor,” in Critical information infrastructures security, vol. 6712 LNCS, Springer Berlin Heidelberg, 2011, pp. 116–127.

[31] “MODBUS Application Protocol Specification V1.1b3,” 2012.

[32] Wireshark Foundation, “Wireshark.” 2017.

[33] L. De Moura and N. Bjørner, “Z3: An efficient SMT solver,” in International conference on tools and algorithms for the construction and analysis of systems, 2008, pp. 337–340.

[34] R. Sebastiani and P. Trentin, “OptiMathSAT: A Tool for Optimization Modulo Theories,” in International conference on computer aided verification, 2015, pp. 447——454.

[35] Docker Inc, “Docker.” 2017.

[36] JS Foundation, “Node-RED.” 2017.

[37] G. Collins, “Pymodbus 1.2.0.” 2017.

[38] InfluxData Inc, “InfluxDB.” 2017.

[39] W. McKinney, “Data structures for statistical computing in python,” in Proceedings of the 9th python in science conference, 2010, pp. 51–56.

[40] W. McKinney, Python for data analysis: Data wrangling with pandas, numpy, and ipython. " O’Reilly Media, Inc.", 2012.

[41] P. Authors, “Prometheus-monitoring system & time series database.” prometheus. io, 2017

Authors

Alessio Coletta has 10+ years R&D experience in cyber security of Industrial Control Systems (ICS), working at the Joint Research Centre of the European Commission in the Security of Networked Critical Infrastructures unit, at the Global Cyber Security Center in Rome, in the Incident Prevention and Management unit of Poste Italiane, and currently at Magneti Marelli. He is a PhD candidate at the University of Trento (Italy) and Foundation Bruno Kessler (FBK, Trento). He holds a Master degree in Information Security at the Royal Holloway University of London and a Master degree in Computer Science at the Scuola Normale Superiore of Pisa.

SECURE STRATEGY FOR OPTICAL IMAGE ENCRYPTION SYSTEM BASED ON AMPLITUDE MODULATION, PHASE MODULATION AND MODIFIED LOGISTIC MAP

Ahmed M. Elshamy[1], Aziza I. Hussein[2,3], Hesham F. A. Hamed[4], M. A. Abdelghany[4], and Hamdy M. Kelash[5]

[1]Department of Network and Security, College of Information Technology, Fujairah University, Fujairah, UAE
[2]Department of Computer & Systems Engineering, Faculty of Engineering, Minia University, Minia, Egypt
[3]Electrical & Computer Engineering Department, Effat University, Jeddah, KSA
[4]Department of Communication & Electronics, Faculty of Engineering, Minia University, Minia, Egypt
[5]Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt

ABSTRACT

This paper presents an optical image encryption system based completely on amplitude modulation, phase modulation in the discrete Fourier transform and modified chaotic logistic map. Amplitude modulation and phase modulation are accomplished by the use of spatial light modulator (SLM). SLMs are normally used to control incident light in amplitude-best, phase-best or the mixture (amplitude-phase). The random amplitude modulation based on a chaotic Baker map is carried out in time domain, while the random phase modulation is accomplished in the frequency domain. In this paper, we proposed a technique to regulate and enhance protection in a chaotic logistic map method leading to increased variety of key space of the logistic map. This causes our encryption system to become exceptionally sturdy against brute pressure. An exhaustive analysis of the proposed encryption system is undergone and shows positive results in encryption metrics when compared to several different photo encryption techniques. The analysis demonstrates the highly valued security and immunity to noise of the photograph encryption. The proposed modified logistic map with amplitude and phase modulation is suitable for real-time application.

KEYWORDS

Image Encryption, Fourier Transform, Security, Chaotic Logistic Map, Chaotic Baker Map

1. INTRODUCTION

Technological advances in internet connectivity have led to a massive increase in transmitted data over the internet, including media sharing, photos, videos and social networking. Therefore, it has emerged as a major concern to maintain the security of this data. The prime method of ensuring

Dhinaharan Nagamalai et al. (Eds) : CSEIT, NCS, SPM, NeTCoM - 2018
pp. 101–116, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81808

the safety of this data is through the process of encryption. There are many encryption methods, but websites, as well as their users, will always prefer the most efficient encryption systems that still protect them against unauthorized hackers. Thus it is essential to understand and improve upon the most recent proposed techniques in order to guarantee the safety of different types of data, including the most important, such as private conversations and official records.

There are a few chaos strategies in picture encryption and phase modulation encryption techniques in the optics field proposed by researchers. Picture encryption strategies have been a particular focus to fulfill the demand of photoprotection in digital and electric conversation systems. Chaos encryption techniques are essential for increasing verbal exchange protection. Unauthorized hackers attempt to intercept the original data in the course of the transmission from the sender to the receiver via wired or wireless media. Chaotic systems are high in randomness and sensitivity of the initial conditions of the transmission. These properties make chaotic systems ideal for implementation of a cipher, which is needed for encryption and decryption in the encryption technique. Despite encryption systems being well built and implemented, there remains the possibility of hacking of any system. The goal is to minimize this opportunity, and in an effort to do so, unique chaotic logistic map techniques were proposed.

In reference [1], the Logistic chart is implemented aimed at the chaotic mapping, for optical orthogonal occurrence department multiplexing system (OFDM) in the time and frequency domains in a fast Fourier remodel. In [2-4], authors proposed cozy orthogonal frequency-department-multiplexing passive optical community (OFDM-PON) primarily based on the chaos scrambling in the OFDM frequency domain. Amongst them, chaotic Logistic maps based totally on pseudorandom quantity generator PRNGs were proposed [5-6]. In [7], authors proposed a picture encryption gadget primarily based on the changed logistic map, compressive ghost imaging and coordinate sampling. The cipher text may be received by discrete cosine remodel (DCT). Multichannel random discrete fractional Fourier remodel with arbitrary increment coefficients and fractional remodel kernel features has been proposed with the aid of Kang [8]. In [9], the novel model offered by implementing the chaotic Logistic map in embedded structures using the synchronization phenomenon of discrete fractional logistic maps have been proposed. A logistic chaotic map and a multichannel arbitrary unconnected fractional Fourier convert was proposed [10]. In [11], presented a photograph encryption system founded on the unconnected manifold parameter and coupled Logistic maps. A new data encryption approach based on the location substitution, shuffling and a selection manner is proposed [12]. A unique shade photo encryption set of rules based totally on the Logistic map and double random section encoding by rapid Fourier transform has been offered through the way of Huang [13].

In [14], they proposed optical chaos based totally on confusion (Arnold cat map) and diffusion (logistic map) encryption algorithms, which confuse the connection among the authentic photograph and encrypted image. [15] offered an encryption approach for photo based on chaos blending, which reduces the encryption time manner, in contrast to unique chaotic maps. In [16], a grayscale photograph encryption device based on chaotic Baker map and optical segment modulation in frequency area was offered by means of Discrete Fourier transformation. The authentic image randomized with the aid of chaotic baker map first. After this, it is transformed to optical signs by means of optical emitter, like an optical source, to transform it from electrical sign to optical signal, and encrypt it via phase modulation. This follows two phase modulation, one in time domain and one in Fourier area and finally, transformed by way of CCD virtual digital camera to virtual layout to show it on the laptop.

In [17], a hybrid encryption device based on Arnold cat map and optical phase encryption in frequency area by way of discrete Fourier remodel was presented. The original image is randomized through Arnold cat map first, and then it is transformed to optical signal via an optical emitter inclusive of optical source to convert it from electric signal to optical sign.

However, it encrypts through section modulation with the aid of applying two-phase modulation on it, one in the time domain and one in Fourier area. It detects it by means of CCD virtual camera to transform it to digital format to show it on the computer. Within the decryption technique, it applies the conjugate of two random phase modulation to the optical signal to decrypt the photo, after that it converts the optical signal to electrical sign with the aid of optical detector and randomized with the aid of chaotic Arnold's cat map to get the authentic picture, and then accomplish chaotic Arnold's cat map decryption.

In [18], an encryption method for color photo founded entirely on twofold arbitrary part modulation is described as well as the shade indexed map as the preprocessing cover for altering the color image from three components (RGB) to at least one aspect. [19] presented a video encryption approach primarily based on Henon chaotic map and the optical segment modulation. The Henon chaotic map may be applied digitally, then it demonstrates a second technique optical section modulation optically. The implementation of the proposed method used two classes of video encryption absolutely and permutation encryptions. In [20], there is contrast among numerous encryption technique based on the chaos map and the optical section modulation.

In this paper, the picture is passed through a confusion and diffusion procedure. We compared between special encryption approaches to decide which technique is most appropriate for use in communication network structures for relaxed and efficient transmission. To confirm the validity of the proposed encryption device, numerical Matlab simulation, and cryptanalysis consequences are done.

The structure of the current study is arranged as follows:

Phase II clarifies some preliminary knowledge of several encryption techniques. Phase III gives the proposed encryption techniques. Segment IV presents the high-quality metrics, performance evaluation. In the end, the belief and destiny guidelines are drawn in phase V.

2. Literature Review of Image Encryption Techniques

2.1. Logistic Map

Chaotic maps may be classified into three degrees: 1-D map, 2-D maps, and 3-D [21]. The Logistic map has been considerably utilized for chaotic cryptosystems and released as a paradigm for the dynamics of a population. It includes a maximum of the chaotic traits and an example of a 1D map [22]. This chaotic logistic map is determined by way of refer to (1).

$$Z_m = \beta Z_{m-i}(I - Z_{m-i}) \tag{1}$$

Where (0, 1) and β are bifurcation parameters. When 3.57 ≤ β ≤ 4 the machine is in chaotic conduct. The chart in Fig. 1 demonstrates the bifurcation of Logistic Map as indicated by β. Its value explores and determines the conduct of the chaotic logistic map.

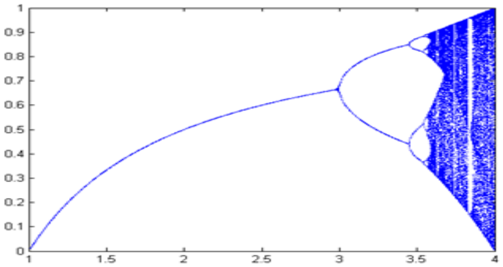


Figure 1. Logistic map chart.

2.2. Baker Map

The chaotic Baker map encryption approach in a photo processing network called a device of encryption. It's a primarily confusion-based device that accomplishes the scrambling of a four-sided matrix photograph M × M dimension by using converting places for pixels founded off a stealthy key.

Baker map of the discretized is represented by $B(v_1,\ldots\ldots,v_k)$, wherever the arrangement of k integers, $v_1, v_2,\ldots\ldots,v_k)$ is selected as where every integer v_i divisions M, and $M_i = v_1 + \ldots\ldots + v_i$. The pixel at indices (l, s), with $M_i \le l \le M_i + v_i$ and $0 \le s \le M$ is mapped to [23]:

$$B_{(n_1,\ldots\ldots\ldots,n_k)}(l,s) = \left[\frac{M}{v_i}(l - M_i) + s \bmod \frac{M}{v_i}, \frac{v_i}{M}(s - s \bmod \frac{M}{v_i}) + M_i\right] \tag{2}$$

This technique is applied to the subsequent phases:

1. The rectangular matrix M × M is split into ok squares of thickness VI and quantity of factors M.
2. Each factor in the rectangle are rearranged to a row within the permuted rectangle. Rectangles are decided upon from right to left beginning with top rectangles, and then lower ones.
3. The examination starts off read out inside each rectangle, from the lowest left nook in the direction of upper elements.

Fig. 2 suggests an instance for the chaotic Baker map for (M × M) rectangular matrix (M = eight), where the name of the game key S = [2, 4, 2].

2.3. Optical Phase Modulation

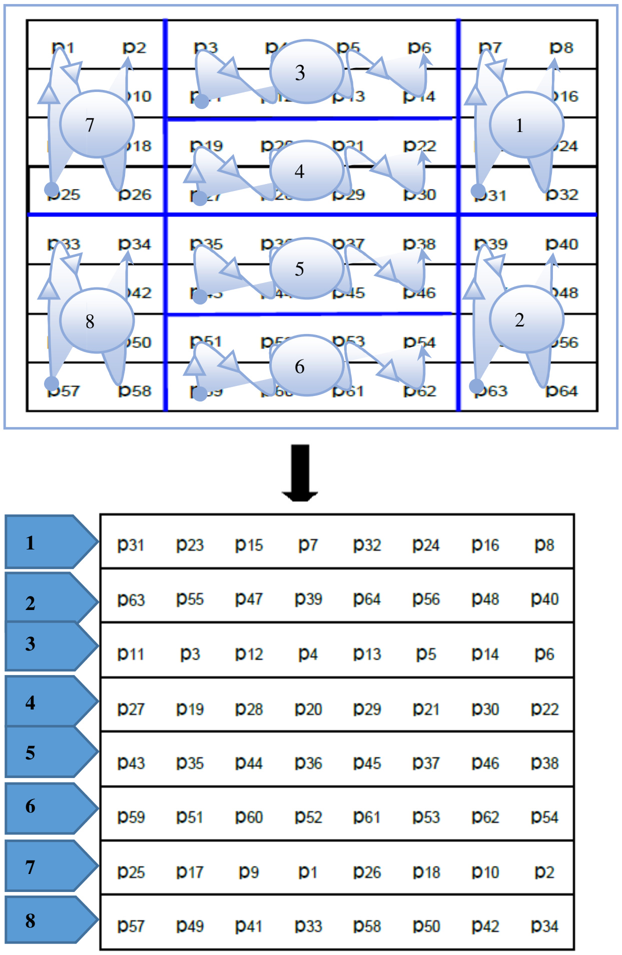
Optical segment modulation was proposed as an optical encryption method in 1997 via Refregier and Javidi known as Double Random phase Encryption (DRPE). DRPE used two random segment mask presented as keys. This encryption approach carried out in pure optical conversation systems, by means of generating optical original signal from laser generator and making use of first phase modulation through Spatial Light Modulator (SLM1) and passing it via first unique lens to convert the signal in frequency domain and observe 2nd phase modulation through SLM2 and bypass it via lens2 to transform lower back signal in time area and retrieve it with the aid of Charge Coupled Device (CCD) as visible in Figure 3.

$\varphi(x,y)$ Coded image, $f(x,y)$ present inventive image, $\delta_n(x,y)$ first amplitude mask in the time domain (first key), $\delta_m(\gamma,\mu)$ and second phase mask in the frequency domain [16].

$$\delta_n(x,y) = \exp\left[2i\pi n(x,y)\right] \tag{3}$$

$$\delta_m(x,y) = \exp\left[2i\pi m(x,y)\right] \tag{4}$$

$$DFT\ \delta_m(x,y) = \delta_m(\gamma,\mu) = \exp\left[2i\pi m(\gamma,\mu)\right] \tag{5}$$



1	p31	p23	p15	p7	p32	p24	p16	p8
2	p63	p55	p47	p39	p64	p56	p48	p40
3	p11	p3	p12	p4	p13	p5	p14	p6
4	p27	p19	p28	p20	p29	p21	p30	p22
5	p43	p35	p44	p36	p45	p37	p46	p38
6	p59	p51	p60	p52	p61	p53	p62	p54
7	p25	p17	p9	p1	p26	p18	p10	p2
8	p57	p49	p41	p33	p58	p50	p42	p34

Figure 2. Chaotic Baker map randomization for 8 × 8 matrices with a secret key S= [2, 4, 2].

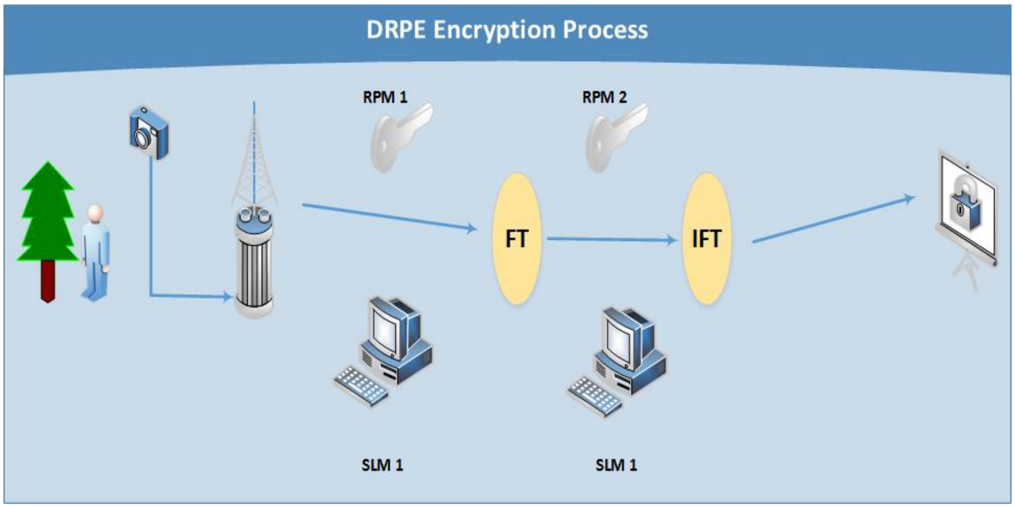


Figure 3. Fully encryption technique with double phase modulation.

Encryption process for the grayscale image in two dimensions is defined as follows:

$$\varphi(x,y) = FT^{-1}\{FT\{f(x,y)\delta_n(x,y)\} * \{\delta_m(\gamma,\mu)\}\} \tag{6}$$

Equation (6) the symbol (*) denotes convolution.

But, in decryption process to do away with first and second segment modulation it has to use conjugate of first and second section mask, as it is applied in the time domain and in the frequency domain. Decryption system algorithm is illustrated as follows:

$$f(x,y) = FT^{-1}\{FT\{f(x,y)\delta_n^*(x,y)\} * \{\delta_m^*(\gamma,\mu)\}\} \tag{7}$$

In first and second phase masks (*) present conjugate of the mask.

$$\delta_n^*(x,y) = \exp\left[-2i\pi n(x,y)\right] \tag{8}$$

$$\delta_m^*(\gamma,\mu) = \exp\left[-2i\pi n(\gamma,\mu)\right] \tag{9}$$

3. THE PROPOSED IMAGE ENCRYPTION TECHNIQUE

The one-dimensional Logistic chaotic encryption set of rules is an easy cipher technique, the modified chaotic equations are carried out to scramble and unscramble pixels sequentially. The proposed encryption method based on random amplitude modulation followed on chaotic Baker rework map (BT) in the time domain by way of first SLM (key 1), random section encryption in frequency area by means of 2nd SLM (key 2) and modified Logistic transformation map (MLT). Changed Logistic map is a development of logistic map where a polynomial time period is $(1-2Z_{m-i})^2$ supplementary. The modified Logistic map equation may be as follows:

$$Z_m = \beta Z_{m-i}(I - Z_{m-i})\,(I - 2Z_{m-i})^2 \tag{10}$$

Where $Z_m \in$ (0, 1), $\beta \in$ (0, 16), the initial value Z_0 =0.3.
When $\beta \in$ (0, 4.2), the system seems as episodic behavior.
When $\beta \in$ (4.2, 6.5), the system seems as deprived of chaotic behavior.
When $\beta \in$ (6.5, 16), the system is now chaotic behavior.

The changed Logistic map reveals that it is going to have precise chaos characteristics due to the enhanced extensive variety of β (key space variety) from traditional range (3.57 - four) to (6.5 - 16) as visible in Figure 4, which rise key space and may be beneficial for image cryptosystems.

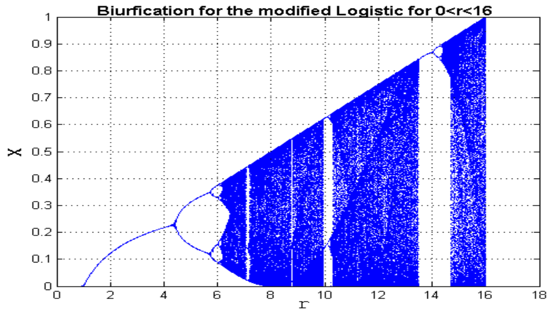


Figure 4. The modified Logistic map.

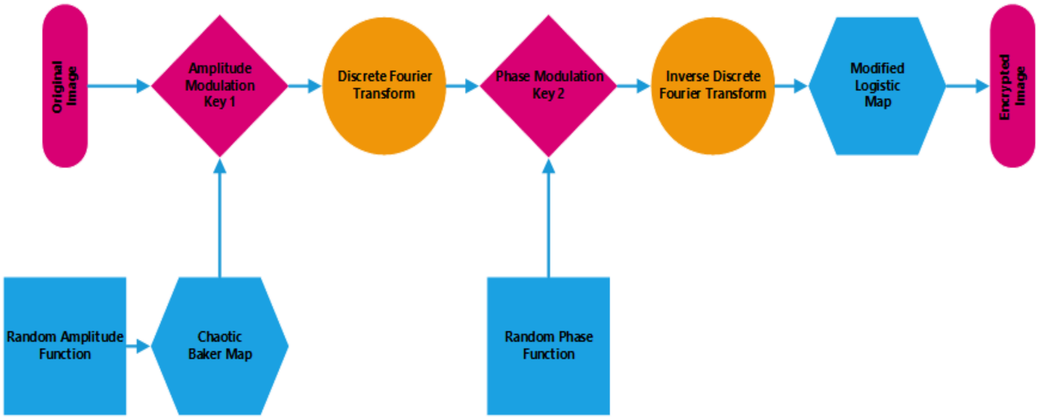

Original Image
Amplitude Modulation Key 1
Discrete Fourier Transform
Phase Modulation Key 2
Inverse Discrete Fourier Transform
Modified Logistic Map
Encrypted Image
Random Amplitude Function
Chaotic Baker Map
Random Phase Function

Figure 5. The proposed encryption technique block diagram.

The series steps for the encryption process are:

1. Randomize the pixels positions of amplitude masks by chaotic Baker map, this step completed digitally.

2. Trade the picture into an optical signal by way of laser beam generator (LED).

3. Follow amplitude modulation by first SLM (key 1) to the optical sign (authentic photograph) in time area using $BT\ \delta_n(x, y)$.

4. Convert it to Fourier domain by the first lens and apply section modulation by using SLM (Key 2).

5. Convert it to time area via the second lens and scramble pixels by using modified Logistic map (key three).

6. Retrieve the encrypted picture through CCD digital camera or convert it to electrical sign by means of detectors and display it on computer.

The encryption procedure is defined mathematically as:

$$\vartheta(x, y) = MLT\ \{FT^{-1}\{FT\{f(x, y)\ (BT\,\delta_n(x, y))\}*\{\delta_m(\gamma, \mu)\}\}\} \qquad (11)$$

$\vartheta(x, y)$ Is the proposed encrypted image. MLT is denoted as the modified Logistic transform.

The original image $f(x, y)$ randomized by $BT\ \delta_n(x, y)$ chaotic baker map for amplitude masks. After this, it is transformed to optical sign with the aid of optical emitter, like optical supply, to transform it from electric signal to optical signal and encrypt it with the aid of section mask modulation, the end result scrambled by using changed Logistic map.

The decryption procedure is defined mathematically as

$$f(x,y) = IMLT\{FT^{-1}\{FT\{f(x,y)\ (IBT\delta_n^{*}(x,y))\}*\{\delta_m^{*}(\gamma,\mu)\}\}\} \qquad (12)$$

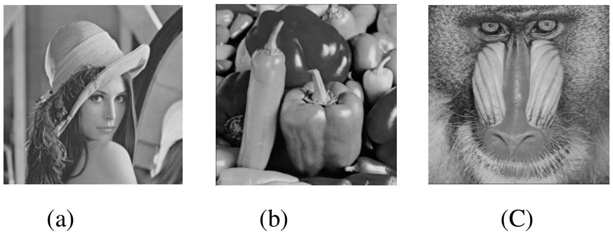
$IMLT$ consult with inverse modified Logistic transform and IBT check with the inverse Baker map. The conjugate of two amplitude and segment modulations are applied to the optical signal to decrypt the photograph, after that convert the optical sign to electric sign via optical detector and randomized via the changed Logistic map to get the original picture.

4. ENCRYPTION QUALITY METRICS AND ANALYSIS

Several Matlab simulation tests have been completed to research the proposed encryption approach, which has been applied to the Lena, Peppers and Baboon photos as shown in Fig. 6 to compare the proposed technique with a Logistic map, Baker map and DRPE in overall performance and noise immunity. These pics database specifications which were utilized in simulation experiments are defined in Table I.

Table 1. Images database specifications

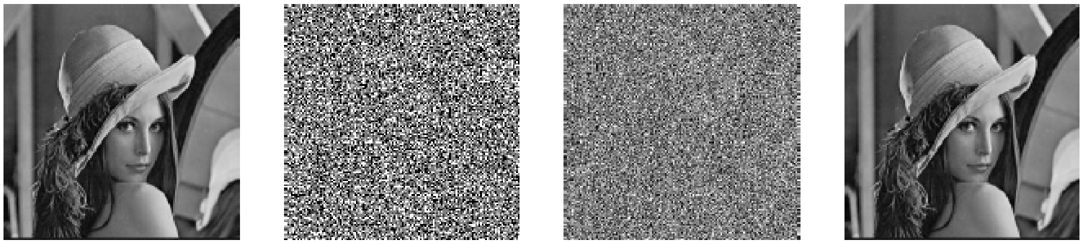
Encryption technique	**Lena**	**Peppers**	**Baboon**
Color	Grayscale	Grayscale	Grayscale
Dimensions	512×512	512×512	512×512
Bit depth	8	8	8
Image type	Bitmap	Bitmap	Bitmap



(a) (b) (C)

Figure 6. (a) Lena, (b) Peppers, and (c) Baboon images.

Visible inspection is a critical metric of photograph encryption, but it isn't sufficient to determine the robustness of proposed algorithm [23].



a. Original image

b. Amplitude and phase modulation

c. Modified Logistic map Encryption

d. Decrypted image

Figure 7. Visual inspection for Lena image.

It's clear that the cryptograph pictures are absolutely unrecognizable and do well to hide the information of the original photos. Therefore, the anticipated encryption set of rules is suitable from visual inspection factor of view [24].

4.1. Histogram Analysis

A grayscale picture is given the very best depth value L (for a picture with eight bits/ pixel L=255). The intensity degree histogram (grey) is described as a characteristic h(g) which is the same as value the number of pixels within the photo (or inside the region of the hobby) that have a depth equal to g, for every depth degree g ϵ [0 … L] [25].

$$h(g)= Ng \tag{12}$$

Where Ng present within the photograph is the number of pixels inside the location of hobby that have the intensity identical tog. Histogram evaluation is used to ensure factors: the first factor is that the original photograph and encrypted picture ought to be absolutely different, 2nd point is that the unique picture and the decrypted photo are much like every different. From Figure. 8 it's clear that all encryption techniques fulfilled the terms of histogram evaluation but Baker map encryption method no longer fulfills the terms because the histogram of the encrypted image is identical to histogram of the unique picture.

4.2. Correlation Coefficient Analysis

This evaluation applied among authentic sample photograph and encrypted sample photograph is used as a metric to evaluate the encryption method. This metric can be calculated as the subsequent equation [26]:

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{13}$$

In which x and y are the gray-scale standards of pixels on the equal directories in the apparent and cipher snap shots. In arithmetical calculations, the subsequent distinct formulations can be used.

$$E(x) = \frac{1}{L}\sum_{i=1}^{L} x_i \tag{14}$$

$$D(x) = \frac{1}{L}\sum_{i=1}^{L} (x_i - E(x))^2 \tag{15}$$

$$\mathrm{cov}(x, y) = \frac{1}{L}\sum_{i=1}^{L}(x_i - E(x))(y_i - E(y)) \qquad (16)$$

Where L is the quantity of pixels worried within the scheming. The nearer value of r_{xy} is to 0, the better the incomparability of the encryption procedure.

Table II. demonstrates values of correlation coefficient parameters for all encryption techniques. The power of encryption technique increases the lower the value of correlation coefficient and near 0. Table II. Clarifies that the best correlation coefficient value appears in the proposed approach in comparison to other encryption techniques.

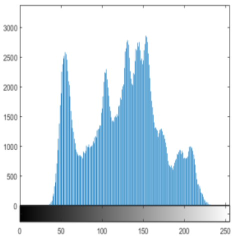
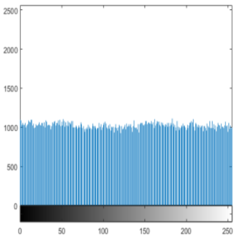
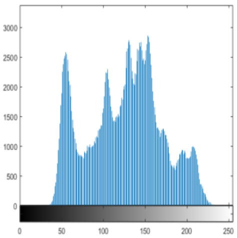
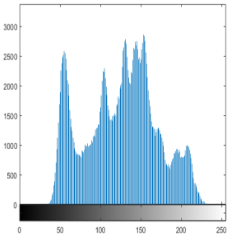
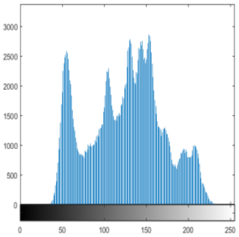
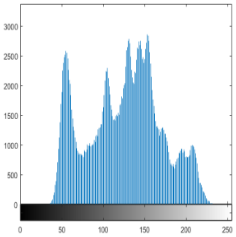
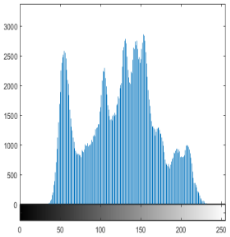
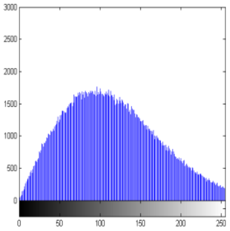
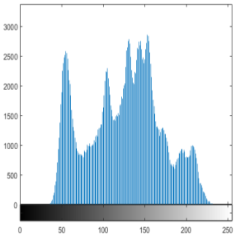
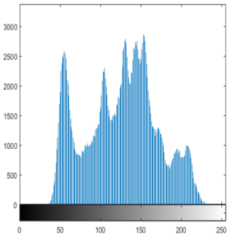
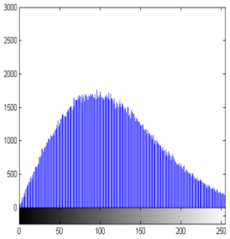
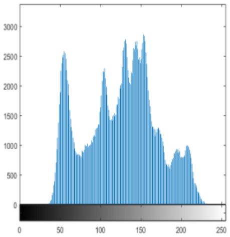
Techniques	**Original sample image**	**Encrypted sample image**	**Decrypted sample image**
(a) Logistic Map			
(b) Baker Map			
(c) DRPE			
(d) Proposed Technique			

Table 2. Correlation coefficient analysis between all encryption techniques including the proposed one.

Encryption Technique	Lena	Peppers	Baboon
Logistic map	-0.0154	-0.0165	-0.0291
Baker map	0.0014	0.0098	0.0118
DRPE	0.0016	0.0063	0.0057
Proposed Technique	0.0005	0.0028	0.0001

4.3. Maximum Deviation Analysis

This analysis measures how massive a deviation there may be between the histogram of unique pattern photograph and histogram of the encrypted image via the nature of encryption approach. Ideally, this should be maximum or an excessive value. Table III. Demonstrates that the maximum deviation value appears within the proposed encryption approach when compared to other encryption strategies.

Table 3. Maximum deviation analysis of all encryption techniques including the proposed one.

Encryption Technique	Lena	Peppers	Baboon
Logistic map	0.4860	0.3913	0.5223
Baker map	0	0	0
DRPE	0.8569	0.8550	0.8457
Proposed Technique	1	0.8766	0.8563

4.4. Irregular Deviation Analysis

Abnormal deviation analysis is based on measuring the extent of the deviation through encryption on the encrypted photograph. Higher efficacy of the encryption technique is indicated by low value of these parameters. The abnormal deviation DI is calculated by the following equation:

$$H_D(i) = \left| H(i) - M_H \right| \tag{17}$$

Where H(i) present histogram value of absolute difference matrix between original and encrypted images, MH is the main value of this histogram.

$$D_I = \frac{\sum_{i=0}^{255} H_D(i)}{M \times N} \tag{18}$$

Table IV. Demonstrates that the proposed technique in this metric analysis is lower than other encryption techniques.

Table 4. Irregular deviation analysis of all encryption techniques including the proposed one.

Encryption Technique	Lena	Peppers	Baboon
Logistic map	0.6877	0.5695	0.6932
Baker map	0.9552	0.8364	1
DRPE	0.6707	0.7318	0.7307
Proposed Technique	0.3876	0.3603	0.3592

4.5. Encryption Time Analysis

Encryption time analysis, one of the key parameters for measuring encryption system time, is the time needed for encryption procedure from beginning till giving up. However, internet encryption must consume the least time possible for encryption technique to be used in programs like video conference and live television. Table V. demonstrates the lowest time appears inside the DRPE encryption method, more so than different encryption strategies. However, the proposed encryption approach has a small encryption time which does not exceed 2 seconds.

Table 5. Encryption process time (sec) for all encryption techniques including the proposed one.

Encryption Technique	Lena	Peppers	Baboon
Logistic map	0.8046	0.9058	0.9082
Baker map	0.8764	0.8872	0.9704
DRPE	0.6593	0.6025	0.5367
Proposed Technique	1.1365	1.1211	1.0727

4.6. Noise Immunity

Noise immunity evaluation is one of the most essential metrics to determine if this encryption approach is suitable to use in any verbal exchange gadget. An evaluation of the authentic sample picture and decrypted photograph inside the height sign to noise ratio shows the presence of additive white Gaussian noise with variance 0.01. PSNR is expressed as the following equation:

$$MSE = \frac{1}{XY} \sum_{x=1}^{X} \sum_{y=1}^{Y} \left| f(x,y) - \hat{f}(x,y) \right|^2 \tag{19}$$

Wherever X and Y are the picture magnitudes. $f(x,y)$ and $\hat{f}(x,y)$ denote the innovative and the decrypted pictures, correspondingly.

$$PSNR = 10 \log_{10} \left(\frac{\text{Max Intensity of Image}}{MSE} \right) \tag{20}$$

Table VI. demonstrates that the proposed approach is the best in terms of electricity immunity to noise in comparison to different encryption techniques. Table VI indicates that our proposed approach shows desirable results to be used in all fashions of verbal exchange systems.

Table 6. PSNR (dB) values for all encryption techniques including the proposed one.

Encryption Technique	**Lena**	**Peppers**	**Baboon**
Logistic map	18.5646	17.8999	18.7482
Baker map	8.1517	9.9379	8.8715
DRPE	18.5640	17.9016	18.7461
Proposed Technique	28.0129	30.4805	28.3508

5. CONCLUSION

In this paper, a unique image encryption technique based on randomized pixel positions, amplitude modulation and phase modulation is proposed. The proposed approach based on the modified Logistic chaotic map and modified amplitude modulation increases complexity. Also, the implementation of the proposed technique used numerous keys. Both of these factors increase the solidity of encryption, thus making it exceptionally strong against unauthorized attackers. The proposed technique accomplished excellent evaluation outcomes in correlation coefficient, maximum deviation, irregular deviation, encryption time and immunity to noise. All results indicate the suitability of the proposed encryption technique in ideal conversation networks.

REFERENCES

[1] L. Zhang, Bo Liu, X. Xin, Qi Zhang, J. Yu, and Y wang. (2013). Theory and Performance Analyses in Secure CO-OFDM Transmission System Based on Two-Dimensional Permutation. Journal of Lightwave Technology, VOL 31, pp74-80.

[2] L. Zhang, X. Xin, Bo Liu, and Y Wang. (2011). Secure OFDM-PON Based on Chaos Scrambling. IEEE Photonics Technology, VOL 23, pp 998-1000.

[3] M. Bi, X. Fu, X. Zhou, Lu Z., G. Yang, X. Yang, S Xiao, and W Hu. (2017).A Key Space Enhanced Chaotic Encryption Scheme for Physical Layer Security in OFDM-PON. IEEE Photonics Journal, VOL 9, pp 1-10.

[4] W. Zhang, C. Zhang, C. Chen, H. Zhang, W. Jin, and Kun Qiu. (2017). Hybrid Chaotic Confusion and Diffusion of Physical Layer Security in OFDM-PON. IEEE Photonics Journal, VOL 9, pp 1-7.

[5] S. Chen, T. Hwang, and Wen-Wei Lin. (2010). Randomness Enhancement Using Digitalized Modified Logistic Map. IEEE Transactions on Circuits and Systems, VOL 57, pp 996-1000.

[6] Lingfeng Liu, Suoxia Miao, Hanping Hu, Yashuang Deng. (2015). Pseudorandom bit generator based on nonstationary logistic maps. IET Information Security, VOL 10, pp 87-94.

[7] Xianye Li, Xiangfeng Meng, Xiulun Yang, Yongkai Yin, Yurong Wang, Xiang Peng, Wenqi He, Guoyan Dong, and Hongyi Chen. (2016). Multiple-Image Encryption Based on Compressive Ghost Imaging and Coordinate Sampling. IEEE Photonics Journal, VOL 8, pp 1-11.

[8] Xuejing Kang, Feng Zhang, and Ran Tao. (2015). Multichannel Random Discrete Fractional Fourier Transform. IEEE Signal Processing, VOL 22, pp 1340-1344.

[9] P. Harsha. (2017). A Novel Micro-architecture using a Simplified Logistic Map for Embedded Security. IEEE Embedded Systems, VOL 9, pp 41-44.

[10] Guo Cheng Wu, Dumitru Baleanu. (2014). Chaos synchronization of the discrete fractional logistic map. Signal Processing Elsevier Journal, VOL 102, pp 96-99.

[11] Liansheng Sui, Kuaikuai Duan, Junli Liang. (2015). Double-image encryption based on discrete multiple-parameter fractional angular transform and two-coupled logistic maps. Optics Communications Elsevier Journal, VOL 343, pp 140-149.

[12] Manish Kumar, Sunil Kumar, Rajat Budhiraja, M.K. Das, Sanjeev Singh. (2016). A cryptographic model based on the logistic map and a 3-D matrix. Journal of Information Security and Applications Elsevier Journal, VOL 32, pp 47-58.

[13] Huiqing Huang, Shouzhi Yang. (2017). Colour image encryption based on logistic mapping and double random-phase encoding. IET Image Processing Journal, VOL 11, pp 211-216.

[14] Yiyuan X., Jiachao Li, Zhoufan K., Yushu Z., Xiaofeng L., and Yong L., “Exploiting Optics Chaos for Image Encryption-then-Transmission,” IEEE JLT, VOL 34, No. 22, PP. 5101-5109, NOVEMBER VOL 15, pp 2016.

[15] Yannick A, Alain T. (2016). Image encryption by chaos mixing. IET Journal Image Processing, VOL10, No. 10, pp 742-750.

[16] Ahmed M. Elshamy, Ahmed N., Abd El-Naser A., Osama S. Faragallah, Yi Mu, Saleh A., Fathi E. (2013). Optical Image Encryption based on Chaotic Baker Map and Double Random phase Encoding. Light Wave Technology Journal- IEEE, Vol 31, No. 15, pp. 2533-2539.

[17] Ahmad M. Elshamy, Fathi E. Abd El-Samie, Osama S. Faragallah, Elsayed M. Elshamy, Hala S. El-sayed, S. F. El-zoghdy, Ahmed N. Z. Rashed , Abd El-Naser A. and Ahmad Q. Alhamad. (2016). Optical Image Cryptosystem Using Double Random Phase Encoding and Arnold's Cat Map. Optical and Quantum Electronics-Springer Journal, VOL 48, No. 3, pp. 1-18.

[18] Ahmed M. Elshamy, Aziza I. Hussein, Hesham F. A. Hamed, M. A. Abdelghany, Hamdy M. Kelash, and Ahmad Q. Alhamad. (2016). Optical Cryptosystem for Color Image Based on Double Random Phase Encryption in Discrete Fourier Domain and Color Indexed Map. IJCSIS, VOL 14, No. 8, pp. 763-780.

[19] Ahmed M. Elshamy, Aziza I. Hussein, Hesham F. A. Hamed, M. A. Abdelghany, Hamdy M. Kelash, and Ahmad Q. Alhamad. (2017). Secure Implementation for Video Streams Based on Fully and Permutation Encryption Techniques. IJCIS- IEEE Conference, PP. 50-55.

[20] Ahmed M. Elshamy, Aziza I. Hussein, Hesham F. A. Hamed, M. A. Abdelghany, and Hamdy M. Kelash. (2018). Image Encryption Techniques Based on Chaos Maps and Two Random Phase Modulation in Discrete Fourier Transform. Wulfenia Journal, VOL 25, No. 2, PP. 81-90.

[21] N.K. Pareek, Vinod Patidar, and K.K. Sud.(2005). Cryptography using multiple one-dimensional chaotic maps. Commun. Nonlinear Sci.umer. Simul. VOL 10, pp. 715-723.

[22] Z. Yun-peng, L. Wei, C. Shui-ping, Z. Zheng-jun, N. Xuan, and D. Weidi.(2009). Digital image encryption algorithm based on chaos and improved DES. Systems, Man and Cybernetics, IEEE Int. The conference, pp. 474-479.

[23] Y. Honglei , W. Guang-shou, W. Ting , L. Diantao, Y. Jun, M. Weitao, F. Y. Shaolei and M. Yuankao. (2009). An image encryption algorithm based on two-dimensional baker map. in Proc. ICICTA.

[24] Rajinder Kaur, Er. Kanwalpreet Singh. (2013). Comparative Analysis and Implementation of Image Encryption Algorithms. IJCSMC, VOL. 2, Issue. 4, pg.170 – 176.

[25] Nidhi Sethi. (2012). A New Image Encryption Method using Chirikov and Logistic Map. International Journal of Computer Applications (0975 – 8887), VOL 59– No.3.

[26] Sudip G., Sambaran H, Santi P, Hafizur R. (2015). A new algorithm for grayscale image histogram computation. INDICON IEEE conference.

[27] Fangjun H., JiwuH., Yun Q. (2016). New Framework for Reversible Data Hiding in Encrypted Domain. IEEE SPS Journal, VOL 11, No. 12, pp 2777-2789.

Authors

Ahmed M. ELShamy received his Bachelor's degree in Electronics and Electrical Communication Engineering, 2010, his graduation project got best project in the level of EGYPT in Communication Engineering Field, 2010. He completed his Masters in Electronics and Electrical Communication Engineering from the University of Menofiah, Egypt, 2014.

He is currently Lecturer in Information Technology College at Fujairah University, Fujairah-UAE. Moreover, he is working in Fujairah e-Government as a Network and Security Specialist. He had many publications in international journals and conferences, his research interests include Network Security for its Analysis and Enhancement, Multimedia Security, Digital Encryption, Optical Encryption, Image Processing, Chaos Theory, authentication and Communications Networks. He has worked for various conferences at different levels from reviewer to organizer-chairman.

Aziza I. Hussein received her Ph.D. degree in Electrical & Computer Engineering from Kansas State University, USA in 2001 and the M.Sc. and B.Sc. degrees from Assiut University, Egypt in 1989 and 1983, respectively.

She joined Effat University in Saudi Arabia In 2004 and established the first Electrical and Computer Engineering program for women in the country and taught related courses. She was the head of the Electrical and Computer Engineering Department at Effat University from 2007-2010. She was the head of Computer and Systems Engineering Department, Faculty of Engineering, Minia University, Egypt from 2011-2016. Currently she is the head of the Electrical & Computer Engineering Department at Effat University Saudi Arabia.

Her research interests include microelectronics, analog/digital VLSI system design, RF circuit design, high-speed analog-to-digital converters design and wireless communications.ziza I. Hussein received her Ph.D. degree in Electrical & Computer Engineering from Kansas State University, USA in 2001 and the M.Sc. and B.Sc. degrees from Assiut University, Egypt in 1989 and 1983, respectively.

Her research interests include microelectronics, analog/digital VLSI system design, RF circuit design, high-speed analog-to-digital converters design and wireless communications.

Hesham F. A. Hamed was born in Giza, Egypt, in 1966. He received the B.Sc. degree in electrical engineering, the M.Sc. and Ph. D. degrees in electronics and communications engineering from EL-Minia University, EL-Minia, Egypt, in 1989, 1993,and 1997 respectively. He currently is the dean of faculty of engineering ,Minia University. He was a Visiting Researcher at Ohio University, Athens, Ohio. From 1989 to 1993 he worked as a Teacher Assistant in the Electrical Engineering Department, EL-Minia University. From 1993 to 1995 he was a visiting scholar at Cairo University, Cairo, Egypt. From 1995 to 1997 he was a visiting scholar at Texas A&M University, College Station, Texas (with the group of VLSI). From 1997 to 2003 he was an Assistant Professor in the Electrical Engineering Department, EL-Minia University. From 2003 to 2005 he was Associate Professor in the same University. He has published more than 80 papers. His research interests include analog and mixed-mode circuit design, low voltage low power analog circuits, current mode circuits, nano-circuits design, and FPGA.

Mahmoud A. Abdelghany was born in Saudi Arabia in 1979. He received the B.S. (Electrical Engineering) and the Master of Science (Communication Engineering) degrees from Minia University in 2000 and 2005, respectively and PhD degree from Kyushu University, Japan in 2011. He had been a post-doctoral research fellow with the Radio-Frequency Integrated Circuits (RFIC) & Microwave Communication Devices Laboratory, Kyushu University, Japan from October 2013 to April 2014. In December 2011, he joined the Electrical Engineering Department, Faculty of Engineering, Minia University as an assistant professor. In February 2017, he joined the Electrical Engineering (Communication and computer Engineering) Department, Faculty of Engineering, Nahda University as an assistant professor. His current research interests include the study and design of RF CMOS System LSI and low-power, low-noise and highly linear CMOS RF front-end architectures. Dr. Mahmoud is a member of the Institute of Electrical and Electronics Engineers (IEEE).

Hamdy Kelash received the B.Sc. and M.Sc degrees in Computer Science and Engineering from Menoufia University, Menouf, Egypt, in 1971 and 1979,also he received PhD from France in 1985. respectively. He is currently Full Professor with the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University. His current research interests include network security, cryptography, internet security, multimedia security, image encryption, watermarking, steganography, data hiding, medical image processing, and chaos theory.

AN ELASTIC-HYBRID HONEYNET FOR CLOUD ENVIRONMENT

Nguyen Khac Bao, Sung Won Ahn, Minho Park

Department of Information Communication, Materials, and Chemistry
Convergence Technology Soongsil University, Seoul 156-743, Korea

ABSTRACT

When low-interaction honey net systems are not powerful enough and high-interaction honey net systems require a lot of resources, hybrid solutions offer the benefit's of both worlds. Affected by this trend, more and more hybrid honey net systems have been proposed to obtain wide coverage of attack traffic and high behavioral ideality in recent years. However, these system themselves contain some limitations such as the high latency, the lack of prevention method for compromised honey pots, the waste of resources and the finger printing problem of honey pot that hinder them to achieve their goals. To address these limitations, we propose a new honey net architecture called Efficient Elastic Hybrid Honey net. Utilizing the advantages of combining SDN and NFV technologies, this system can reduce the response time for attack traffic, isolate compromised honey pots effectively, defeat the finger printing problem of honey pots, and optimize the resources for maintenance and deployment. Testing our system with real attack traffic, the results have showed that Efficient Elastic-Hybrid Honey net system is not only practical, but also very efficient.

INDEX TERMS

Honey net, Honey pot, Elastic, Hybrid, Software defined Networking, Network Function Virtualization

1. INTRODUCTION

Since 1990s, honey pots [1] have been used to cope with various security threats by observing and understanding the exploits, methods, and strategies used by attackers. Throughout the years, a lot of honey pots have been proposed and developed to capture, analyze, and ultimately react against these new types of attacks [12-16]. These honey pots can be classified by the level of interaction [2]. High-interaction honey pots allow attackers to interact with a real operating system running some vulnerable services with few restrictions. By using high-interaction honey pots, we can obtain the information of how the honey pots were being probed, and misused, as well as the motivation of the attackers. On the other hand, low-interaction honeypots just provide limited functionalities to attackers by using emulated operating systems and services. However, low-interaction honey pots can deal with the large of different types of network traffic in a short time.

Honey net, a network of honey pots, was first introduced in 1999 by a long-term project called Honey net Project. Since then, some researchers have proposed several hybrid honey net systems

Dhinaharan Nagamalai et al. (Eds) : CSEIT, NCS, SPM, NeTCoM - 2018
pp. 117–127, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81809

[6-9] which can utilize the both advantages of low and high interaction honey pots. However, there are four main limitations in the existing honey nets: (1) the high latency of the system, (2) the finger printing problem of honey pots, (3) the large amount of resources required for deployment and maintenance, and (4) the lack of prevention mechanism when honey pots are compromised by attackers. Because the existing hybrid honey net systems just adopted both types of honey pots they still have the same problems of honey pots. The fingerprinting issue is an example of the problems. So far, a wide range of fingerprinting techniques have been developed to detect the existence of honey pots. In [3], the authors revealed that most low-interaction honey pots can be easily fingerprinted. For example, two low-interaction honey pots called Kippo and Kojoney which always return a hardcoded timestamp when attackers access these systems. In addition, low-interaction honey pots can be detected by checking their environmental variables. Relying on the operating system types and these services running on them is also a honey pot fingerprinting technique that skilled attackers have always used [4]. In the current honey nets, most of the authors did not take into account the compromised problem of the high-interaction honey pots. Therefore, when these honey pots are compromised by attackers, they can be used to attack production servers or internal hosts in the network. In term of resource efficiency, these existing honey net systems may bring resource waste if there is no attacker. In other words, they waste a lot of resources to run these honey nets without attackers.

To overcome these limitations of the existing systems, in this paper, we propose an SDN and NFV based honey net, called Efficient Elastic-Hybrid Honey net (E2H2). In our system, each type of honey pots deals with different phases of attacks to maximize the advantages of both low-interaction honey pots and high-interaction honey pots. Initially, only a low-interaction honey pot with less used resources runs. All of the discovering attacks are taken by this low-interaction honey pot to get the wide coverage of attack traffic. Along with these reconnaissance attacks, high-interaction honey pots are created in a form of virtual machines to interact with the attacker in the specific attacks to obtain the deep understanding of the attacker's behaviors. The number of high-interaction honey pots increases proportional to the number of the attacks. When the specific attacks end, the system collects all log files in the high-interaction honey pots, and destroys the virtual machines of the high-interaction honey pots to save resources.

To defeat finger printing techniques, E2H2 system uses the same information of OS types and number of services in high interaction honey pots and virtual hosts created by the low interaction honey pot. Hence, when switching the connections from the low-interaction honey pot to the new high-interaction honey pot the attackers hardly discover the changes. Moreover, the abundant number of high-interaction honey pot images are created in NFV platform to confuse even skilled attackers. Currently, the existing honey net systems have to process all of attack traffic then depends on the capabilities of the honey pots to find appropriate ones. By leveraging SDN technology, E2H2 system can easily observe all connections belonging to the existing the high-interaction honey pots in the network. Thus, any abnormal action of these honey pots raises an alarm to indicate the compromised problem has occurred. These compromised honey pots will be isolated and disconnected from the network immediately for offline analyses.

This paper is organized as follows. The related work is reviewed in Section 2. In Section 3, we provide a full presentation of Efficient Elastic-Hybrid Honey net system. In Section 4, serveral experiment results are discussed. Section 5 concludes this paper.

2. RELATED WORK

A. HYBRID HONEYNET ARCHITECTURE

Along with the development of honey pots, a lot of researchers have been interested in developing a hybrid honey net system. Bailey [6] is the first person who tried to integrate low and high-interaction honey pots to solve the trade-off problem between two types of honey pots. In his system, low-interaction honeypots used as sensors to collect information to get the wide coverage of attack traffic. Their approach can reduce the number of the high-interaction honey pots in a network while still get the wide coverage of different attack traffic. However, it increases the burden for the low-interaction honey pots and raises the fingerprinting issue of honey pots.

In 2013, VMI-Honey mon [8] appeared as a hybrid honey net system which solves the routing problems when using multiple identical high-interaction honey pot clones. Since these high-interaction honey pots share the same MAC and IP addresses, they have to put each clone into separate network bridges. They used ip tables to forward incoming connections to the low-interaction honeypots and then queued them. Thus, this can increase the latency of system response time and decrease the opportunities to successfully lure attackers.

Based on Bailey work, in 2015, FAN [7] proposed a dynamic hybrid honeynet with two main modules: decision engine and redirection engine. The author used a server acts as a gateway, which gets the attackers requests, forwards messages to the low-interaction honeypots, and then redirects connections to the high-interaction honeypots. As VMI Honeymon, this system also has the high latency since their server has to modify TCP headers of all response packets time by time. Moreover, by using an additional server, this system consumes more resources than other existing honeynet systems.

HoneyMix [9] is the latest work which related to NFV and SDN environment. This system focused on two main limitations of the existing honeynets: (1) fingerprinting problem, and (2) Gen-III honeynets only provide coarse-grained data control. By using dynamic connection selection mechanism, this system can provide various responses for attacker’s requests. Hence, this kind of system might be not practical in the real world. In addition, both types of honeypots can be selected; therefore, the low-interaction honeypots get the high probability to be detected by the attacker.

B. SOFTWARE-DEFINED NETWORKING AND NETWORK FUNCTION VIRTUALIZATION

Software-defined networking (SDN) is an emerging network paradigm that provides a flexible way to control entire the network. By separating data plane and control plane, SDN allows moving part of the decision-making logic from network devices to the controllers.

Network Function Virtualization (NFV) [10] aims at providing network functions such as gateways, firewall... in software, which can be run on commodity hardware in data centers.

3. ELASTIC HYBRID SYSTEM

Normally, before performing a specific attack, attackers always try to discover the network for obtaining the useful information. Thus, network reconnaissance is the primary and initial step of any advanced and persistent attack. Performing network recon naissance, attackers can(1) discovering and enumerating active hosts, (2) detecting the current OS, open ports and related application names in these hosts, (3) discovering vulnerabilities in each host.

Based on the obtained information of active hosts, the attacker can perform further attacks such as flooding attack, brute force, SQL injection, etc. Therefore, the normal attack process can be divided into two phases:

1) Reconnaissance attack: Attackers try to find out the active hosts inside the network and the services, which are running on these host, by using some attack tools such as Nmap, Zenmap [4]. After discovering an active IP address, Nmap can issue a reverse-DNS query to obtain the domain name from the host's address.

2) Specific attack: Based on the information from reconnaissance attack, attackers will use some dedicated tools to attack some given services

A. SYSTEM MODELING

Utilizing the SDN technology, the network inside E2H2 system is controlled by SDN controllers to get more flexible and reduce the computational cost when steering network traffic. Beside that, with the help of NFV technology, we can create or remove instances as well as network between them quickly and easily. Basically, E2H2 system consists of five main components:

- Selecting services provides an active way to deal with scanning attacks. By choosing a random number, this module synchronizes with the low-interaction honeypot to give some available services for attackers. This number also relates to the image id in the NFV platform which will be used to initiate a new high-interaction honeypot later.

- Forwarding engine keeps an important role in E2H2 system. When the attacker sends a lot of scanning traffic for discovering network, forwarding engine redirects the traffic to the low-interaction honeypot which opened some services based on random number created by selecting services. All of the new traffic from the attacker will be forwarded to a recently created high-interaction honeypot to get deeper attacker's behaviors learning.

- Observation engine checks the connections between the attacker and the high-interaction honeypot periodically. It sends a message to add/removing engine to start removing this high-interaction honeypot. The handle honeypot module will use NFV APIs to remove the high-interaction honeypot for resource restoration.

- Adding/Removing engine works as a bridge between SDN controllers and NFV orchestrator. It receives messages from selecting services and observation module then sends add/remove requests to handle honeypot engine for further processes.

- Handle honeypot engine is located in NFV orchestrator. Whenever receiving requests from Add/Removing engine, handle honeypot engine uses all open APIs of NFV platform to initiate or remove instances

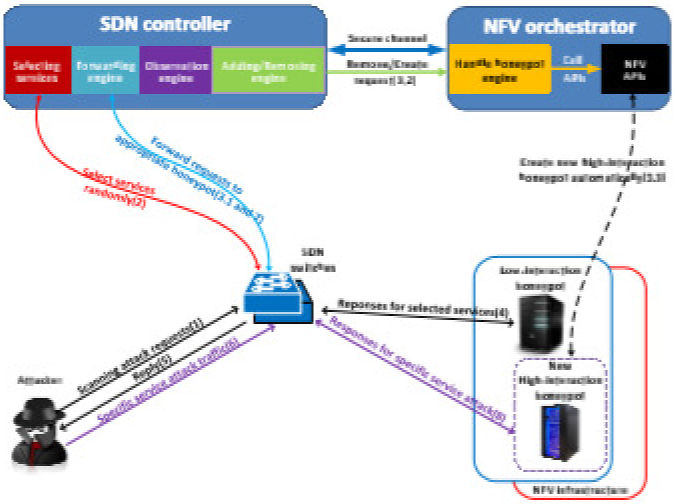

SDN controller
Selecting services
Forwarding engine
Observation engine
Adding/Removing engine
Secure channel
Remove/Create request(3.2)
NFV orchestrator
Handle honeypot engine
Call APIs
NFV APIs
Select services randomly(2)
Forward requests to appropriate honeypot(3.1 and 7)
Create new high-interaction honeypot automatically(3.3)
SDN switches
Responses for selected services(4)
Low-interaction honeypot
New High-interaction honeypot
Responses for specific service attack(8)
NFV infrastructure
Attacker
Scanning attack requests(1)
Reply(5)
Specific service attack traffic(6)

Fig. 1. Efficient Elastic-Hybrid Honeynet architecture

B. LOGIC SYSTEM WORK FLOW

In E2H2 system, there is only one low-interaction honeypot which runs all the time to deal with network reconnaissance attacks. All high-interaction honeypots will be created to handle further attacks from the adversary.

Figure 1 shows an use case of how E2H2 system works. When the attacker performs scanning attack to find out active hosts and opening ports, the selecting services module randomly creates a number which related to image id in NFV orchestrator. With NFV platform, we can make a large number of images manually by using CD or DVD ISO files. Each image corresponds with an OS type and some fixed services running on it. By this way, a honeynet with abundant different services was made for attackers to attack to. The relationship between virtual hosts created by the low-interaction honeypot and image list of NFV infrastructure is showed in Figure 2.

After creating random number, the forwarding engine selectively forwards all of the attacker's requests which related to designated available services to the low-interaction honeypot. Since these requests are belong to the scanning attack, the forwarding engine just sets a small value of hard timeout for all of them. Beside that, a historic used source port list is created by the forwarding engine to save all source ports in the reconnaissance attack. In the existing honeynet architecture, they have to receive all attacker's scanning traffic and then provide the responses back to the attacker based on the ability of the current honeypots.

Along with this step, Adding/Removing engine sends the creation request to handle honeypot module in NFV orchestrator. This means a new high-interaction honeypot is creating while the low-interaction honeypot is responding to the attackers scanning requests. Figure 3 gives the straight view of our mechanism for traffic redirection.

When the attacker receives the responses from the low-interaction honeypot, he/she knows which ports are opening so he/she will choose one of these ports to perform further attacks such as flooding attack, brute force, SQL injection, etc. These attacks can be performed by using some tools e.g., bonesi, loic or sqlmap. By checking the used source ports and the relation between used source ports and the source port of new flow, the system can know when the second phase of the attack starts.

The observation engine inspects the connections between the attacker and the high-interaction honeypots periodically. If the connections are closed, observation engine will collect all log files in high-interaction honeypot then send to offline server for deep analyses. After that, it sends a message to Add/Removing engine to delete this high-interaction honeypot. The handle honeypot module calls NFV APIs to remove the high-interaction honeypot instance and get back the resources. In addition, the observation engine also takes into account the infection of the compromised high-interaction honeypots. According to the authors of the paper [5], the higher the interaction level, the higher the possible misuse. Proving the real environments for the attackers is the both advantage and disadvantage of high-interaction honeypots. In E2H2 system, all of the high-interaction honeypots are supervised by the observation engine. If any connection with internal hosts is found, this high-interaction honeypot is identified as a compromised honeypot. It rapidly be disconnected from the network for offline investigation, then another similar one will be created to replace.

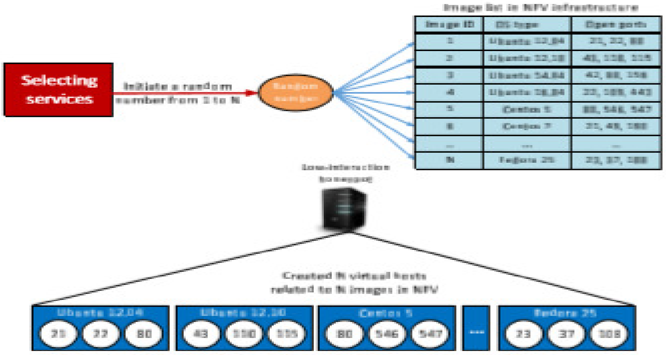


Fig. 2. Relation between two types of honeypots in E2H2 system

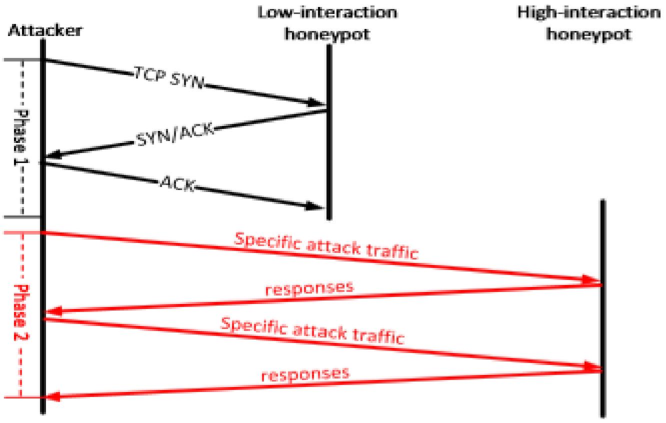


Fig. 3. Illustration of the traffic redirection mechanism

C. RESOURCE OPTIMIZATION MODEL

In the normal existing honeynet architecture, all the honeypots have one common problem, i.e., they are worthless if there is no attacker. As long as attackers do not send any packet to the honeynet, the system wastes a lot of resources for running these honeypots. Low-interaction honeypots can typically be deployed with fewer resources because they do not fully offer the real services and they also incur less risk. Resource optimization is an important problem that we want to solve since it is the limitation of the existing honeynet architecture.

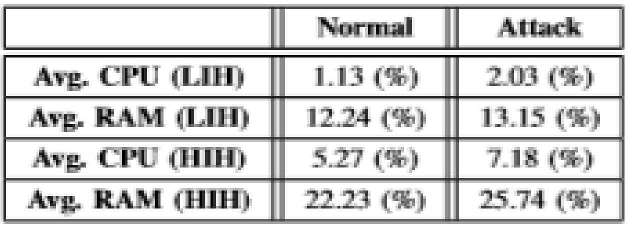
Normally, the used resources of honeypots is vary depended on the state of them. Under the attack, a honeypot uses more resources than it is in normal state. Assume that we have N honeypots with the same type, the function of average used resource for each honeypot in different states can be defined as follows:

$$\overline{R}_{Honeypot}(nor) = \frac{\sum_{i=1}^{N} \left(P_i^{CPU}(nor) + P_i^{RAM}(nor)\right)}{N} \qquad (1)$$

$$\overline{R}_{Honeypot}(atk) = \frac{\sum_{i=1}^{N} \left(P_i^{CPU}(atk) + P_i^{RAM}(atk)\right)}{N} \qquad (2)$$

We assume that there are m low-interaction honeypots and n high-interaction honeypots in the normal system. Under the attack, the probability of a low-interaction honeypot will be chosen is p. With k attacks at the same time, the average used resources of honeynet in the normal system is:

$$\begin{aligned}\overline{R}_{NS}^{k} = {} & (m-kp)\overline{R}^{LIH}(nor) + [n-k(1-p)]\overline{R}^{HIH}(nor) \\ & + kp\overline{R}^{LIH}(atk) + k(1-p)\overline{R}^{HIH}(atk) \qquad (3)\end{aligned}$$



	Normal	Attack
Avg. CPU (LIH)	1.13 (%)	2.03 (%)
Avg. RAM (LIH)	12.24 (%)	13.15 (%)
Avg. CPU (HIH)	5.27 (%)	7.18 (%)
Avg. RAM (HIH)	22.23 (%)	25.74 (%)

Table I Average Used Resources Of Lih And Hih In Different States

In E^2H^2 system, there is only one low-interaction honeypot which always runs. High-interaction honeypots will be created depend on the number of attacks. Therefore, with k attacks at the same time, the average used resources of honeynet in E2H2 system is:

$$\begin{aligned}\overline{R}_{E-H}^{k} = {} & \overline{R}^{LIH}(atk) + (k-1)\left(\overline{R}^{LIH}(atk) - \overline{R}^{LIH}(nor)\right) \\ & + k\overline{R}^{HIH}(atk) \qquad (4)\end{aligned}$$

4. EXPERIMENTS

E^2H^2 was tested using Open Stack platform and POX controller which supports Open Flow protocol version 1.0. We used two SDN-enable switches: an Open v Switch version 2.3 and HP3800 switch, along with two compute nodes in Open Stack environment. With the Mitaka Open Stack platform, we ran the Open Stack controller in a high hardware configuration machinewith32GBRAMandinteli73.4ghzQuadCoreCPU.

A. BANDWIDTH EXPERIMENT

With the help of SDN technology, we can have a better control of our network. The New mechanism can help to reduce the number of responses for the attackers requests. The nethogs tool was used for bandwidth calculation in this experiment

As the results, in Figure 4, the reduction of bandwidth in the low-interaction honeypot is significant. With our system, even receiving the large number of concurrent attacks, the increasing of bandwidth in the low-interaction honeypot is very small (≈ 33 KBytes/s). In the other existing systems, the low-interaction honeypots receive and respond to all attackers requests; therefore, it can cause an overload in low-interaction honeypots with the increasing of bandwidth is 203.943 KBytes/s.

B. RESOURCES EXPERIMENT

For collecting the largest possible amount of information including complete attack logs, data access, executed byte codes, etc, they preferred to use high-interaction honeypots rather than low-interaction honeypots in the normal existing honeynet systems. Thus, the number of low-interaction honeypots and high-interaction honeypots in the normal systems respectively are 4 and 10. Another reason is that the small number of the high-interaction honeypots can lead to the high probability that attackers can detect the low-interaction honeypots in these systems. We set the value of p is 0.7. The average used resource of them are equal. Table I shows all information related to both types of honeypots in two different states.

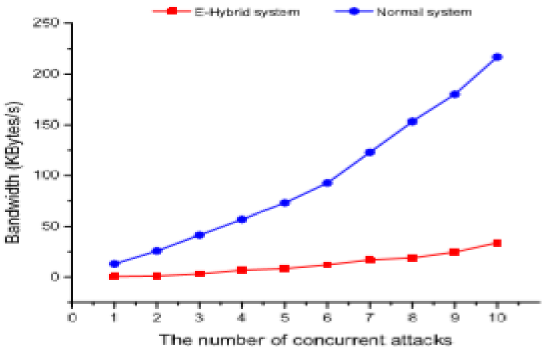


Fig. 4. Bandwidth comparison of low-interaction honeypots in two systems

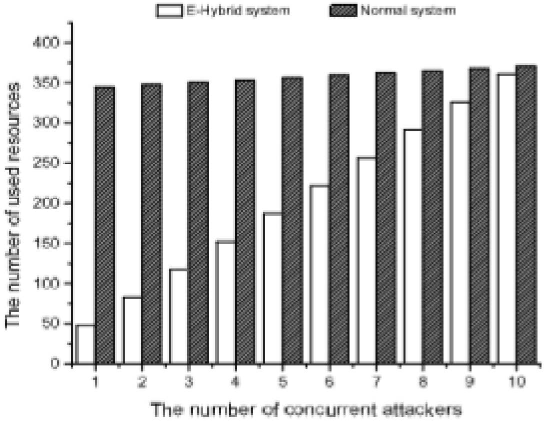


Fig. 5. Resource comparison under multiple concurrent attackers

In Figure 5, when the number of attackers attack in the same period of time is small, our system can save a lot of resources (just used ≈ 14 % in compare with the normal systems). The probability of multiple attackers attack a system at the same period of time is very small; however, even when this event can be occurred (with 10 concurrent attackers) E2H2 system still uses a less resources than the other existing ones.

C. AVERAGE RESPONSE TIME EXPERIMENT

The average response time of a system is also an important criteria to evaluate the effectiveness of a honeynet system. The experiment was performed by running the bonesi tool to generate a large number of packets in 10 seconds. We captured all the packets by using wireshark and calculate the average response time based on the time for a TCP connection establishment (three-way handshake).

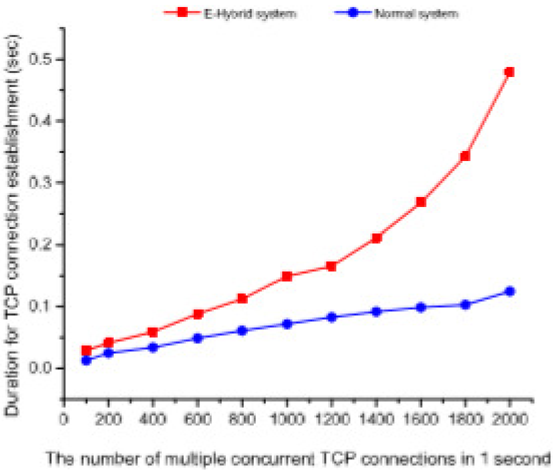


Fig. 6. Connection establishment time comparison

In E^2H^2 system, the high-interaction honeypot creation step runs along with the scanning attack process of the attacker. The main latency comes from the first data process step when we select the image id of high-interaction honeypots and choose some services which will be attacked by the attacker. In the Figure 6, that latency seems very small. Even when the attacker sends 2000 TCP connections per 1 second, the latency of our system is just 0.4 seconds. It is acceptable since this latency does not cause any suspicion to the attacker.

5. CONCLUSIONS

In this paper, we proposed Efficient Elastic-Hybrid Honeynet system, a new architecture for honeynet to enhance the efficiency of using resources. Moreover, by using different type of honeypots to deal with different phases of attacks, this system can obtain the advantages of both low-interaction and high-interaction honeypots. The system not only gains the wide coverage types of network traffic but also gets the high behavioral fidelity. Currently, while implementing E2H2 system in the real world, we have gotten some optimal results. In the future, we will try to reduce the response time of the low-interaction honeypot and deploy this system in some large-scale networks in order to make it be practical for enterprise environment.

ACKNOWLEDGEMENTS

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00254, SDN security technology development)

REFERENCES

[1] L. Spitzner, ”Honeypots: Catching the insider threat,” In the IEEE 19th Annual Conference on Computer Security Applications, pp.170179, 2003.

[2] Seifert, C., Welch, I., and Komisarczuk, P., Taxonomy of Honeypots. [Online]. Available: http://www.mcs.vuw.ac.nz/comp/ Publications/archive/CS-TR-06/CS-TR-06-12.pdf.

[3] Black Hat USA 2015 - Breaking Honeypots For Fun And Profit. [Online]. Available: https://www.youtube.com/watch?v=Pjvr25lMKSY.

[4] J. H. Jafarian, E. Al-Shaer, and Q. Duan, ”Adversary-aware IP address randomization for proactive agility against sophisticated attackers,” in Proceedings of the IEEE Conference on Computer Communications, pp. 738746, April, 2015.

[5]Marcin Nawrocki, Matthias Whlisch, Thomas C. Schmidt, Christian Keil, Jochen Schnfelder, ”A Survey on Honeypot Software and Data Analysis,” August, 2016.

[6] Bailey, M., Cooke, E., Watson, D., Jahanian, F., Provos, N.: A hybrid honeypot architecture for scalable network monitoring. Technical Report CSE-TR-499-04, U. Michigan, October 2004.

[7] FAN, Wenjun, et al. ”Dynamic Hybrid Honeypot System Based Transparent Traffic Redirection Mechanism,” In International Conference on Information and Communications Security, pp.311-319, 2015.

[8] Lengyel, T.K., Neumann, J., Maresca, S., Kiayias, A., ”Towards hybrid honeynets via virtual machine introspection and cloning,” In: Lopez, J., Huang, X., Sandhu, R. (eds.) NSS 2013. LNCS, vol. 7873, pp. 164177. Springer, Heidelberg (2013).

[9] HAN. Wonkyu, et al. HoneyMix, ”Toward SDN-based Intelligent Honeynet,” In Proceedings of the 2016 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, pp.1-6, 2016.

[10] ETSI GS NFV-MAN Network Functions Virtualization (NFV); Management and Orchestration v1.1.1, Dec. 2014. [Online]. Available: http://www.etsi.org/deliver/etsi gs/NFVMAN/001 099/001/01.01.01 60/gs NFV-MAN001v010101p.pdf.

[11] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, ”Openflow: enabling innovation in campus networks,” ACM SIGCOMM Computer Communication Review, 38(2):6974, 2008.

[12]C. Leita, V. Pham, O. Thonnard, E. Ramirez-Silva, F. Pouget, E. Kirda, and M. Dacier, The leurre. com project: collecting internet threats information using a worldwide distributed honeynet, in Information Security Threats Data Collection and Sharing, 2008. WISTDCS08. WOMBAT Workshop on, pp. 4057, 2008.

[13] V. Yegneswaran, P. Barford, and V. Paxson, Using honeynets for internet situational awareness, in Proceedings of the Fourth Workshop on Hot Topics in Networks (HotNets IV). Citeseer, pp.1722, 2005.

[14] P. Baecher, M. Koetter, T. Holz, M. Dornseif, and F. Freiling, The nepenthes platform: An efficient approach to collect malware, in Recent Advances in Intrusion Detection. Springer, pp. 165184, 2006.

[15]M. Gruber, D. Hoffstadt, A. Aziz, F. Fankhauser, C. Schanes, E. Rathgeb, and T. Grechenig, Global voip security threatslarge scale validation based on independent honeynets, in IFIP Networking Conference (IFIP Networking), pp. 19, 2015.

[16] M. Wahlisch, A. Vorbach, C. Keil, J. Sch onfelder, T. C. Schmidt, and J. H. Schiller, Design, implementation, and operation of a mobile honeypot. [Online]. Available: http://arxiv.org/abs/1301.7257.

INTENTIONAL BLANK

A MACHINE LEARNING APPROACH TO DETECT AND CLASSIFY 3D TWO-PHOTON POLYMERIZATION MICROSTRUCTURES USING OPTICAL MICROSCOPY IMAGES

Israel Goytom and Gu Yinwei

Department of Microelectronics Science and Engineering,
Faculty of Science, Ningbo University, Ningbo,315211,China

ABSTRACT

For 3D microstructures fabricated by two-photon polymerization, a practical approach of machine learning for detection and classification in their optical microscopic images is state and demonstrated in this paper. It is based on Faster R-CNN, Multi-label classification (MLC) and Residual learning framework Algorithms for reliable, automated detection and accurate labeling of Two Photo Polymerization (TPP) microstructures. From finding and detecting the microstructures from a different location in the microscope slide, matching different shapes of the microstructures classify them among their categories is fully automated. The results are compared with manual examination and SEM images of the microstructures for the accuracy test. Some modifications of ordinary optical Microscope so as to make it automated and by applying Deep learning and Image processing algorithms we can successfully detect, label and classify 3D microstructures, designing the neural network model for each phase and by training them using the datasets we have made, the dataset is a set of different images from different angles and their annotation we can achieve high accuracy. The accurate microstructure detection technique in the combination of image processing and computer vision help to simulate the values of each pixel and classify the Microstructures.

KEYWORDS

Multi-label classification, Faster R-CNN Two-Photon Polymerization, computer vision, 3D Microstructures

1. INTRODUCTION

In the last two decades, two-photon polymerization (TPP) has been established as a versatile tool for the microfabrication of three-dimensional structures [1]. Applications include the fabrication of photonic crystals [2], directly printed lens systems [3], micro fluidic devices[3], biological scaffolds[4] and templates for metamaterials[5]. In general, TPP relies on similar principles as known for common optical lithography, namely, exposure of an often-negative photo resist and a wet development process followed by the drying of the structures. Most of the 3D conductive patterns in the literature are fabricated using a layer-by-layer strategy with planar lithography techniques. On the other side to see and study the 2D microstructures we can use the optical microscope while the 3D microstructures see by either 3D microscopes or scanning electron microscope (SEM). Microscopes are a widely used optical instrument at this stage optical microscopes can amplify the objects up-to Micron size· It amplifies the observed objects through the optical system and displays the microstructure to recognize and study the characteristics of the objects from the microform. Currently, it has been widely used in biology, pathology, cell

Dhinaharan Nagamalai et al. (Eds) : CSEIT, NCS, SPM, NeTCoM - 2018
pp. 129–136, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81810

histology, genetics, clinical diagnosis, materials testing, aviation and space technology, geology and archeology, Electronic components performance testing and analysis and other fields.A traditional microscope looks at the sample from one specific direction and acquires a two-dimensional (2D) projection of the sample in that direction. Although the information collected by a conventional microscope is beneficial in understanding the microstructures of the sample, under many circumstances 2D information alone is not enough or even confusing. In recent decades deep learning techniques are being used for all different purposes with great success and are becoming more popular within various disciplines. Because of its generality, similar architectures put together through deep learning can be applied to many classification problems. Within the given amount of data, they are increasingly being used as a tool for multi-label classification [6]. Applying Deep learning algorithms for Detection of Microstructures results in efficiency, fast and accurate. Separating any structures in the Microscope slides is an outcome of image processing like thresholding and edge detection. On the machine learning side, there is a pre-training phase because there is no previous dataset available for this area we need a pre-training phase. In the pre-training phase, we need to collect images for the dataset and labeling them manually; this will help us to make datasets for Faster R-CNN and MLC. After we build the dataset let’s review the Faster R-CNN architecture, along with its earlier variants, by Girshick et al. [7]– [9] The R-CNN architecture has gone under a few iterations and improvements, but with the latest Faster R-CNN architecture, we can train end-to-end deep learning object detectors. The architecture itself includes four primary components. The first component is the base network (i.e., ResNet[10], VGGNet[11], etc.) which is used as a feature extractor. We then have the Region Proposal Network (RPN), which accepts a set of anchors, and outputs proposals as to where it thinks objects are in an image. Because RPN does not know what the object is in the image, rather a potential object exists at a given location. The region of Interest Pooling is used to extract feature maps from each proposal region. Finally, a Region-based Convolutional Neural Network is used to obtain the final class label predictions for the proposal and further refine the proposal locations for better accuracy. Given a large number of moving parts in the R-CNN architecture, we didn’t want to implement the entire architecture by hand, Instead, it's we use the TensorFlow Object Detection API [12] the TensorFlow Object Detection API is an open source framework built on top of TensorFlow that makes it easy to construct, train and deploy object detection models. After training the detection model, train our model using multi labeling algorithm[6] which is useful for classifying different types of samples. By using our trained models, we can detect samples from the slide, matching the sample and classify the sample. Image processing and Deep learning integrated when it comes to counting the pixels with edges and later on make the 3D Model simulation or 3D construction. Making the dataset is collecting images and labeling them, to collect the images we use mini servo motor attached to microscope knobs (mechanically modified) and take sequenced images, labeling the collection and use them as a separate file in one compression. Preparing the dataset images for training our classifier network contains reshaping the layers to 2D array form, the use of reshaped layers is to change the shape of the data back into a 2D image for the convolutional layer. For convolutional layers, we need to select how many filters, and the size of the convolution area like too small or too large and we won't be able to obtain interesting features. The dropout layers, the dropout rate is also important to balance learning and overfitting. Each input is represented as 64×64 grayscale image; we will simply resize our 640x480 images to 64×64 using Open CV resize function or any other like Pillow's resize. These resized grayscale pixel intensities are unsigned integers, with the values of the pixels falling in the range [0, 255]. All digits are placed on a black background with a light foreground (i.e., the sample itself) being white and various shades of gray. Modification of the Microscope was done by mechanically attaching servo and stepper motors to the Microscope knobs. The servo controlling mechanism is, within a given range of the rotation **R** If the range of the servo motor is from 0 to 90 degrees. To get the pixel values of the sample in the Z direction by giving the height of the structure and range factor is calculated from the angle difference of the maximum angle. With each and given T (where T is the time used to rotate the servo motor by one angle) there will be X frames which will be saved as new frame arrays.

2. RESULTS

2.1. Our Dataset:

We have collected around ~10,000 positive images from each of five different types of microstructures. We added mini servo motor to the focus knobs (Fine Adjustment) of the microscope, by rotating the servo motor in given angle T we can get a unique image feature from the sample. Applying traditional image processing techniques thresholding, edge detection and Gaussian smoothing techniques used to binarize and augmentation. Our dataset contains images and label file which includes file name, height, type, and xMins, xMaxs, yMins, and yMaxs.The xMins, xMaxs, yMins, and yMaxs will store the (x; y)-coordinates for our bounding boxes, respectively. The Labels list is a list of human-readable class labels for each bounding box. Similarly, we have classes, a list of integer IDs for each class label. We make a constructor which merely performing a series of initializations from our dataset, then export the constructor values as output and make them annotation file for training.

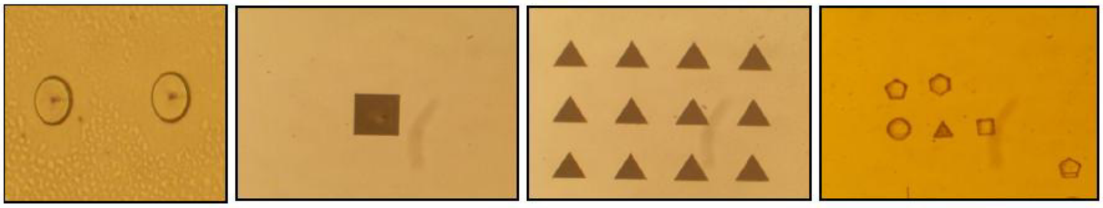


Figure 1. Different types of Microstructures fabricated using TPP

2.2. Our Model:

We have prepared two models for detection and classification. We use Tensorflow object detection-API for detection and Multi-label classification for a class classifier. The F-RCNN we use in this paper has four stages; Input an Image, Extract region proposals (regions of the image that potentially contain objects) by using selective search, use transfer learning for feature extraction to compute features for each proposal (effectively an ROI) using pre-trained CNN and classify each proposal using the extracted features with a support vector machine (SVM). The architecture is end-to-end trainable, and the complete object detection pipeline takes place inside the network this includes Regional Proposal, Feature extraction, computing the bounding box coordinates of the box. For the training we separate our dataset 80 % for training and 20 % for testing, we use ResNet-101 as base network (feature extractor), then our RPN which accepts anchors and outputs proposals, here we know that our RPN doesn't know what the object is in the image, our RoI (region of interest) pooling is used to extract feature maps from each proposal region ,and finally a Region based CNN is used to obtain the final class label predictions for the proposal and further refine the proposal location for better accuracy. We have trained using NVIDIA GTX 1080ti GPU, and by the time we reach step 20,000 the loss value is a ~ 0.03 with 97 % mAP. We test the model on NVIDIA Jetson TX2 for autonomous mode, and we have reached 9 FPS (frame per second) speed for real-time detection.

2.3. Train Our Model:

After Design the Network structure using Multi-label classification and Residual learning framework we trained our model using our dataset using Keras for classifier and TFOD API for detection. For the classifier, we used the images containing our Sample gathered using previous Technique and randomly 20000~ Images that do not include our samples. Reshaping each image to get the filtered data is the preprocessing of the Program. The model has a similar structure with

Le-net. We have classified our dataset as 80% training and 20% test data. For detection, we work on Tensorflow object detection API. When working with the TFOD API, we need to re-build a dataset consisting of both the images and their associated bounding boxes. However, before we can get to building the dataset, we need to consider

what makes up "data point" for object detection? According to the TFOD API, we need to supply some attributes, including:

- The TensorFlow-encoded image
- The width and height of the image
- The file encoding of the image (i.e., JPG, PNG, etc.)
- The filename
- A list of bounding box coordinates, normalized in the range [0;1], for the image
- A list of class labels for each bounding box

We make a constructor which merely performing a series of initializations. The xMins, xMaxs, yMins, and yMaxs will store the (x; y)-coordinates for our bounding boxes, respectively. The textLabels list is a list of human-readable class labels for each bounding box. Similarly, we have classes, a list of integer IDs for each class label. Then save export the constructor values as output and make them annotation file for training.

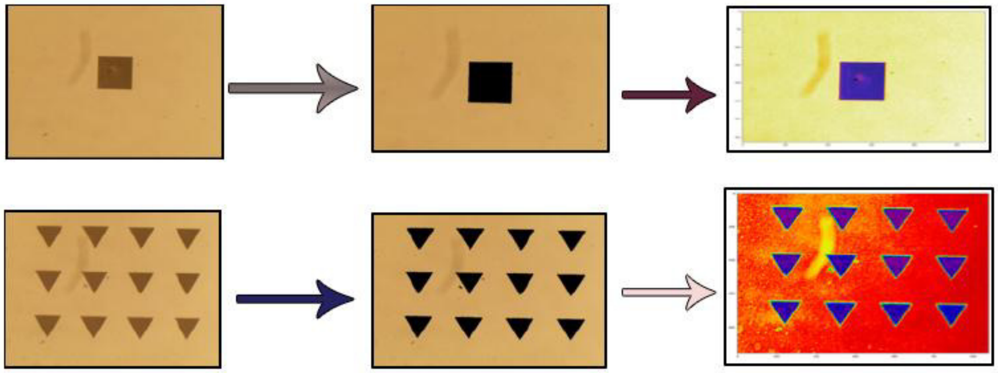


Figure 2. Making Roi and Define Each edge for Training. ***Left*** Input Images ***Middle*** Encoding Image's Edges ***Right*** Getting The xMins, xMaxs, yMins, and yMaxs from (x:y) coordinates

Training Network Architecture steps:

1. Input an image
2. Extract regions proposals (i.e., regions of the image that potentially contain objects) using an algorithm such as Selective Search [13].
3. Use transfer learning, specifically feature extraction, to compute features for each proposal (which is an effectively an ROI) using the pre-trained CNN.
4. Classify each proposal using the extracted features with a Support Vector Machine (SVM).

2.4. Test Our Model:

To test our models, we have to handle scaling our image to the range [0, 1], converting it to an array and adding an extra dimension. As we train/, classify images in batches with CNNs. Adding an extra dimension to the array using NumPy arrays which allows our image to have the shape that we want. All our models succeeded with detecting Samples and Non-Samples and classification of the sample. Detecting the microstructures by accepting the thresholding and masked images, export the detected microstructures then train the classifier to classify under desired Samples label category. Identifying (classifying) type of the sample from the category list and focusing to each unique edge to draw their equivalent 3D model all required training using labeling uniquely from single input has been done under testing the model.

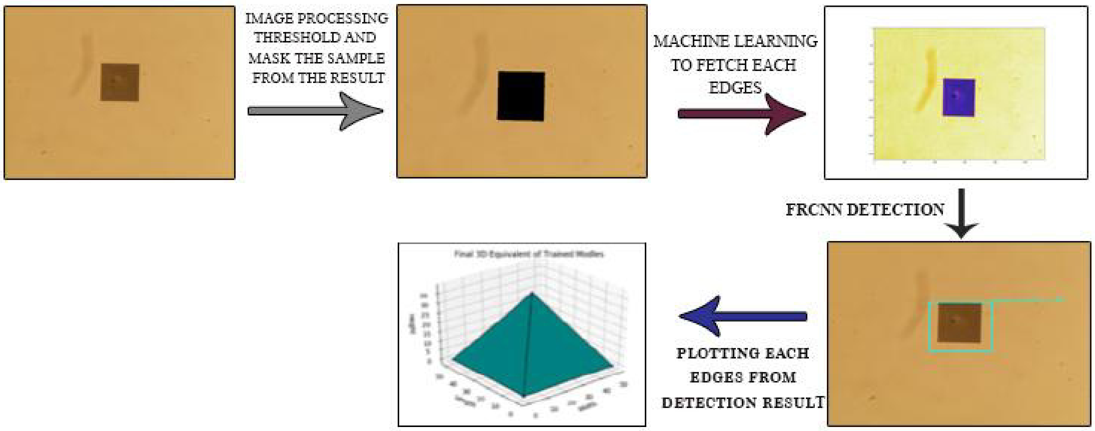


IMAGE PROCESSING THRESHOLD AND MASK THE SAMPLE FROM THE RESULT
MACHINE LEARNING TO FETCH EACH EDGES
FRCNN DETECTION
PLOTTING EACH EDGES FROM DETECTION RESULT
Final 3D Equivalent of Trained Modles

Figure 3. The image analysis protocol with tensor-based analysis and edge estimation for detection and classification of the Microstructures.

2.5. Finding the Sample Using CNN and CV (The Automated)

After we put our slide on the microscope, the program will start to find the sample by controlling the stepper motors using Arduino when the Arduino is connected and managed by the Machine learning based scripts running on the Nvidia Jetson TX. We use computer vision to differ the plane and any blobs. When there is a blob on the slide, the motion is paused to know the blobs are either dirty or real sample, to analyze this we use our trained model if the detected object is our sample we will save the location into NumPy arrays for later analysis. This process is continuous from the slice X_0, Y_0, Z_0 to X_n, Y_n, Z_n.

2.6. Detecting the structures From the Slice:

By using one of the Image Processing technique thresholding [14], we can apart the image into structures and background. Image thresholding [14] is yet effective way of partitioning an image into a foreground and background. This image analysis technique is a type of image segmentation that isolates objects by converting grayscale images into binary images. By thresholding, we can differentiate any structures in the slide. Thresholding image will make our detection more accurate; many Deep Learning techniques use the specific location of the object they want to detect to Train their Neural Network [15] in Fig (5 (b)) We applied different types of thresholding methods [16] according to their effectiveness on different edges. By thresholding, we can speed up out detector network because our detector network won't check every object in given frame.

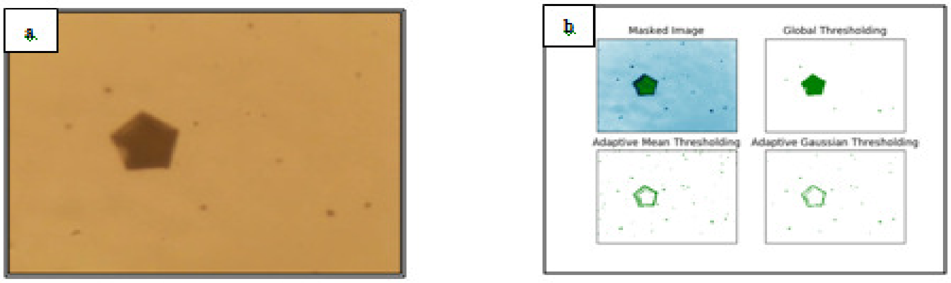


Figure 4. (a) Input Original Image (b) Thresholding Input image using Global,
Adaptive Mean, and Adaptive Gaussian thresholding.

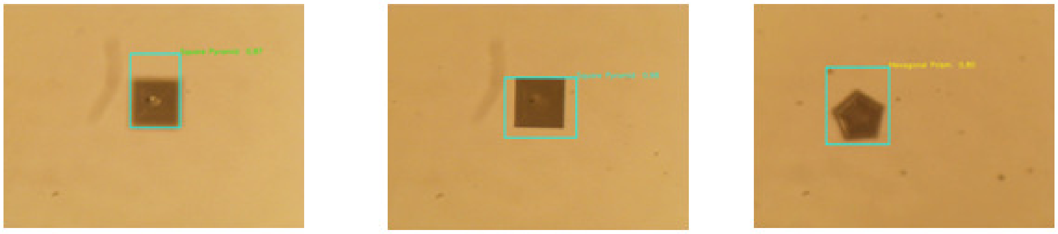


Figure 5. Detection Result using Faster R-CNN

Augmentation

As we have a limited number of Positive data and our Classifier and detector network big data for better accuracy, we need to augment our input images for the Augmentation of our simple augmented data generator. The augmentation code state as follows.

```
aug=ImageDataGenerator(rotation_range=30,width_shift_range=0.1,height_shift_range=0.1,shear_range=0
.2,zoom_range = 0.2,horizontal_flip=True, fill_mode="nearest")
```

3. Conclusion and Future Works:

We have performed an experiment of different types of Two-Photon Polymerization (TPP) Microstructures and detected them from their Optical Microscopy real-time Image and classify their 3D structure type. The main aspects that influence the speed and accuracy of the object detectors methods that we have been used are the complexity of the designed structures like many dimensional images, after all, we compared the results with SEM images, and manual examination the results are almost similar with 25 % faster detection speed in dense slides. We hope this will help practitioners and Researchers choose an appropriate AI method for detection. We have also identified some new techniques for classification without sacrificing much accuracy. Auto focusing to the Widest Edge which will help to see the exact structure at a given time and 3D plotting from their 2D input which will help to get the 3D image in matplotlib 3D axis. This work is available at https://github.com/isrugeek/2dto3d/

Acknowledgment:

Ningbo University Faculty of Science supported this work, and we would like to acknowledge Professor Zhou for Nvidia GPU and Jetson TX2 support, Dr. Lin Dong Dong and Professor Weidong Tao for reviewing our Paper before Submission.

Author Contributions

Israel Goytom developed the machine learning algorithms, performed the image analyses, and wrote the manuscript. Gu Yinwei, did the TPP experiments, preparing the 3D structure, observed the microstructures, performed the SEM image analysis, making up the device in machine mechanical part and wrote the manuscript. The manuscript was written up through contributions of all authors. All authors have approved the final version of the manuscript.

Competing Interests

The author(s) declare no competing interests

REFERENCES

[1] K. S. Lee, R. H. Kim, D. Y. Yang, and S. H. Park, "Advances in 3D nano/microfabrication using two-photon initiated polymerization," Progress in Polymer Science (Oxford), vol. 33, no. 6. pp. 631–681, 2008.

[2] M. Rybin et al., "Band Structure of Photonic Crystals Fabricated by Two-Photon Polymerization," Crystals, vol. 5, no. 1, pp. 61–73, 2015.

[3] S. Thiele, K. Arzenbacher, T. Gissibl, H. Giessen, and A. M. Herkommer, "3D-printed eagle eye: Compound microlens system for foveated imaging," Sci. Adv., vol. 3, no. 2, 2017.

[4] L. Valdevit and J. Bauer, "Fabrication of 3D Micro-Architected/Nano-Architected Materials," in Three-Dimensional Microfabrication Using Two-Photon Polymerization: Fundamentals, Technology, and Applications, 2015, pp. 345–373.

[5] X. Zheng et al., "Multiscale metallic metamaterials," Nat. Mater., vol. 15, no. 10, pp. 1100–1106, Oct. 2016.

[6] J.Read and F.Perez-Cruz, "Deep Learning for Multi-label Classification," arXiv Prepr. arXiv1502. 05988, pp. 1–8, 2014.

[7] R. Girshick, J. Donahue, T. Darrell, and J. Malik, "Rich feature hierarchies for accurate object detection and semantic segmentation," Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., pp. 580–587, 2014.

[8] K. Buhler et al., "Fast R-CNN," Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., vol. 2015 Inter, no. Voc 2012, pp. 580–587, 2015.

[9] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks," IEEE Trans. Pattern Anal. Mach. Intell., vol. 39, no. 6, pp. 1137–1149, 2017.

[10] S. Wu, S. Zhong, and Y. Liu, "Deep residual learning for image steganalysis," Multimed. Tools Appl., pp. 1–17, 2017.

[11] K. Simonyan and A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Image Recognition," pp. 1–14, 2014.

[12] J. Huang et al., "Speed/accuracy trade-offs for modern convolutional object detectors," Proc. - 30th IEEE Conf. Comput. Vis. Pattern Recognition, CVPR 2017, vol. 2017–Janua, pp. 3296–3305, 2017.

[13] J. R. R. Uijlings, K. E. A. Van De Sande, T. Gevers, and A. W. M. Smeulders, "Selective Search for Object Recognition," 2012.

[14] H. K. A. Devi, “Thresholding: A Pixel-Level Image Processing Methodology Preprocessing Technique for an OCR System for the Brahmi Script,” Anc. Asia, vol. 1, no. 0, p. 161, Dec. 2006.

[15] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “ImageNet Classification with Deep Convolutional Neural Networks.”

[16] P. K. Sahoo, S. Soltani, and A. K. C. Wong, “A survey of thresholding techniques,” Computer Vision, Graphics and Image Processing, vol. 41, no. 2. pp. 233–260, 1988.

Additional Resources

1. https://github.com/tensorflow/models/blob/master/research/object_detection
2. https://docs.opencv.org/2.4/modules/imgproc/doc/geometric_transformations.html?highlight=resize#cv2.resize
3. https://pillow.readthedocs.io/en/5.2.x/releasenotes/2.7.0.html?highlight=resize
4. https://www.nvidia.com/zh-cn/autonomous-machines/embedded-systems-dev-kits-modules/

Authors

Israel Goytom

Israel Goytom is Degree Student with Microelectronics Science and Engineering Major in Ningbo University. My research areas are an application of Deep learning and Computer Vision in Physics, Optics and Robotics.

Gu Yinwei

I am a Master’s Degree student of the Faculty of Science in Ningbo University. My research areas are Two-photon microstructure processing.

VIDEO SEQUENCING BASED FACIAL EXPRESSION DETECTION WITH 3D LOCAL BINARY PATTERN VARIANTS

Kennedy Chengeta and Serestine Viriri

[1]University of KwaZulu Natal
[2]School of Computer Science and Mathematics,
Westville Campus, Durban, South Africa

ABSTARCT

Facial expression recognition in the field of computer vision and texture synthesis is in two forms namely static image analysis and dynamic video textures. The former involves 2D image texture synthesis and the latter dynamic textures where video sequences are extended into the temporal domain taking into account motion. The spatial domain texture involves image textures comparable to the actual texture and the dynamic texture synthesis involves videos which are given dynamic textures extended in a spatial or temporal domain. Facial actions cause local appearance changes over time, and thus dynamic texture descriptors should inherently be more suitable for facial action detection than their static variants. A video sequence is defined as a spatial temporal collection of texture in the temporal domain where dynamic features are extracted. The paper uses LBP-TOP which is a Local Binary Pattern variant to extract facial expression features from a sequence of video datasets. Gabor Filters are also applied to the feature extraction method. Volume Local Binary Patterns are then used to combine the texture, motion and appearance. A tracker was used to locate the facial image as a point in the deformation space. VLBP and LBP-TOP clearly outperformed the earlier approaches due to inclusion of local processing, robustness to monotonic gray-scale changes, and simple computation. The study used Facial Expressions and Emotions Database(FEED) and CK+ databases. The study for the LBP -TOP and LGBP-TOP achieved bettered percentage recognition rate compared to the static image local binary pattern with a set of 333 sequences from the Cohn–Kanade database.

KEYWORDS

Local binary patterns on Three Orthogonal Planes (LBPTOP) · Volume Local Binary Patterns(VLBP)

1. INTRODUCTION

Video based facial expression analysis has received prominent roles of late, in crowd analysis, security and border control among others[13]. Its also used in image retrieval, clinical research centers and social communication. Facial expressions remain the most effective way of emotion display. Previous work on 2D facial expression recognition has focused more into single image frame based analysis than video or image sequence analysis. The former assumes one image is

Dhinaharan Nagamalai et al. (Eds) : CSEIT, NCS, SPM, NeTCoM - 2018
pp. 137–149, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81811

representing the facial expression where as for the video image sequence, each facial image is a temporal dynamic process[14, 15, 11].

The study focuses on facial motions and locating key facial components namely, nose, eyes, face and mouth. The dynamic features are then extracted using key algorithms like local Gabor binary patterns from three orthogonal planes (LGBP-TOP) which is a LBP variant with Gabor filtering as well [14, 15, 11]. This feature descriptor (LBP from Three Orthogonal Planes LBP-TOP) is proposed to extract dynamic textures from video sequences to characterize facial appearance changes [14, 15, 11]. The facial expression video image sequences are then modeled as a histogram sequence which is a sum of concatenated local facial regions[1]. Support Vector Machines and KNN algorithms are used to classify the datasets. The experiments used the extended Cohn-Kanade (CK+) database and the FEED database. The facial expression sequence is modeled as a histogram sequence by concatenating the histogram pieces of all the local regions of all the LGBP-TOP maps. For recognition, support vector machine (SVM) is exploited. The experimental results on the extended Cohn-Kanade database (CK+) demonstrate that the proposed method has achieved the best results compared to other methods in recent years.

Video-based face recognition system typically consists of face detection, tracking and recognition[16, 10, 6, 17]. The video sequences picked up depict key universal expressions (surprise, sadness, joy, disgust and anger). Each signal expression is performed by 7 different subjects beginning from the neutral expression. This paper mainly focuses on the integration of spatial-temporal motion LBP with Gabor multi-orientation fusion and compares the 3 LBP histograms on three orthogonal planes to accuracy of face expression recognition[1, 14]. An ensemble voting classifier is used for each plane and the overall LBP-TOP algorithm. The LBP-TOP is also compared against its variants like LBP-MOP [1, 14]. Experiments conducted on the extended Cohn-Kanade (CK+) database and FEED database show that our approach is robust in dealing with video-based facial expression recognition problems compared better than the 2D image texture local binary pattern variants.

2. Literature Review

In recent researches use of spatio-temporal representations has been successfully used to address limitations of static image analysis[8, 3–5, 2]. Successful research has been done by fusing PCA, Gabor Wavelets, local binary patterns permanent features like eyes ,moth or lips' feature vectors were generated from the facial appearances in the spatial and the frequency domains. And local directional patterns. Classification has included support vector machines(SVM), Adaboost, k-nearest neighbor and neural networks[7, 8, 14]. The permanent features like eyes ,moth or lips' feature vectors were generated from the facial appearances in the spatial and the frequency domains.

2.1. Static Facial Expression Analysis Background

Clinical research has been widely studied with 2D images either as a combination of facial expressions in 2D images or universal global facial [7, 8, 3, 5] The Facial Action Coding System (FACS) has been developed to describe facial expressions using a combination of action units (AU)[7, 8, 3, 5]. Each action unit corresponds to a specific muscular activity that produces momentary changes in facial appearance. The global facial expression handles the expressions as a whole without breaking up into AUs. The most commonly studied universal expressions include happiness, sadness, anger and fear, which are referred to as universal emotions. While most of the work has been on static 2D images, the Facial Expression Coding System (FACES) has been designed to analyze videos of facial expressions, in terms of the duration, content and valence of universal expressions [7, 8, 3, 5]. However, these methods need intensive human intervention to rate the images and videos of facial expressions. Such rating methods are prone to subjective errors, and have difficulties in providing unified quantitative measurements. There is need for automated, objective and quantitative measurements of facial expressions.

Challenges with static 2D images Based Methods Major clinical research in facial expression analysis includes subjective and qualitative scenarios in the 2D image family[8, 3]. The 2D static images lack temporary dynamics[14, 4, 13, 15, 16, 18]. They also are prone to subjectivity and poor qualitative features. The 2D static images do not capture temporary dynamics and expression changes [14, 4, 13, 15, 16, 18]. Therefore, there was need for automated, objective and quantitative measurements of facial expressions captured using videos. In this paper, we present a computational framework that uses videos for the analysis of facial expression changes. This framework explores the dynamic information that is not captured by static images during emotion processing, and provides computationally robust results [14, 4, 13, 15, 16, 18]. The study's chosen framework includes the video face detection and tracking incorporating shape variability. Based on tracking results, features are extracted from faces and then weighted facial expression classifiers applied on the given histograms[18, 1].

2.2. Facial Recognition With Video Image Sequences

Temporal information has capability to improve static image classification. In the work of Yacoob et al. , each facial expression is divided into three segments: the beginning, the apex and the ending [18, 14, 15, 2, 1]. Rules are defined to determine the temporal model of facial expressions. Such rules are ad-hoc and cannot be generalized to complex environments. In the work of Cohen et al., facial expressions are represented in terms of magnitudes of predefined facial motions, termed Motion-Units (MU) [18, 1]. A Tree-Augmented-Naive Bayes classifier is successfully applied to recognize facial expressions on static images, and then a multi-level Hidden Markov Model (HMM) structure is applied to recognize video sequences based facial expressions [14, 16]. Yeasin et al. applied a two stage approach to classify images in 3D by measuring the video intensity as we; using optical flow [1, ?,16]. Several probabilistic methods like particle filtering and condensation can also track facial expression in video sequences [18, 1]. Separate manifold substances have also been applied in video based facial expression analysis. To track video sequences models like 3d wireframe models, facial mesh models, net models and ASM models were successfully used. Videos subtle changes of facial expression can be measured on video facial expression recognition than on static image analysis[14, 16, 1, 10, 12].

3. Local Based Facial Expression Feature Extraction

Facial expression analysis influences wide areas in human computer interaction. Local binary patterns and their wide 2D and 3D variants have been used in this field. Holistic and local based feature extractors have been used successfully. PCA are prominent holistic algorithms and local binary patterns, Gabor filters and Gabor wavelets and local directional patterns have been successfully applied as local feature extractors.

3.1. Local Binary Patterns (LBP) For Static Image Feature Extraction

Local binary patterns are based on facial images being split into local sub regions. The challenges of facial occlusion and rigidness are faced though grey scale image conversion is used to reduce illumination[8, 7, 3]. Local binary patterns are invariant to grey level images. Localized feature vectors derived are then used to form the histogram which is used by machine learning classifiers or deep learning methods. The local features are position dependent [8, 7, 3]. For local binary patterns, the facial region is divided into small blockers like mouth, eyes, ears, nose and forehead[4]. The basic local binary pattern non center pixels use the central pixel as the threshold value taking binary values [8, 7, 3]. Uniform binary patterns are characterized by a uniformity measure corresponding to the bitwise transition changes. The local binary pattern has 256 texture patterns. The local binary LBP r,n operator is represented mathematically as follows The LBP feature for a local neighborhood of radius r, with n number of neighbor pixels is defined as:

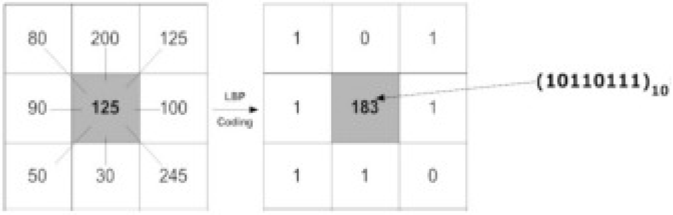


Fig. 1. Local Binary Patterns (LBP)

$$LBP_{(n,r)} = \sum_{n-1}^{n=0} s(p_n - p_c)2^n. \tag{1}$$

The neighborhood is depicted as an m-bit binary string leading to n unique values for the local binary pattern code. The grey level is represented by 2n-bin distinct codes. The value pc is the grayscale value of the center pixel, pn is the gray scale value of a neighbor pixel

LBP Variants Various LBP variants were successfully proposed and used. These include TLBP for Ternary Local Binary Pattern as well as Central Symmetric Local Binary Patterns [8, 9, 4]. Over-Complete Local Binary Patterns (OCLBP) is another key variant that takes into overlapping into adjacent image blocks. The rotation invariant LBP is designed to remove the effect of rotation by shifting the binary structure [8, 4]. Other variants include the monogenic and central symmetric (MCS-LBP).

Local directional patterns For local directional patterns or LDP a key edge detection local feature extractor, the images were divided into LDPx histograms, retrieved and then combined into one descriptor[9, 3, 5, 1, 11].

$$LDP_x(\sigma) = \sum_{K}^{r=0} \sum_{L}^{r=0} f(LDP_q(o,u),\sigma). \tag{2}$$

The local directionary pattern, includes edge detection using the kirsch algorithm.

For video sequencing facial image analysis Volume Local Directional Binary Pattern (VLDBP) and Local Gabor Binary Patterns from Three Orthogonal Planes have been successfully been used.

$$\begin{bmatrix}-3 & -3 & 5\\ -3 & 0 & 5\\ -3 & -3 & 5\end{bmatrix} \begin{bmatrix}-3 & 5 & 5\\ -3 & 0 & 5\\ -3 & -3 & -3\end{bmatrix} \begin{bmatrix}5 & 5 & 5\\ -3 & 0 & -3\\ -3 & -3 & -3\end{bmatrix} \begin{bmatrix}5 & 5 & -3\\ 5 & 0 & -3\\ -3 & -3 & -3\end{bmatrix}$$

$$\begin{bmatrix}5 & -3 & -3\\ 5 & 0 & -3\\ 5 & -3 & -3\end{bmatrix} \begin{bmatrix}-3 & -3 & -3\\ 5 & 0 & -3\\ 5 & 5 & -3\end{bmatrix} \begin{bmatrix}-3 & -3 & -3\\ -3 & 0 & -3\\ 5 & 5 & 5\end{bmatrix} \begin{bmatrix}-3 & -3 & -3\\ -3 & 0 & 5\\ -3 & 5 & 5\end{bmatrix}$$

Fig. 2. Local Directional Patterns (LDP)

Volume Local Directional Binary pattern (VLDBP) Volume Local Directional Binary pattern (VLDBP) is used as an extension of LBP in the dynamic texture field. Dynamic texture extends the temporal domain and is used in video image analysis. The face regions of the video sequence images are modeled with VLDBP which incorporates movement and appearance together. It uses three parallel planes and the middle plan contains the center pixel to derive the localized binary patterns. VLBP will also consider co-occurrence of all neighboring points from the 3 planes and generate binary representative codes. The extraction considers a local volumetric neighborhood against each pixel. The grey levels of the central pixels and the surrounding pixels are then compared against each other.

$$VLBP_{LPR} = \sum_{q=0}^{3P+1} v_q 2^q \tag{3}$$

3.2. Local Gabor Binary Patterns from Three Orthogonal Planes

3D dynamic texture recognition which concatenates three histograms from LBP on three orthogonal planes was proposed. The three orthogonal planes namely XY, XT, and YT have been widely [1, 14, 17]. LBP-TOP extracts features from the local neighborhoods over the 3 planes. The spatial-temporal information can be regarded as a set of volumes in the (X, Y, T) space, where X and Y represent the spatial coordinates, while T denotes the frame index (time) in temporal domain [1, 14, 15]. The neighborhood of each pixel no longer falls in a two dimensional space, where LBP operation can be used to extract features into histograms. Instead, we need to compute feature descriptor in the three dimensional space (X, Y, T). LBP-TOP was proposed to describe the spatial-temporal information in the three dimensional space. LBP-TOP computes the local binary patterns of a center pixel through thresh holding the neighboring pixels [1, 14, 17]. The algorithm decomposes the 3 dimensional volume into 3 orthogonal planes namely XY, XT and YT[1, 2]. The XY plane indicates appearances features in the spatial domain. The XT is a visual representation of a row with respect to time. The YT represents the features of motion for a column in the temporal space domain.

The spatial plane XY is similar to the regular LBP in static image analysis. The vertical spatio-temporal YT plane and horizontal XT plane are the other 2 planes in the 3 dimensional space. The resulting descriptor enables encoding of spatio-temporal information in video images. The performance and accuracy of the latter was also comparable to the LBP-TOP. The LBP STCLQP or spatio-temporal completed local quantized patterns (STCLQP) was also used to consider the pixel sign, orientation and size or magnitude. Local Gabor Binary Patterns from Three Orthogonal Planes (LGBPTOP) add Gabor Filtering to improve accuracy. With the added filtering algorithm rotational misalignment of consecutive facial images is mitigated[1, 16, 10]. To avoid LBP-TOP statistical instability, a re- parametrization technique whose foundation is second local Gaussian jet was proposed [1, 14, 17].

$$k = (H_L, X_Y, H_L, XT, H_L, Y_T, H_C, X_Y, HC, XT, HC, YT) \qquad (4)$$

(LBP/C)T OP feature is denoted in vector form where Hv, m (v= LBP or C, and m = XY,XT,YT where m = XY,XT,YT) are the 6 LBP sub-histograms which contrast feature in the three orthogonal planes [1, 14, 17]. The LBP-TOP algorithm describes video sequence changes in both spatial and temporal domains hence captures structural information of the former domain and longitudinal data of the latter [16, 18, 1]. LBP histogram features encode spatial data in the XY plane and the histograms from the XT and YT planes include the temporal and spatial data. With facial actions causing local and expression changes over time, the dynamic descriptors have an edge in facial expression analysis over the static descriptors [16, 18, 1].

$$H_i, j = \sum x, y, t f_j(x, y, t) = i \qquad (5)$$

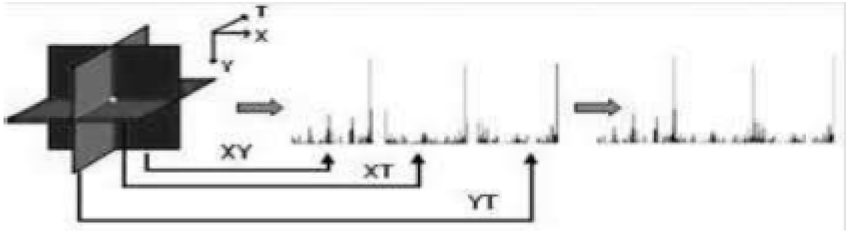


Fig. 3. LBP from three orthogonal planes. Three planes intersecting one pixel. LBP histogram of each plane and concatenating the histograms [1].

Likewise, the contrasts in the three orthogonal planes are also computed, which are denoted as Cm (m= XY, XT and YT) [1]. These contrast values are then represented as three sub-histograms Hx ,y (x= C and y= XY, XT , YT) [16, 18, 1]. Because of the contract, Cy is used to refer to the 3 features in all three orthogonal planes, and is called LBP CT-OP variant. Image device quality of the facial expression videos also impacts frame rates and spatial resolution quality as well [16, 18, 1].

Six Intersection Points (SIP) The LBP-SIP or Local Binary Pattern— Six Interception Points (LBP-SIP) considered 6 unique points along the intersecting lines of the 3 orthogonal planes to derive the binary pattern histograms [16, 18, 1].

$$AB, DF, EG = L_A \cap L_B \cap L_C \qquad (6)$$

where AB,DF and EG are intersection points. 6 unique neighbor points carry sufficient information to describe the spatio-temporal textures centered upon point C[16, 18, 1]. LBP-SIP produces a compact set of features in high dimensional features spaces where there is sparse data [16, 18, 1].

LBP-Three Mean Orthogonal Planes (MOP) LBP-MOP or mean orthogonal plane is another variant to have been successfully used by concatenating mean images from image stacks derived along the 3 orthogonal planes[16, 18, 1]. It also preserves essential image patterns and reduces redundancy which affects encoded features

4. Facial Expression Implementation

The implementation involves analyzing video streams to track facial feature points over time. The feature vectors are then calculated and emotions detected from the trained models. Training and classification of the models is done using the popular algorithms namely support vector machines, k-nearest neighbor and neural network machine learning classifiers. Recognition of the model and new expressions on new images is then done on the selected annotated databases which includes CK+ database and FEED database. The section describes the approach, databases selected and then classification algorithm chosen and implemented.

4.1. Approach

The study's objective was to recognize facial expressions from video sequences. The approach involved locating and tracking the faces and expressions during the video segmentation and sequential modeling phase. The video sequence detection involved landmark detection and tracking, which define the facial shapes[15]. Viola Jones openCV detection tools are used. The features were then extracted using various 3D video feature extraction variants of the LBP-TOP algorithm. Gabor filters [16, 18, 1, 12, 5] were then applied during preprocessing. Geometric features were normalized and they were immune from skin color and illumination changes. Several machine learning classifiers namely support vector machines, k-nearest neighbor and neural networks were used for the classification. The algorithm used is shown in Algorithm 1.The study analyzed a sequence of frames that change from one form to another to detect faces from a live video based on the CK+ dataset and the FEED dataset [16, 18, 1].

```
Data: Copy and preprocess video image datasets
Result: Facial expression classification results for the image datasets
while  For each image I inside the CK+ and FEED database do
        1.  divide the database into training and test sets;
        2.  for each image inside the given datasets;
        3.  apply Viola Jones algorithm for extraction and preprocess the image
        4.  using Principal Component Analysis;
        5.  extract the LBP-TOP, LBP-XY,LBP-XT and LBP-YT features;
        6.  extract the features using the LBP-MOP, LBP-SIP algorithm
        7.  apply Gabor Filters to get the LGBP-TOP and LGBP-MOP features
        8.  calculate the Euclidian distance matrix;
        9.  apply the classification on each with different classifiers;
        10. the best classification results is then labeled the best algorithm;
        End For'
end
```

Algorithm 1: Local Gabor Binary Patterns from Three Orthogonal Planes to analyse video sequences[20, 1]

4.2. Facial Expression Preprocessing

The first step of establishing the PCA classifier was to determine parameters such as the number of principal components to consider (PCs) and the number of training images [20, 1]. Gabor filters (a linear filter) were then used to detect edges in texture analysis. In the spatial domain. A given Gabor filter acts like a Gaussian kernel function modulated by a sinusoidal plane wave as shown in the equation below [20, 16, 18, 1] . The Gabor filters extract expression-invariant features.

$$G\_c[i,j] = Be^{-\frac{(i^2+j^2)}{2\sigma^2}} \cos(2\pi f(i\cos\theta + j\sin\theta)); \tag{7}$$

$$G\_s[i,j] = Ce^{-\frac{(i^2+j^2)}{2\sigma^2}} \sin(2\pi f(i\cos\theta + j\sin\theta)); \tag{8}$$

where B and C are normalizing factors that will be derived[20].

4.3. Facial Expression Databases

The study used video sequences lasting around 10 seconds with 15 second frames per second. The facial expressions are dynamic and evolve over time from the start, when reaching the apex and offsets. The video sequence datasets that could have been used included the CK+, YouTube Faces Database, Acted Facial Expressions in the Wild (AFEW) as well as the BU-3DFE, MMI+ dataset and the Facial Expressions and Emotions Database (FEED) [16, 18, 1]. The FEED dataset included 400 webcam video extracts from 18 voluntary participants in mpg format of sizes 480 times 640. There were labeled as 6 facial expression classes [16, 18, 1]. YouTube Faces Database data set contains over 3 000 videos from about a thousand and five hundred video sequence images. The videos average around 2 to 3 seconds and clips frame sizes from 48 to 6000 frames with a mean of 180. The BU-4DFE database has 101 subjects for identifying the emotion and it also has 83 feature points to recognize the emotion. In the total 101 subjects, 58 subjects are female and remaining 43 subjects are male. The study chose the FEED and CK+ dataset for implementation [16, 18, 1]. For static image analysis the study used the CK+ dataset and Google set dataset. The static image analysis was then compared to the video sequence databases.

CK+ dataset The CK+ dataset includes 593 video sequences and 7 expression types from 123 participants. The participants included African-Americans and euro- Americans and other races accounted for 6 percent [16, 18, 1]. The video sequences were 640 by 490 by 640 by 480 pixels. The grey images made with 8-bit precision made up the frames dataset[13]. The study used 90 participants and considered the 6 expressions namely anger, disgust, fear, happiness, sadness, and surprise[9].

4.4. Facial Expression Video Sequences Classification

The study uses the k-nearest neighbor, random forest, neural networks and support vector machines[19, 8, 5]. For a KNN machine learning classifier *k* NN, the nearest neighbor, given x_q, with *k* nearest discreet neighbors, will take a mean of *f* values of *k* nearest neighbors[19, 9, 12, 15].

$$kNN = f(x_q)\frac{\sum_{i=1}^{k} f(x_i)}{k} \qquad (9)$$

Support Vector Machine Support vector machines consider the that points close the given class boundaries[10]. A hyperplane is chosen to separate 2 classes which are initially given as linearly separable. The hyperplane separating the two classes is represented by the given equation[19, 9, 12, 15]:

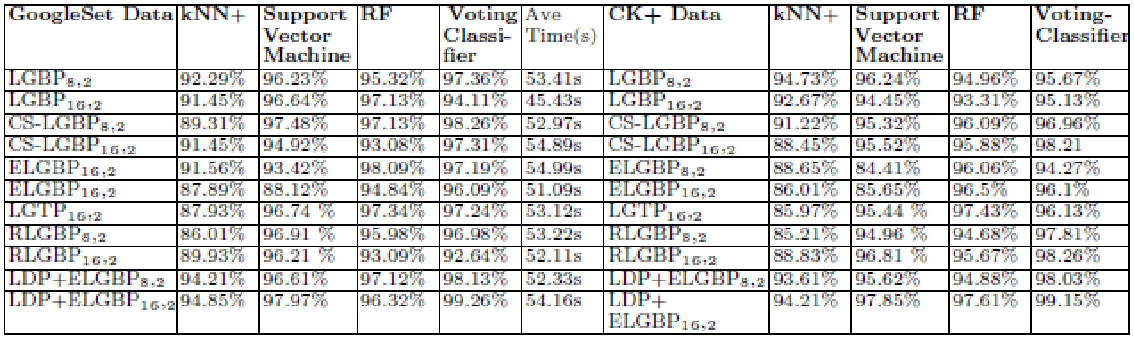
$$w^T x_n + b = 0, \qquad (10)$$

such that:

$$w^T, x_n + b1 \qquad y_n = +1, \qquad (11)$$

5. Experiment And Results

Static image analysis experimental results For the 2D experiments the CK+ dataset was tested against an ensemble of classifiers as well as major local binary and directional patterns. The highest results were experienced when local binary patterns and binary patterns were applied with an ensemble of classifiers. Whilst the 2D classification results showed greater accuracy they lacked the 3D and dynamic spatial properties. The best classification was found on a combined LBP+ELBP and Gabor Filters combination with a 16, 2 radius combination that resulted in a classification rate of 99.15 percent for the ensemble voting classifier. The voting classifier had support vector machines, random forests and k-nearest neighbour with a ratio of 2:4:2 respectively.



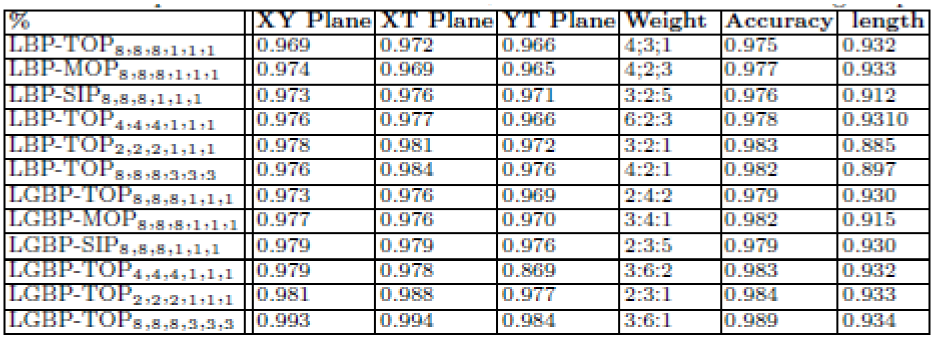
GoogleSet Data	kNN+	Support Vector Machine	RF	Voting Classi-fier	Ave Time(s)	CK+ Data	kNN+	Support Vector Machine	RF	Voting-Classifier
$LGBP_{8,2}$	92.29%	96.23%	95.32%	97.36%	53.41s	$LGBP_{8,2}$	94.73%	96.24%	94.96%	95.67%
$LGBP_{16,2}$	91.45%	96.64%	97.13%	94.11%	45.43s	$LGBP_{16,2}$	92.67%	94.45%	93.31%	95.13%
$CS\text{-}LGBP_{8,2}$	89.31%	97.48%	97.13%	98.26%	52.97s	$CS\text{-}LGBP_{8,2}$	91.22%	95.32%	96.09%	96.96%
$CS\text{-}LGBP_{16,2}$	91.45%	94.92%	93.08%	97.31%	54.89s	$CS\text{-}LGBP_{16,2}$	88.45%	95.52%	95.88%	98.21
$ELGBP_{16,2}$	91.56%	93.42%	98.09%	97.19%	54.99s	$ELGBP_{8,2}$	88.65%	84.41%	96.06%	94.27%
$ELGBP_{16,2}$	87.89%	88.12%	94.84%	96.09%	51.09s	$ELGBP_{16,2}$	86.01%	85.65%	96.5%	96.1%
$LGTP_{16,2}$	87.93%	96.74 %	97.34%	97.24%	53.12s	$LGTP_{16,2}$	85.97%	95.44 %	97.43%	96.13%
$RLGBP_{8,2}$	86.01%	96.91 %	95.98%	96.98%	53.22s	$RLGBP_{8,2}$	85.21%	94.96 %	94.68%	97.81%
$RLGBP_{16,2}$	89.93%	96.21 %	93.09%	92.64%	52.11s	$RLGBP_{16,2}$	88.83%	96.81 %	95.67%	98.26%
$LDP+ELGBP_{8,2}$	94.21%	96.61%	97.12%	98.13%	52.33s	$LDP+ELGBP_{8,2}$	93.61%	95.62%	94.88%	98.03%
$LDP+ELGBP_{16,2}$	94.85%	97.97%	96.32%	99.26%	54.16s	$LDP+ ELGBP_{16,2}$	94.21%	97.85%	97.61%	99.15%

Fig. 4. 2D static image classifier for CK+ and GoogleSet combined Dataset with Gabon Filters applied

5.1 Experimental Results on CK+ and FEED 3D Datasets

Three experiment types were executed on the CK+ dataset's facial motions. Recognition rates were executed for the LBP-XY plane, LBP-XT plane as well as the LBP-YT planes. The combined recognition rate for the LBP-TOP was also calculated.

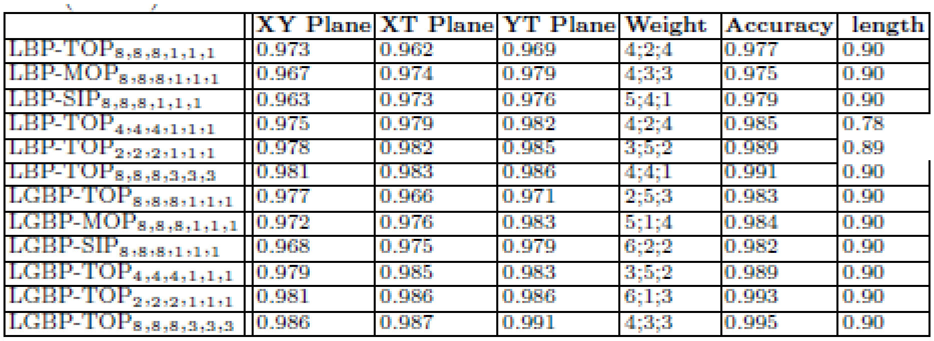
The 4 scenarios used an ensemble classifier of support vector machines, k-nearest neighbor as well as random forest classifiers with different weighted ratios. The following tables indicate classification of the CK+ and FEED datasets based on the XY, YT and XT plane dimensions with an average length of 0.9 seconds. The minimum length was 0.78 seconds and the highest length was 0.934 seconds.



%	XY Plane	XT Plane	YT Plane	Weight	Accuracy	length
LBP-TOP$_{8;8;8;1;1;1}$	0.969	0.972	0.966	4;3;1	0.975	0.932
LBP-MOP$_{8;8;8;1;1;1}$	0.974	0.969	0.965	4;2;3	0.977	0.933
LBP-SIP$_{8,8,8,1,1,1}$	0.973	0.976	0.971	3:2:5	0.976	0.912
LBP-TOP$_{4;4;4;1;1;1}$	0.976	0.977	0.966	6:2:3	0.978	0.9310
LBP-TOP$_{2,2,2,1,1,1}$	0.978	0.981	0.972	3:2:1	0.983	0.885
LBP-TOP$_{8;8;8;3;3;3}$	0.976	0.984	0.976	4:2:1	0.982	0.897
LGBP-TOP$_{8,8,8,1,1,1}$	0.973	0.976	0.969	2:4:2	0.979	0.930
LGBP-MOP$_{8;8;8;1;1;1}$	0.977	0.976	0.970	3:4:1	0.982	0.915
LGBP-SIP$_{8,8,8,1,1,1}$	0.979	0.979	0.976	2:3:5	0.979	0.930
LGBP-TOP$_{4,4,4,1,1,1}$	0.979	0.978	0.869	3:6:2	0.983	0.932
LGBP-TOP$_{2;2;2;1;1;1}$	0.981	0.988	0.977	2:3:1	0.984	0.933
LGBP-TOP$_{8,8,8,3,3,3}$	0.993	0.994	0.984	3:6:1	0.989	0.934

Table. 1. Video Sequence Classification on CK+ Dataset with 593 video image sequences

For the CK+ dataset the combined LGBP-TOP with Gabor Filtering and an ensemble of voting classifier combination of support vector machines, k-nearest neighbor and random forest achieved a higher accuracy of 98.9 percent from a sequence of 593 video sequences. For the FEED database with 400 video image sequences the corresponding accuracy was 99.5 percent.



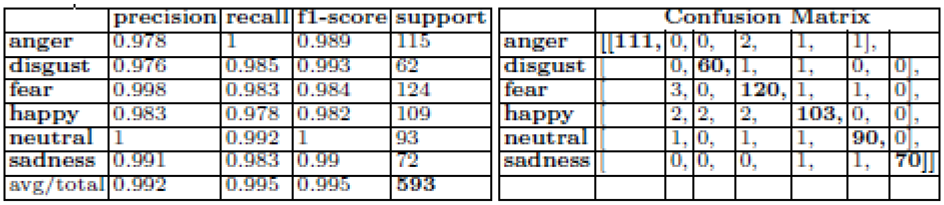
	XY Plane	XT Plane	YT Plane	Weight	Accuracy	length
LBP-TOP$_{8,8,8,1,1,1}$	0.973	0.962	0.969	4;2;4	0.977	0.90
LBP-MOP$_{8;8;8;1;1;1}$	0.967	0.974	0.979	4;3;3	0.975	0.90
LBP-SIP$_{8,8,8,1,1,1}$	0.963	0.973	0.976	5;4;1	0.979	0.90
LBP-TOP$_{4;4;4;1;1;1}$	0.975	0.979	0.982	4;2;4	0.985	0.78
LBP-TOP$_{2;2;2;1;1;1}$	0.978	0.982	0.985	3;5;2	0.989	0.89
LBP-TOP$_{8,8,8,3,3,3}$	0.981	0.983	0.986	4;4;1	0.991	0.90
LGBP-TOP$_{8;8;8;1;1;1}$	0.977	0.966	0.971	2;5;3	0.983	0.90
LGBP-MOP$_{8,8,8,1,1,1}$	0.972	0.976	0.983	5;1;4	0.984	0.90
LGBP-SIP$_{8;8;8;1;1;1}$	0.968	0.975	0.979	6;2;2	0.982	0.90
LGBP-TOP$_{4,4,4,1,1,1}$	0.979	0.985	0.983	3;5;2	0.989	0.90
LGBP-TOP$_{2;2;2;1;1;1}$	0.981	0.986	0.986	6;1;3	0.993	0.90
LGBP-TOP$_{8,8,8,3,3,3}$	0.986	0.987	0.991	4;3;3	0.995	0.90

Table. 2. Video Sequence Classification on Facial Expressions and Emotions Database(FEED) Dataset

The combined feature extractor LBP-TOP achieved higher classification rates as compared to the specific dimension LBP-XT, LBP-XT and LBP-YT accuracy rates. Better variation was experienced for the LBP-XT based plane. The second experiments evaluated the efficiency of using Gabor Filters to enable multi-orientation fusion to the spatial temporal advantages of the LBP-TOP algorithm. Support vector machines, k– nearest neighbor and random forest ensemble classifier was also used in this scenario The combined classifier with Gabor-Filters and LBP-TOP feature extractor showed greater accuracy to the normal LBP-TOP algorithm. The other LBP-TOP variants like SIP and MOP also achieved greated accuracy but the LGBP-TOP with parameters of 8,3 on each dimension achieved better accuracy to all the LGBP-TOP variants.

5.2. Video Sequence Confusion Matrices

The confusion matrix obtained from the video datasets for showed an overall success of 99.51 percent and 99.1% when Gabor Filtered on the CK+ and FEED database respectively. The following two confusion matrices give detail of the precision recall accuracy for the CK+ dataset which included 593 video datasets with video lengths of less than 1 second.

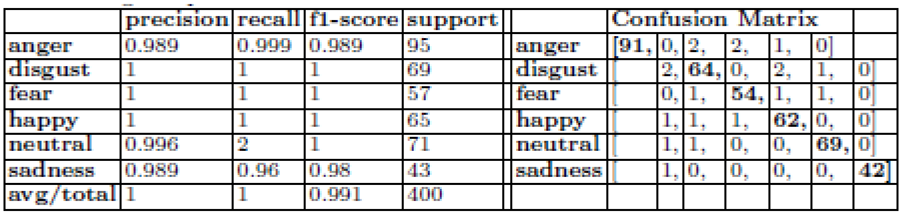


	precision	recall	f1-score	support
anger	0.978	1	0.989	115
disgust	0.976	0.985	0.993	62
fear	0.998	0.983	0.984	124
happy	0.983	0.978	0.982	109
neutral	1	0.992	1	93
sadness	0.991	0.983	0.99	72
avg/total	0.992	0.995	0.995	593

	Confusion Matrix						
anger	[[111,	0,	0,	2,	1,	1],	
disgust	[	0,	60,	1,	1,	0,	0],
fear	[	3,	0,	120,	1,	1,	0],
happy	[	2,	2,	2,	103,	0,	0],
neutral	[	1,	0,	1,	1,	90,	0],
sadness	[	0,	0,	0,	1,	1,	70]]

Fig. 5. LBP-TOP , CK+ Dataset Facial Expression Recognition dataset from 593 video sequences

The FEED Dataset had 400 video sequence images analysed over the 5 expression types namely anger, disgust, fear, happy, sadness and neutral. For the FEED dataset, the anger expression type showed modal frequency in the confusion matrix and for the CK+ video datasets , the fear expression type was highest.



	precision	recall	f1-score	support
anger	0.989	0.999	0.989	95
disgust	1	1	1	69
fear	1	1	1	57
happy	1	1	1	65
neutral	0.996	2	1	71
sadness	0.989	0.96	0.98	43
avg/total	1	1	0.991	400

	Confusion Matrix						
anger	[91,	0,	2,	2,	1,	0]	
disgust	[	2,	64,	0,	2,	1,	0]
fear	[	0,	1,	54,	1,	1,	0]
happy	[	1,	1,	1,	62,	0,	0]
neutral	[	1,	1,	0,	0,	69,	0]
sadness	[	1,	0,	0,	0,	0,	42]

Fig. 6. LBP-TOP , FEED Dataset Facial Expression Recognition dataset of 400 webcam videos image sequences

6. Conclusion

The feature extraction methods of LBP-TOP variants applied to major facial components used by the research to analyze facial expressions in video datasets showed marked improved method compared to traditional methods used before. For each facial component angle namely XY, XT and YT-3D dimension, a different variant of the classification algorithm was used. The classification rate was a weighted ensemble classifier composed of a support vector machine, k-nearest neighbor classifier and a random forest classifier. The contribution of each algorithm to the ensemble classifier had k-nearest neighbor as the majority contribution in the XY axis. For YT domain, the random forest dominated the ensemble classification algorithm. The Gabor filters improved the accuracy and the LBP-TOP variants also showed great accuracy.

7. Future Work

Future work in video facial expression recognition and classification include investigating applicability of analyzing video media like video conferencing, video streamed data, skype and other forms of media. The research also recommends analyzing the expressions of people in a group conversation and if their expressions are correlated based on the conversation at hand. The research also recommends analyzing expressions in an African context where there are different cultures with each culture having different ways of expressing themselves. Some of the key cultures suggested include the Zulu culture in South Africa, Swahili culture in Eastern Kenya and Tanzania, as well as Shona culture in Zimbabwe.

REFERENCES

[1] Y.Wang, J.See, R.C.-W. Phan, Y.-H.Oh, Lbp with six intersection points: Reducing redundant information in lbp-top for micro-expression recognition, in: Computer Vision— ACCV 2014, Springer, Singapore, 2014, pp. 525–537.

[2] Y. Wang, J. See, R.C.-W. Phan, Y.-H. Oh, Efficient spatio-temporal local binary patterns for spontaneous facial micro-expression recognition, PloS One 10 (5) (2015).

[3] M. S. Aung, S. Kaltwang, B. Romera-Paredes, B. Martinez, A. Singh, M. Cella, M. Valstar, H. Meng, A. Kemp, M. Shafizadeh, et al.: "The auto- matic detection of chronic pain-related expression: requirements, challenges and a multimodal dataset," Transactions on A↵ective Computing, 2015.

[4] P. Pavithra and A. B. Ganesh: "Detection of human facial behavioral ex- pression using image processing,"

[5 K. Nurzynska and B. Smolka, "Smiling and neutral facial display recognition with the local binary patterns operator:" Journal of Medical Imaging and Health Informatics, vol. 5, no. 6, pp. 1374–1382, 2015-11-01T00:00:00.

[6] Rupali S Chavan et al, International Journal of Computer Science and Mobile Computing Vol.2 Issue. 6, June- 2013, pg. 233-238

[7] P. Lemaire, B. Ben Amor, M. Ardabilian, L. Chen, and M. Daoudi, "Fully automatic 3d facial expression recognition using a region-based approach," in Proceedings of the 2011 Joint ACM Workshop on Human Gesture and Behavior Understanding, J-HGBU '11, (New York, NY, USA), pp. 53–58, ACM, 2011.

[8] C. Padgett and G. W. Cottrell, "Representing face images for emotion classification," Advances in neural information processing systems, pp. 894–900, 1997.

[9] P. Viola and M. J. Jones: "Robust real-time face detection," Int. J. Comput. Vision, vol. 57, pp. 137–154, May 2004.

[10] Yandan Wang , John See, Raphael C.-W. Phan, Yee-Hui Oh, Spatio-Temporal Local Binary Patterns for Spontaneous Facial Micro-Expression Recognition, May 19, 2015, https://doi.org/10.1371/journal.pone.0124674

[11] A. Sanin, C. Sanderson, M. T. Harandi, and B. C. Lovell, "Spatio-temporal covariance descriptors for action and gesture recognition," in Proc. IEEE Workshop on Applications of Computer Vision (Clearwater, 2013), pp. 103–110.

[12] K. Chengeta and S. Viriri, "A survey on facial recognition based on local directional and local binary patterns," 2018 Conference on Information Communications Technology and Society (ICTAS), Durban, 2018, pp. 1-6.

[13] S. Jain, C. Hu, and J. K. Aggarwal, "Facial expression recognition with temporal modeling of shapes," in Proc. IEEE Int. Computer Vision Workshops (ICCV Workshops) (Barcelona, 2011), pp. 1642–1649.

[14] X. Huang, G. Zhao, M. Pietikainen, and W. Zheng, "Dynamic facial expression recognition using boosted component-based spatiotemporal features and multiclassifier fusion," in Advanced Concepts for Intelligent Vision Systems (Springer, 2010), pp. 312–322.

[15] R. Mattivi and L. Shao, “Human action recognition using LBP-TOP as sparse spatio-temporal feature descriptor,” in Computer Analysis of Images and Patterns (Springer, 2009), pp. 740–747.

[16] A. S. Spizhevoy, Robust dynamic facial expressions recognition using Lbp-Top descriptors and Bag-of-Words classification model

[17] B. Jiang, M. Valstar, B. Martinez, M. Pantic, ”A dynamic appearance descriptor approach to facial actions temporal modelling”, IEEE Transaction on Cybernetics, vol. 44, no. 2, pp. 161-174, 2014.

[18] Y. Wang, Hui Yu, B. Stevens and Honghai Liu, ”Dynamic facial expression recognition using local patch and LBP-TOP,” 2015 8th International Conference on Human System Interaction (HSI), Warsaw, 2015, pp. 362-367. doi: 10.1109/HSI.2015.7170694

[19] Aggarwal, Charu C., Data Mining Concepts, ISBN 978-3-319-14141-1, 2015, XXIX, 734 p. 180 illus., 173 illus. in color.

[20] Ravi Kumar Y B and C. N. Ravi Kumar, ”Local binary pattern: An improved LBP to extract nonuniform LBP patterns with Gabor filter to increase the rate of face similarity,” 2016 Second International Conference on Cognitive Computing and Information Processing (CCIP), Mysore, 2016, pp. 1-5.

INTENTIONAL BLANK

NEAR-DROWNING EARLY PREDICTION TECHNIQUE USING NOVEL EQUATIONS (NEPTUNE) FOR SWIMMING POOLS

B David Prakash

IAG Firemark, Singapore

ABSTRACT

Safety is a critical aspect in all swimming pools. This paper describes a near-drowning early prediction technique using novel equations (NEPTUNE). NEPTUNE uses equations or rules that would be able to detect near-drowning using at least 1 but not more than 5 seconds of video sequence with no false positives. The backbone of NEPTUNE encompasses a mix of statistical image processing to merge images for a video sequence followed by K-means clustering to extract segments in the merged image and finally a revisit to statistical image processing to derive variables for every segment. These variables would be used by the equations to identify near-drowning. NEPTUNE has the potential to be integrated into a swimming pool camera system that would send an alarm to the lifeguards for early response so that the likelihood of recovery is high.

KEYWORDS

Near-drowning Detection, Drowning Detection, Statistical Image Processing, K-means Clustering, Swimming Pools

1. INTRODUCTION

The World Health Organization (WHO) classifies drowning as the 3rd leading cause of unintentional injury worldwide [1]. Globally, the highest drowning rates are among children aged between 1 to 4 years, followed by children aged between 5 to 9 years [1]. In individual countries such as the United States and France, within a short time frame of about 4 months, the number of drowning deaths in swimming pools and spas ranged between 74 and 163 [2-3]. Studies have shown that lifeguards may not be trained well enough to handle a drowning situation [4]. Hence, having a drowning detection system in conjunction with lifeguards in swimming pools would aid to promote swimming pool safety.

The existing drowning detection technologies can be broadly categorized into vision based systems [5-10] and wearable sensor based systems [11-13]. Vision based technologies can be further sub-categorized into those using underwater cameras [5-6] and those employing above water cameras [7-10]. A limitation of the use of underwater cameras is that they might miss the initial struggle that might take place above the water. Some drawbacks of the existing above water camera vision based technologies are that they have been demonstrated only using simulated video [7-10], they are trained to detect above water motionlessness [10] instead of the

Dhinaharan Nagamalai et al. (Eds) : CSEIT, NCS, SPM, NeTCoM - 2018
pp. 151–169, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81812

struggling motion which might pre-occur or might require additional costly fixtures such as a microarray to be mounted above the water to cover the entire swimming pool [7]. The shortcoming of a wearable based system is primarily the discomfort of use [8] which has an unproven possible notion that it might lead to younger children attempting to eliminate the discomfort by removing the device.

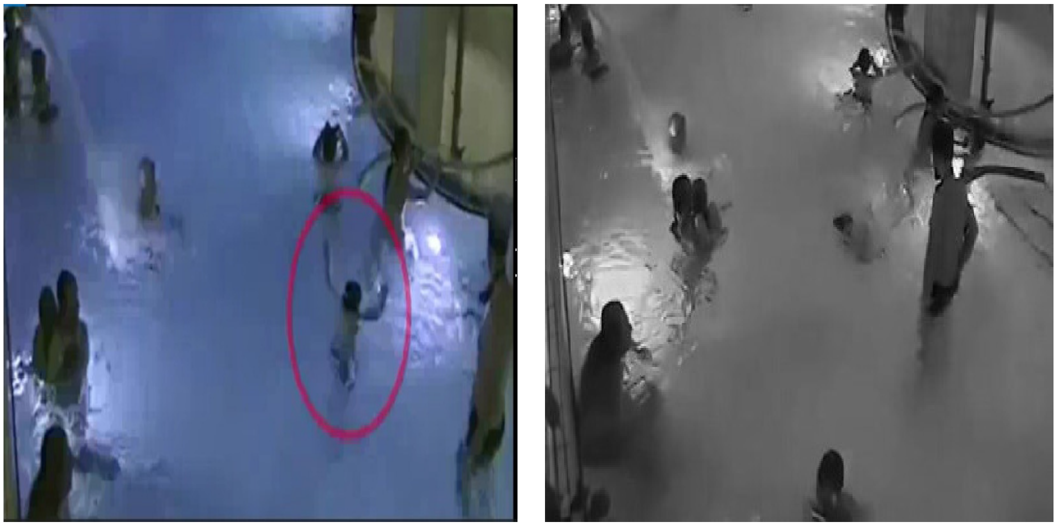
NEPTUNE is aimed at targeting the integration into existing above water camera(s) to enable a cost-effective installation by utilizing images from an existing camera fixture. It can identify pre-drowning struggling motions early using at least 1 but not more than 5 seconds of video sequence. The detection equations that NEPTUNE uses were derived from video sequences using an actual video footage [14-15] *.

*Please be informed that Fig. 1. contains confronting and real still images of a pre-drowning struggling victim.

2. NEPTUNE

2.1. Dataset

Two sets of videos were downloaded [14-15]. The first came with a manual red contour segmentation of the drowning victim throughout the entire video [14] and the second had the red contour segmentation of the drowning victim only in the initial portion of the video prior to the start of the pre-drowning struggle [15]. The second video [15] was used in the processing while the first [14] was applied as a confirmatory guide to locate the drowning victim in the second. Both videos were sequenced at 25 frames per second. Grey scale images were extracted from the second video [15] starting from the point of initial struggle and cropping was performed to output each image to a 447 by 281 dimension to maintain consistency with the camera coverage to the initial video. Fig. 1. shows a sample image extracted from [14] and another sample image extracted from [15] followed by grey scaling and cropping.



(a) (b)

Fig. 1. (a) Sample image extracted from [14] (b) Sample image extracted from [15] which had been grey scaled and cropped to follow similar camera coverage of the video from [14]

2.2. Pre-processing Pipeline

NEPTUNE's pre-processing pipeline consists of a combination of statistical image processing and K-means clustering [16].

The steps to process the images for every m seconds of video sequence are summarized below. The steps were repeated for five different values for m which are 1, 2, 3, 4 and 5.

1. Grey scaling (cropping was performed for the dataset used in this paper but would not be required in an actual setting)

2. Assuming 5 seconds of video sequences were being processed, for every pixel, the maximum absolute of the Fast Fourier Transform [17] across the 125 images was computed to give a two-dimensional matrix of 447 by 281. Since the video was sequenced at 25 frames per second, every 5 seconds would have a total 125 images that can be extracted. Similarly, every 4, 3, 2, and 1 seconds of video sequences would be using 100, 75, 50 and 25 images respectively.

3. The values across the two-dimensional matrix were normalized to a range between 0 and 1 to produce another two-dimensional matrix, N.

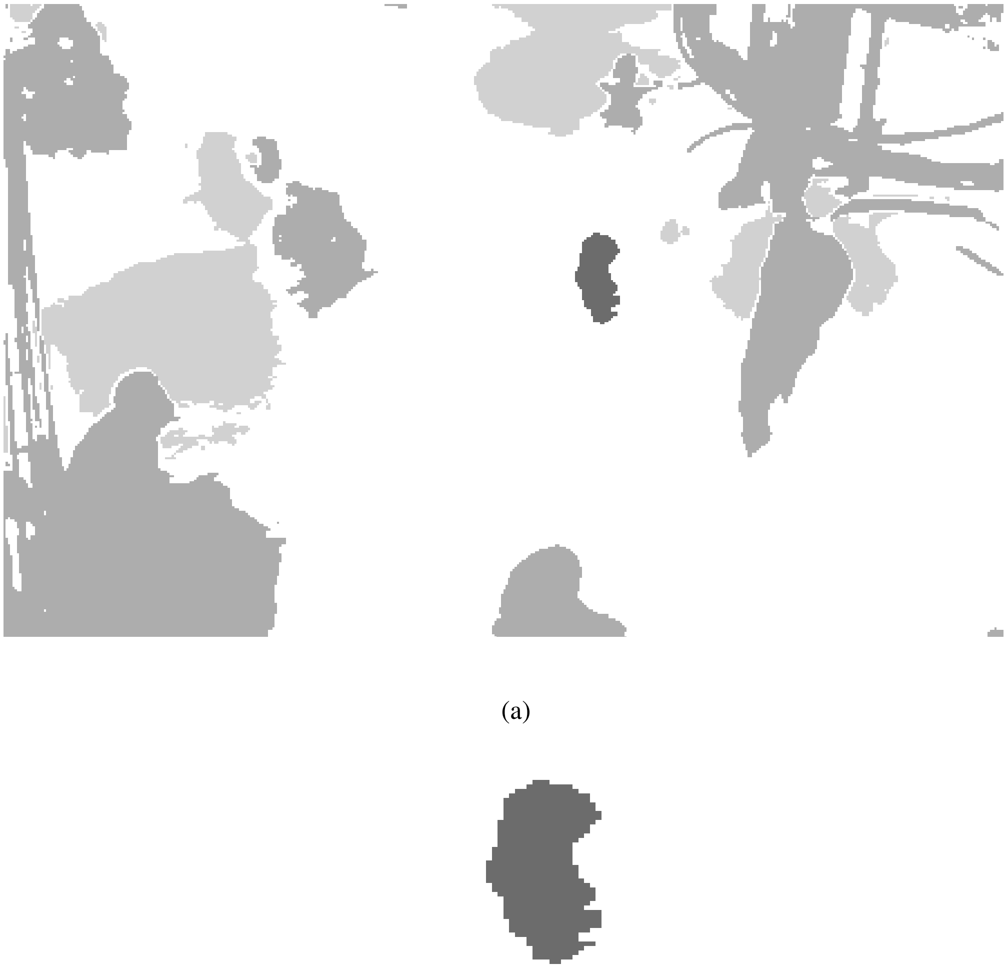
4. N would be transformed to a 1-dimensional array, 1-N via repeated looping across the x-dimension shadowed by an inner loop across the y-dimension. For instance, the values at position (1,1), (1,2) … (1,447) of N would be placed at (1), (2) … (447) of 1-N respectively while the values at position (2,1), (2,2) … (2,447) of N would be placed at (448), (449) … (894) respectively.

5. 3-means and 4-means clustering were performed independently on 1-N. An earlier attempt of using 2-means and 3-means clustering resulted in the inability in finding segments either intersecting or close by the struggling victim for some positive video sequences. More segments were created using a 3-means and 4-means clustering and hence increased the probability of finding a segment that either intersects or is very close by the struggling victim for every positive video sequence. The purpose of having two types of clustering was to find pairs of nearest segments, one from {Sa} and another from {Sb} to have a larger pool of variables to explore.

    a. From the 3-means clustering, the largest of the 3 clusters was excluded using an assumption that it predominantly consisted of water. The 2 smaller clusters were remapped from 1-N to N and a set of connected segments {Sa} was extracted. A connected segment is a set of pixels belonging to the same cluster and each pixel within that segment had to be beside any one of the pixels in that segment.

    b. From the 4-means clustering, the largest of the 4 clusters was excluded using an assumption that it predominantly consisted of water. The 3 smaller clusters were remapped from 1-N to N and a second set of connected segments {Sb} was extracted.

Fig. 2. shows an example of how 3-means clusters would look after remapping 1-N back to N. In comparison to Fig. 1., the cluster with the majority of pixels belonged to water for Fig. 2a. Fig. 2b. illustrates an example of a connected segment.



(a)

(b)

Fig. 2. (a) 3 clusters created from 3-mean clustering. Water is predominantly within the largest cluster which is shaded in white. The two shades of grey represent the remaining two clusters. The connected segment coloured in black intersects with the struggling victim and belongs to the cluster with the darker shade of grey. (b) A zoomed in image of the single connected segment coloured in black.

6. For each segment in {Sa}, variables shown in Table 1 were derived. Variable V1 was reserved for the labelling of presence/absence of a pre-drowning struggling victim within/close by a segment. If there was no segment that intersects the struggling victim, the nearest segment would be considered to contain the pre-drowning struggling victim.

Table 1. Variables derived for each segment in {Sa}

Variable Name	Variable Description
V2	Ratio of V4 to V3
V3	Number of pixels in the segment
V4	Standard deviation of values from 5 points (4 extreme points* and the segment's centre)
V5	Ratio of V2 to the sum of V2 across all segments
V6	Ratio of V3 to the sum of V3 across all segments
V7	Ratio of V4 to the sum of V4 across all segments

*4 extreme points are {minimum(x), minimum(y)}, {minimum(x), max(y)}, {maximum(x), minimum(y)} and {maximum(x), maximum(y)} where x and y are the x-coordinates and y-coordinates of a segment respectively

7. For each segment in {Sa}, similar variables for the respective nearest segment from {Sb} was computed as shown in Table 2.

Table 2. Variables derived from respective nearest segment in {Sb}

Variable Name	Variable Description
V8	Ratio of V10 to V9
V9	Number of pixels in the segment
V10	Standard deviation of values of 5 points (4 extreme points* and the segment's centre)
V11	Ratio of V11 to the sum of V11 across all segments
V12	Ratio of V12 to the sum of V12 across all segments
V13	Ratio of V13 to the sum of V13 across all segments

*4 extreme points are {minimum(x), minimum(y)}, {minimum(x), maximum(y)}, {maximum(x), minimum(y)} and {maximum(x), maximum(y)} where x and y are the x-coordinates and y-coordinates of a segment respectively

8. Next, for each segment in {Sa}, new variables were created as shown in Table 3. These new variables were computed using the variables derived from Table 1 and Table 2.

Table 3. Variables derived from respective nearest segment in {Sb}

Variable Name	Variable Description
V2_8	Ratio of V2 to V8
V3_9	Ratio of V3 to V9
V4_10	Ratio of V4 to V10
V5_11	Ratio of V5 to V11
V6_12	Ratio of V6 to V12
V7_13	Ratio of V7 to V13

9. Finally, the percentile cut-offs for every variable across all segments in {Sa} were computed as shown in Tables A1 (a), (b), (c) and (d) of the Appendix.

Every variable value for each segment would be assigned either a value of 1, 2, 3 or 4 according to the range which they fall into as indicated in Table 4 with respect to length of video sequence. For example, say for a segment in a 5s video sequence having a V2 value of 0.03, it would be transformed to a value of 2 since it is between the 25th and 50th percentiles of V2.

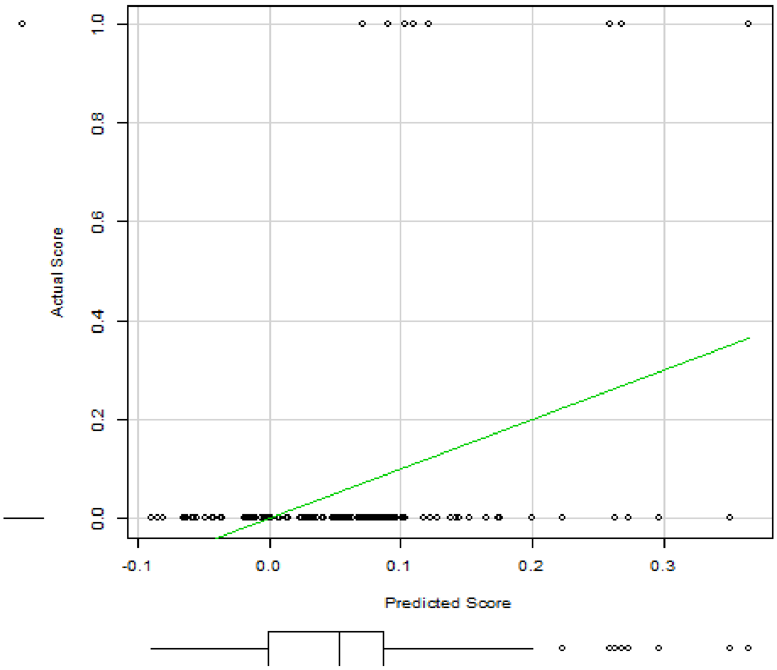
Table 4. Value assigned each variable in every segment in {Sa}

Value Assigned	Range
1	being less than or equal to the 25th percentile
2	being more than the 25th percentile but less than or equal to the 50th percentile
3	being more than the 50th percentile but less than or equal to the 75th percentile
4	being more than the 75th percentile

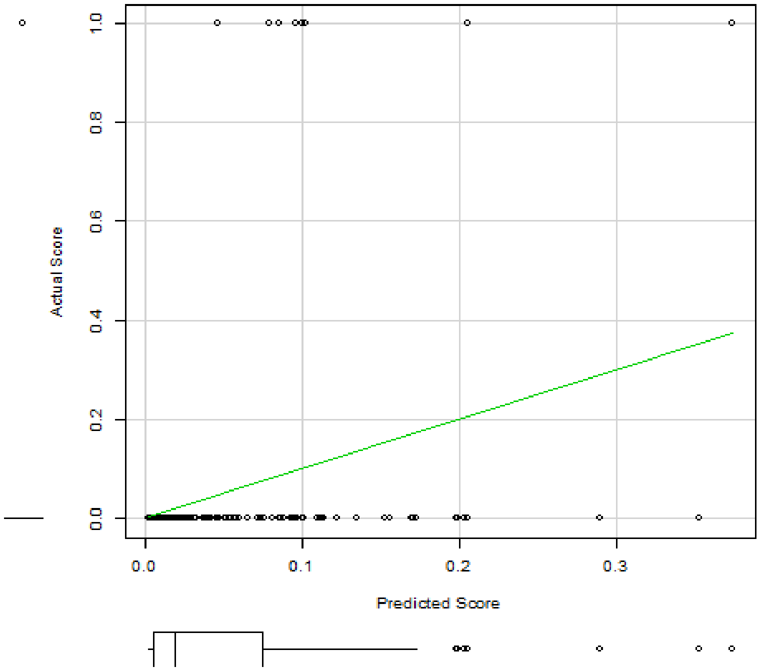
Solely for this training, labelling of V1 for every segment had to be performed. It would contain one of two values; either 1 if it was positive or 0 otherwise. A positive refers to the presence of a struggling pre-drowning victim within or close by the segment. This labelling would not be required for the actual application of NEPTUNE. The video sequence lengths of 1s, 2s, 3s, 4s and 5s respectively contained 36, 17, 12, 9, and 8 positive video sequences. A positive video sequence would each entail a struggling pre-drowning victim. Correspondingly, for the video sequence lengths of 1s, 2s, 3s, 4s and 5s, the respective number of video sequences for which there were no struggling were 946, 406, 269, 179 and 138. Each video sequence may have multiple segments with at most 1 positive segment.

2.3. Equations Derivation

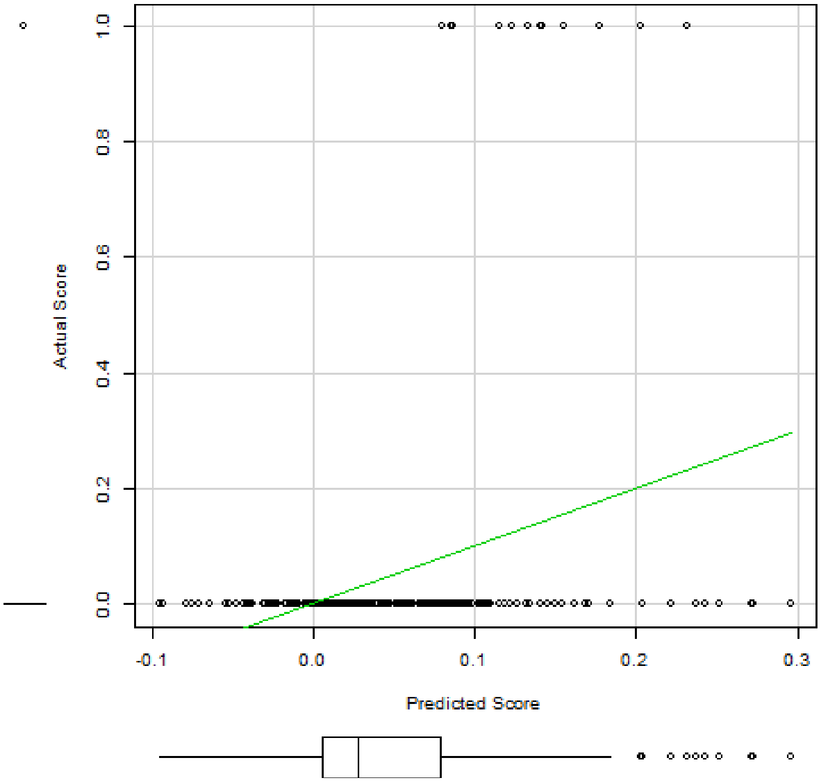
The equations were derived from optimized rules generated via association rules mining [18]. Association rules mining was attempted as an approach to detect the positives as anomalies. The existence of a non-linear relationship between the variables and the presence/absence of positives is shown in Fig. 3 where there is a poor correlation not exceeding 0.37 between the actual and predicted scores for all the video sequence lengths studied. This further justifies the use of association rules mining since it can identify both linear and non-linear properties that would distinguish positives from non-positives. The formulae of the regression model used in Fig. 3a, b, c, d and e are shown in Table A2 of the Appendix.



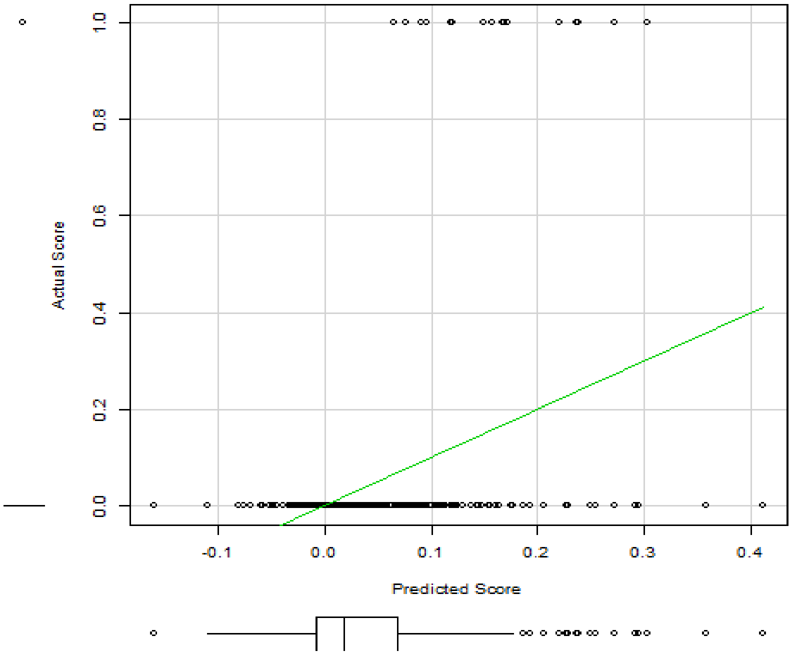
(a) Video Sequence Length of 5s



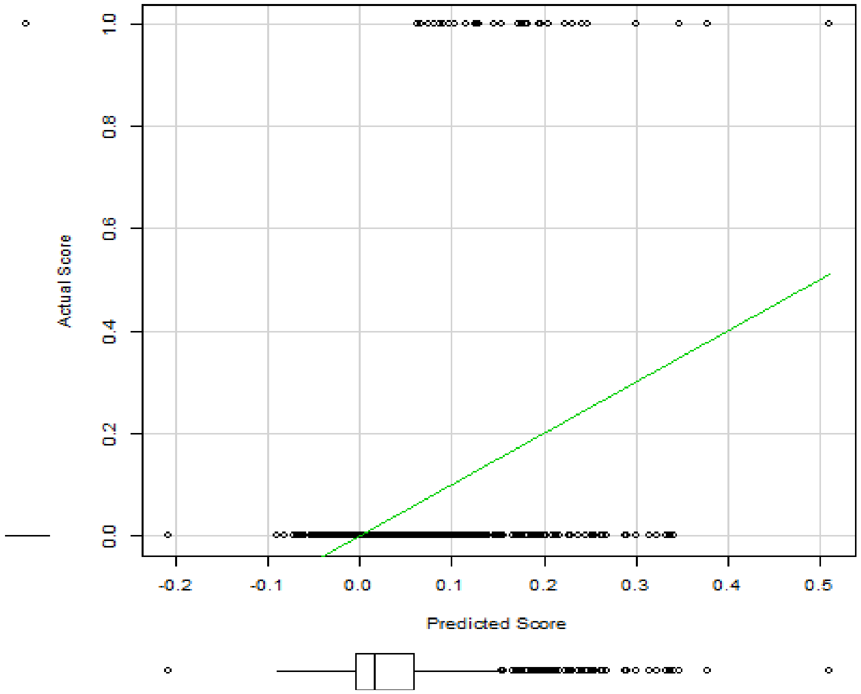
(b) Video Sequence Length of 4s



(c) Video Sequence Length of 3s



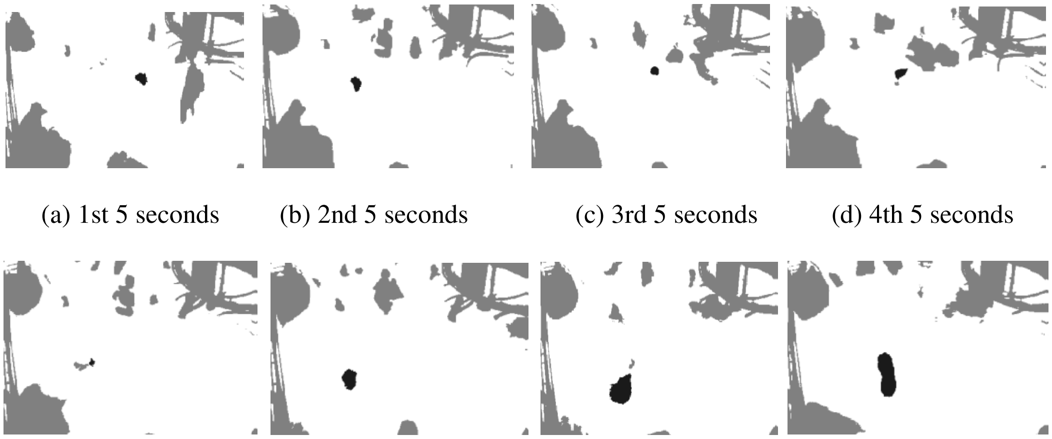
(d) Video Sequence Length of 2s



(e) Video Sequence Length of 1s

Fig. 3. The predicted scores created via a AIC stepwise linear regression model [19] built using the entire dataset against the actual scores for the various video sequence lengths. A score of 1 denotes a positive.

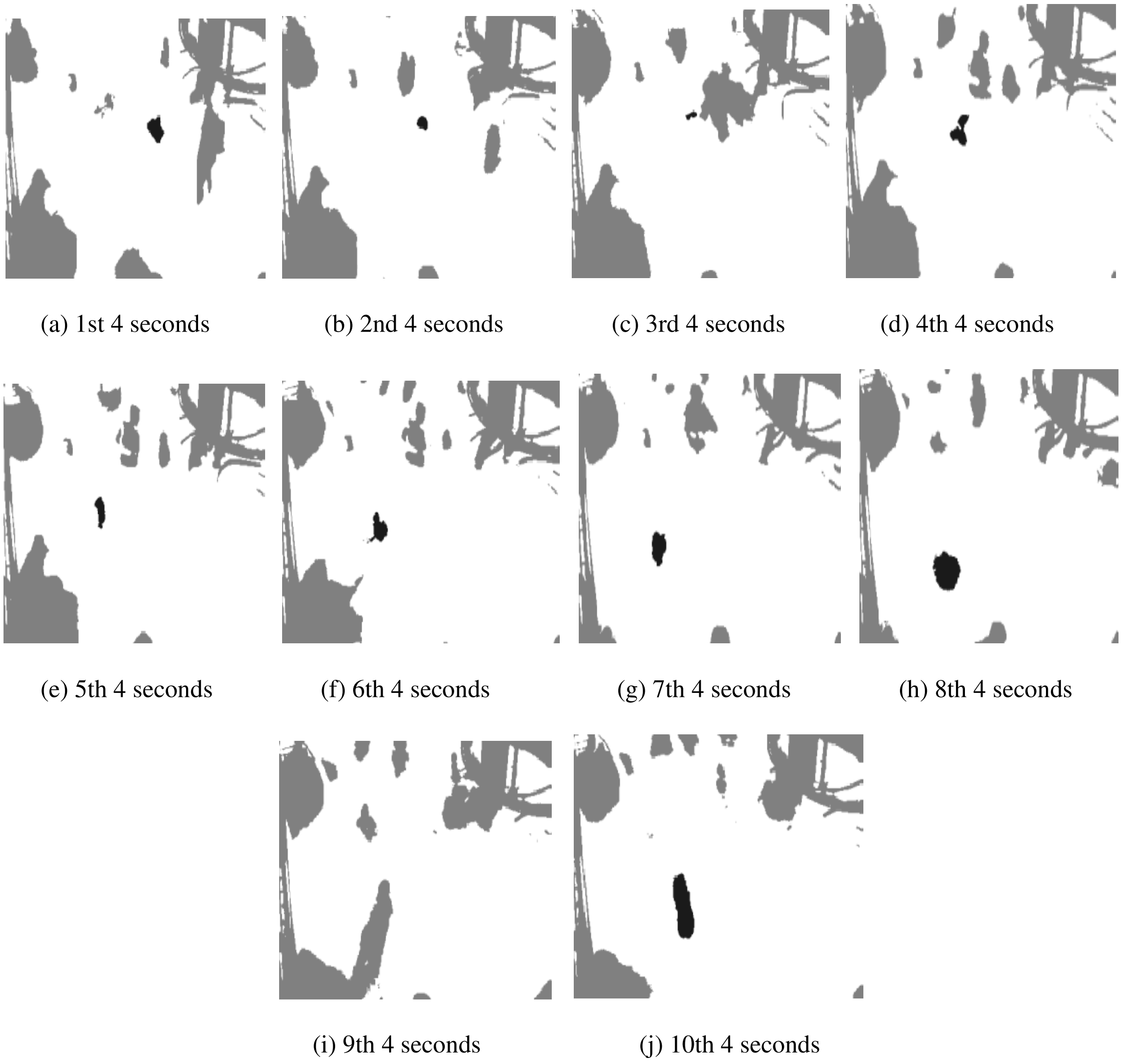
For video sequence lengths of 4s and 5s, the positive segments with the highest predicted score had the largest and most circular segment as shown in Fig. 4 and 5 which made these two positive segments more distinguishable than the other positive segments within the respective video sequence lengths.



(a) 1st 5 seconds (b) 2nd 5 seconds (c) 3rd 5 seconds (d) 4th 5 seconds

(e) 5th 5 seconds (f) 6th 5 seconds (g) 7th 5 seconds (h) 8th 5 seconds

Fig. 4. The positive segments shaded in black for the first 8 video sequences of length 5s where there was a struggling victim. The 7th 5 seconds video sequence had the highest prediction score using linear regression.



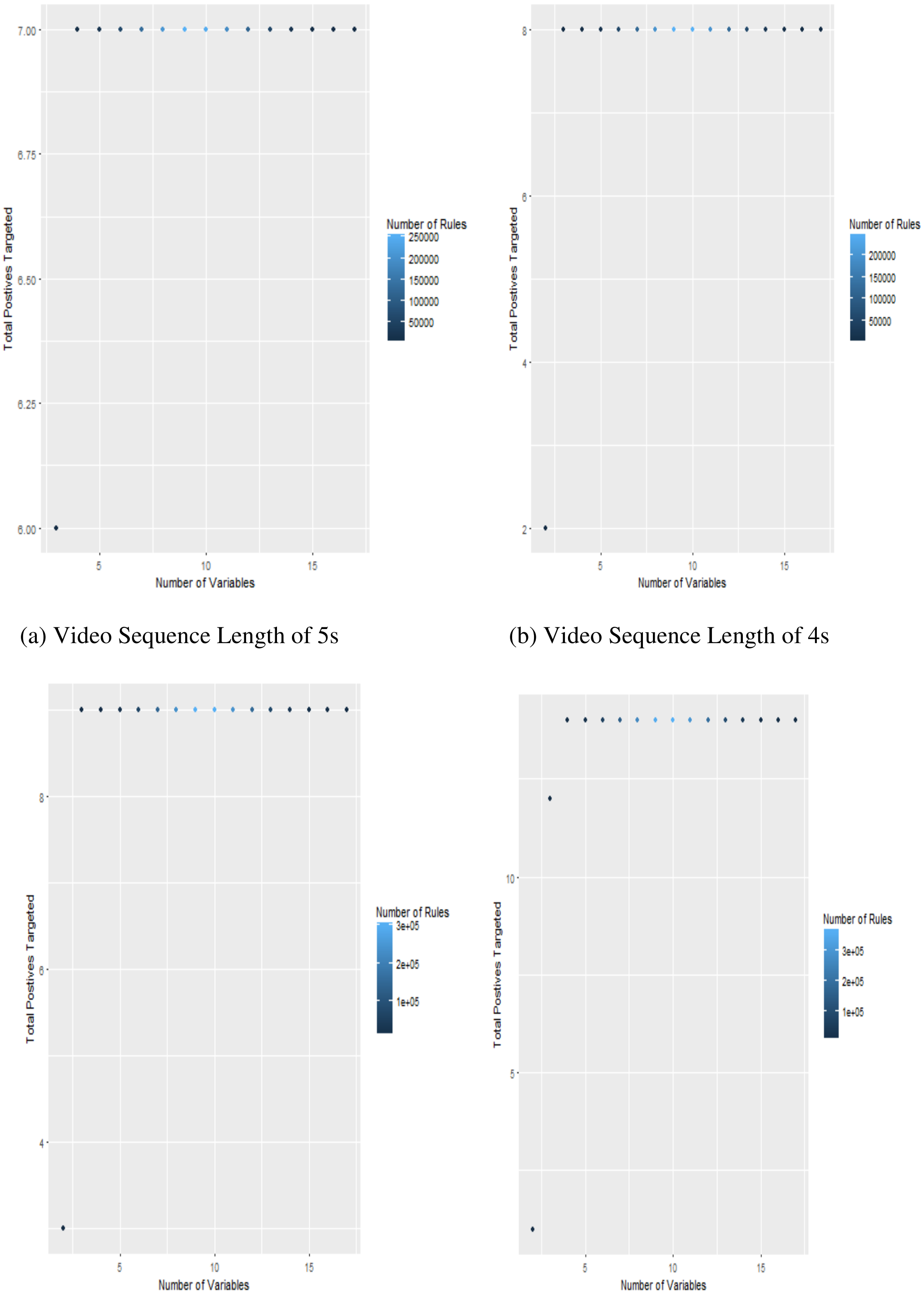
(a) 1st 4 seconds (b) 2nd 4 seconds (c) 3rd 4 seconds (d) 4th 4 seconds

(e) 5th 4 seconds (f) 6th 4 seconds (g) 7th 4 seconds (h) 8th 4 seconds

(i) 9th 4 seconds (j) 10th 4 seconds

Fig. 5. The positive segments shaded in black for the first 10 video sequences of length 4s where there was a struggling victim. The 8th 4 seconds video sequence had the highest prediction score using linear regression. No positive segment was detectable in 9th 4 seconds video sequence although there was a struggling.

Rules were generated independently for the various video sequence lengths to detect presence/absence of a positive segment using 19 variables of which 18 came from Tables 1, 2 and 3. One of the 19 variables, was the label for the absence/presence of a positive. All rules were generated for a confidence of 1 and targeted a minimum of 1 positive. We generated different rule sets across different number of variables ranging from 3 to the full 19. For every number of variables used for rule set generation, one had to be the label. For instance, if 3 variables were used, 2 would be derived variables and 1 would be the label. Fig. 6. shows that the number of number of positives identifiable for various number of variables used across the various video sequence lengths.

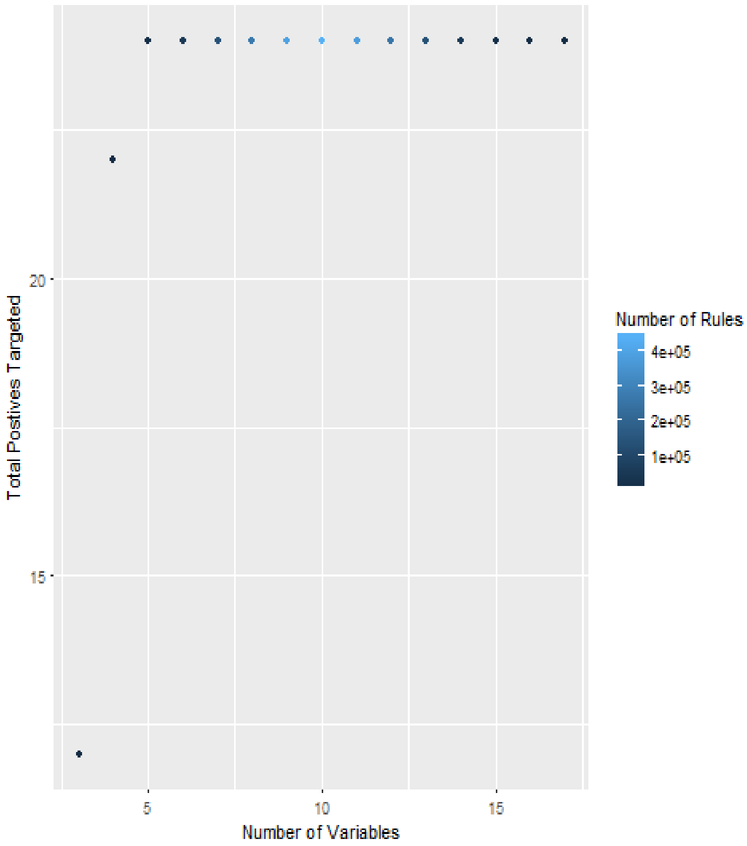


(a) Video Sequence Length of 5s

(b) Video Sequence Length of 4s

(c) Video Sequence Length of 3s

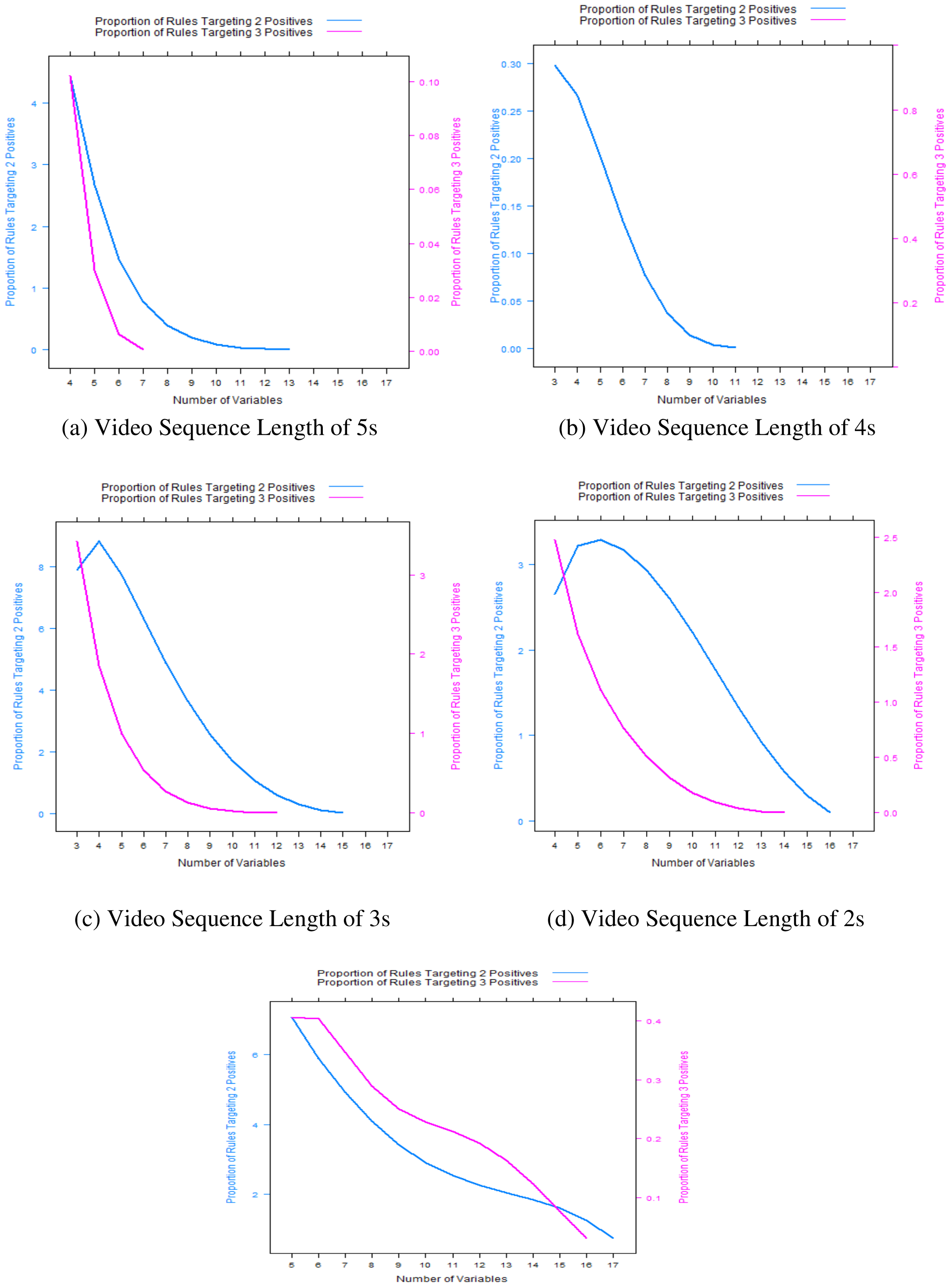
(d) Video Sequence Length of 2s



(e) Video Sequence Length of 1s

Fig. 6. Total positives targeted and number of rules generated with 100% confidence in detecting positives across the corresponding number of variables used in the rules generation. Each spot represents a rule set consisting of rules generated for the respective number of variables. Rule sets which targeted the maximum number of positives detectable for the respective video sequences lengths were enclosed within a red bounding box

The proportion of the rules generated using variables that detected the maximum number of positives either targeting 2 or 3 positives across the different video sequence lengths are shown in Fig. 7. Having a higher proportion of individual rules targeting more positives would ensure that the rule set is more generic and hence applicable across other datasets. Therefore, for the final rule set in each of the video sequence lengths studied, rules generated with the highest proportion of individual rules targeting the most number of positives would be chosen. It can be seen in Fig. 7. that the highest proportion rules targeting 2 or 3 positives tend to be generated when less variables were. Using less variables would reduce the specificity of the rules generated thereby allowing more generic rules to be produced. Each rule in final rule set would be henceforth referred to as an equation.



(a) Video Sequence Length of 5s

(b) Video Sequence Length of 4s

(c) Video Sequence Length of 3s

(d) Video Sequence Length of 2s

(e) Video Sequence Length of 1s

Fig. 7. Proportion of rules targeting 2 or 3 positives across the various number of variables used for rules generation

3. RESULTS

Fig. 8. shows the positive detections during the 40s of struggle. It should be noted there were time points when only one of the video sequence lengths detected the presence of a struggle. For instance, at the 39th second of struggle, only the video sequence length of 3s could detect the struggle. Hence, it is proposed to use all the video sequence lengths in parallel for pre-drowning struggling detection to maximum the detectable time points of struggle.

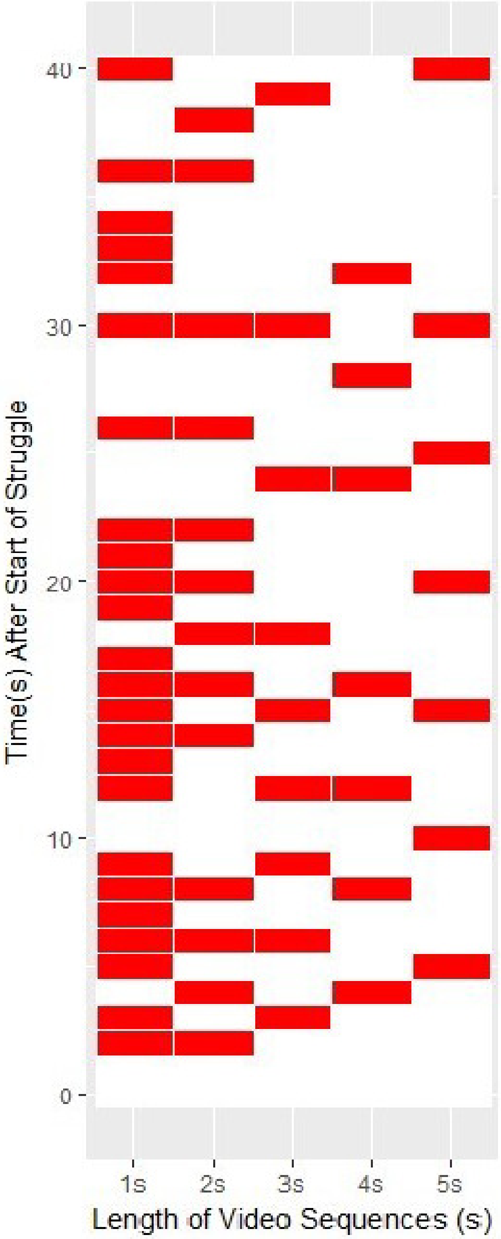


Fig. 8. Detection during the 40s of struggle for the various video sequence lengths. Positive detection only occurs at the time points where there is a red rectangle.

4. CONCLUSION

NEPTUNE was presented in this paper as a feasible technique for early detection of struggling pre-drowning victims. The reliance on solely camera based video sequences would allow an easy integration into existing infrastructure in swimming pools with camera(s). This is the first vision based technique built using real video sequences and the fastest requiring at least 1 but not more than 5 seconds of video footage for detection. With collaborative initiatives to collate more actual pre-drowning video footages, NEPTUNE can be refined and further developed into a real-time cost-effective vision based early pre-drowning detection system.

Acknowledgments

This work has been supported by IAG Firemarks Singapore. I like to thank everyone in the IAG Firemarks Singapore team for their continued encouragement especially Allison Howells for her initial and continued cheering of what started as a simple possibility to a prospective reality.

REFERENCES

[1] World Health Organization (WHO), Drowning Fact Sheet (2018), http://www.who.int/mediacentre/factsheets/fs347/en/

[2] United States Consumer Product Safety Commission, Fatal Child Pool and Spa Drownings (2017), https://www.cpsc.gov/Latest-Pool-Safely-Stats-At-Least-163-Children-Fatally-Drowned-in-Pools-and-Spas-This-Summer

[3] Lasbeur L, Szego-Zguem E, Guillam M, et al. “671 Epidemiological surveillance of drowning: a national survey in France, 1 June to 30 September 2015”. Injury Prevention 22 (2016): A241.

[4] Bierens, Joost, and Andrea Scapigliati. "Drowning in swimming pools." Microchemical journal 113 (2014): 53-58.

[5] Zhang, Chi, Xiaoguang Li, and Fei Lei. “A Novel Camera-Based Drowning Detection Algorithm.” Advances in Image and Graphics Technologies, Springer Berlin Heidelberg (2015): 224-233.

[6] Fei, Lei, Wang Xueli, and Chen Dongsheng. “Drowning Detection Based on Background Subtraction.” Proceedings of the Sixth IEEE International Conference on Embedded Software and Systems (ICESS 2009).

[7] How-Lung Eng, Kar-Ann Toh, Wei-Yun Yau, Junxian Wang. “DEWS: A Live Visual Surveillance System for Early Drowning Detection at Pool.” IEEE transactions on circuits and systems for video technology 18:2 (2008): 194-210.

[8] Wenmiao Lu,Yap-Peng Tan, Yap-Peng Tan. “A Vision-Based Approach to Early Detection of Drowning Incidents in Swimming Pools.” IEEE Transactions on Circuits and Systems for Video Technology 14:2 (2004):159 – 178.

[9] How-Lung Eng, Kar-Ann Toh, Alvin H. Kam, Junxian Wang and Wei-Yun Yau. “An automatic drowning detection surveillance system for challenging outdoor pool environments”. Proceedings of the Ninth IEEE International Conference on Computer Vision (ICCV 2003).

[10] Nasrin Salehi, Maryam Keyvanara, Seyed Amirhassan Monadjemmi. “An Automatic Video-based Drowning Detection System for Swimming Pools Using Active Contours.” I.J. Image, Graphics and Signal Processing 8:8 (2016): 1-8.

[11] S. Nagalikitha, A.V. Kiranmai. “Automatic Waist Airbag Drowning Prevention System Based on Motion Information Measured by Memos Accelerometer and pressure.” International Journal of Emerging Trends in Engineering Research (IJETER) 3:6 (2015): 204-206.

[12] Mohamed Kharrat, Yuki Wakuda, Shinsuke Kobayashi, Noboru Koshizuka, Ken Sakamura. “Near drowning detection system based on swimmer’s physiological information analysis.” Proceedings of the Third World Conference on Drowning Prevention (2011).

[13] McAdams, E., Krupaviciute, A., Gehin, C., Grenier, E., Massot, B., Dittmar, A., Rubel, P., Fayn, J.“Wearable sensor systems: The challenges.”, In Proceedings of the 33rd Annual International Conference of the IEEE Engineering in Medicine Biology Society (EBMC 2011): 3648–3651.

[14] Mirror, World News (2017). https://www.mirror.co.uk/news/world-news/horror-five-year-old-boy-10585736

[15] You Tube (2017). “A 5-year-old child drowns in a swimming pool without anyone noticing (Finland)”https://www.youtube.com/watch?v=zuZIfy4aBEY

[16] Hartigan, J. A. and Wong, M. A. “Algorithm AS 136: A K-means clustering algorithm.” Applied Statistics 28 (1979): 100–108

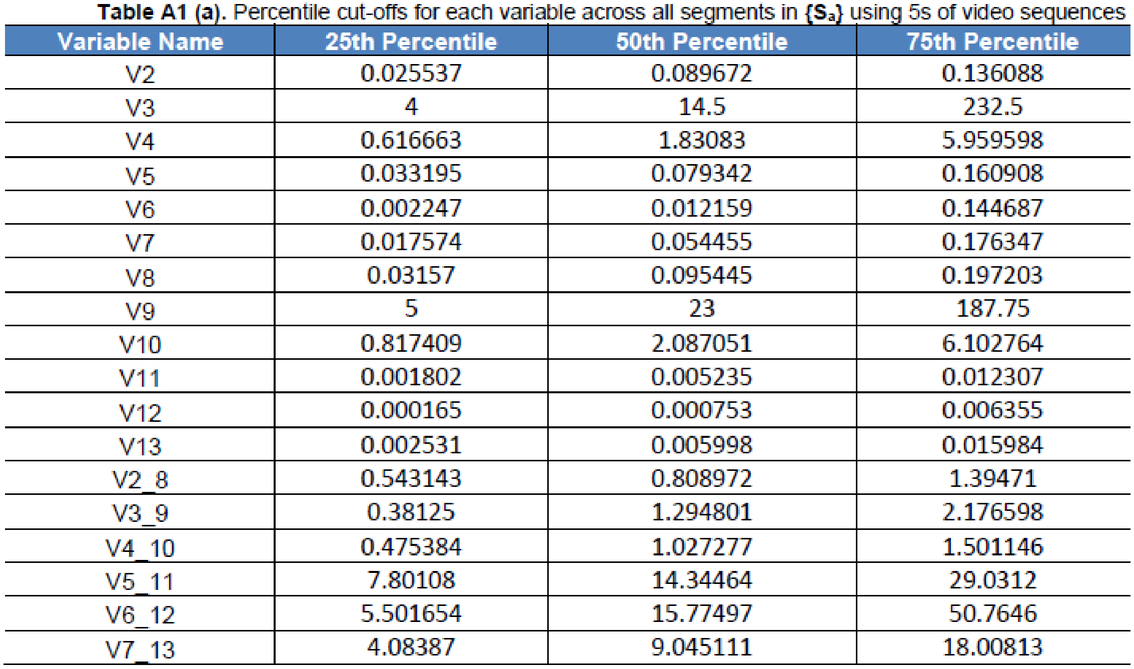
[17] Gentleman, W. M. and Sande, G. “Fast Fourier Transforms: For Fun and Profit”. In Proceedings of the November 7-10, 1966, Fall Joint Computer Conference (AFIPS '66 (Fall)): 563-578.

[18] Michael H., Bettina G. and Kurt H. "arules - A Computational Environment for Mining Association Rules and Frequent Item Sets."Journal of Statistical Software 14:15 (2005):1-25.

[19] Hastie, T. J. and Pregibon, D. "Generalized linear models. Chapter 6 of Statistical Models in S"(1992).

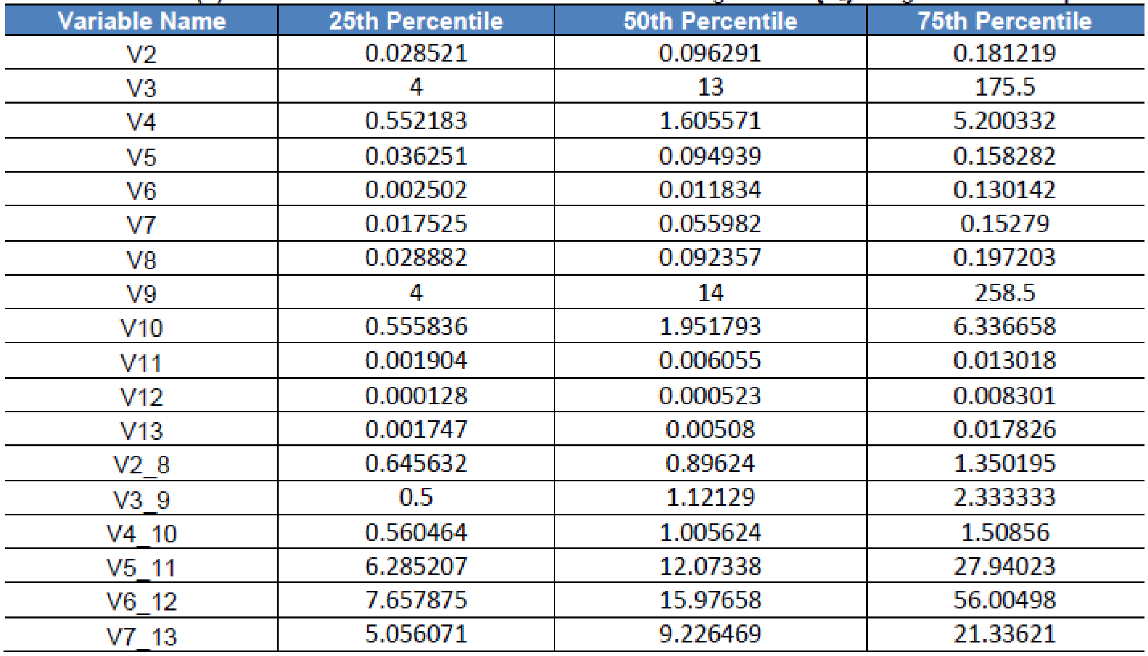
Appendix

Table A1 (a). Percentile cut-offs for each variable across all segments in **{S_a}** using 5s of video sequences



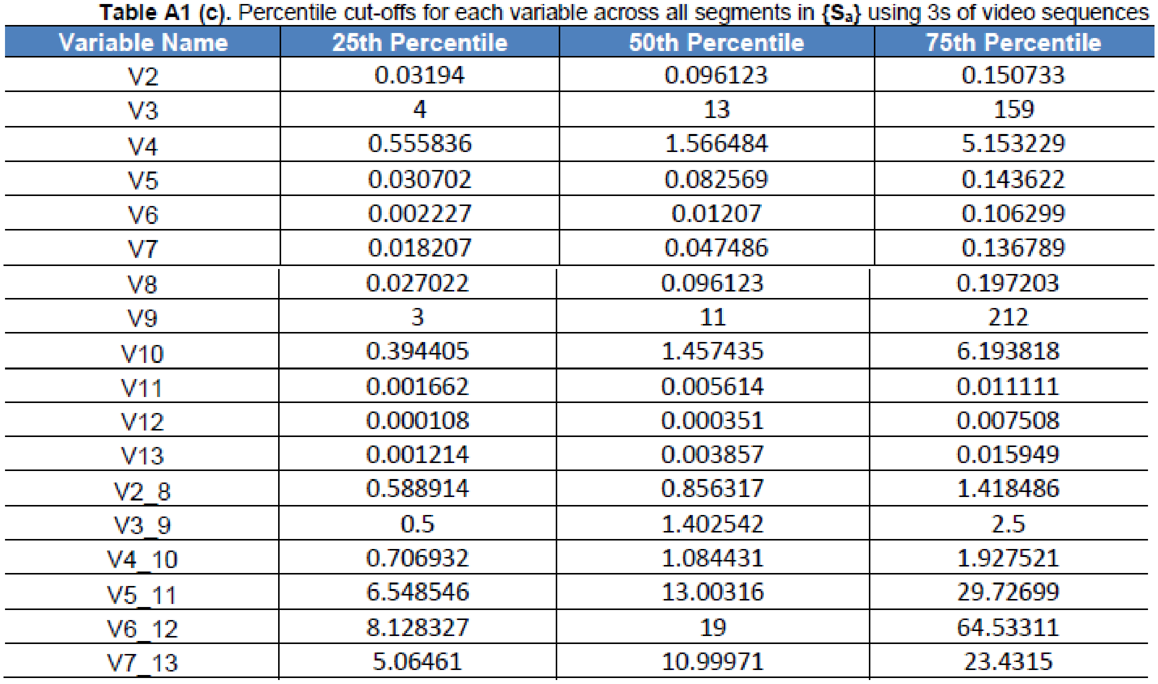
Variable Name	25th Percentile	50th Percentile	75th Percentile
V2	0.025537	0.089672	0.136088
V3	4	14.5	232.5
V4	0.616663	1.83083	5.959598
V5	0.033195	0.079342	0.160908
V6	0.002247	0.012159	0.144687
V7	0.017574	0.054455	0.176347
V8	0.03157	0.095445	0.197203
V9	5	23	187.75
V10	0.817409	2.087051	6.102764
V11	0.001802	0.005235	0.012307
V12	0.000165	0.000753	0.006355
V13	0.002531	0.005998	0.015984
V2_8	0.543143	0.808972	1.39471
V3_9	0.38125	1.294801	2.176598
V4_10	0.475384	1.027277	1.501146
V5_11	7.80108	14.34464	29.0312
V6_12	5.501654	15.77497	50.7646
V7_13	4.08387	9.045111	18.00813

Table A1 (b). Percentile cut-offs for each variable across all segments in **{S_a}** using 4s of video sequences



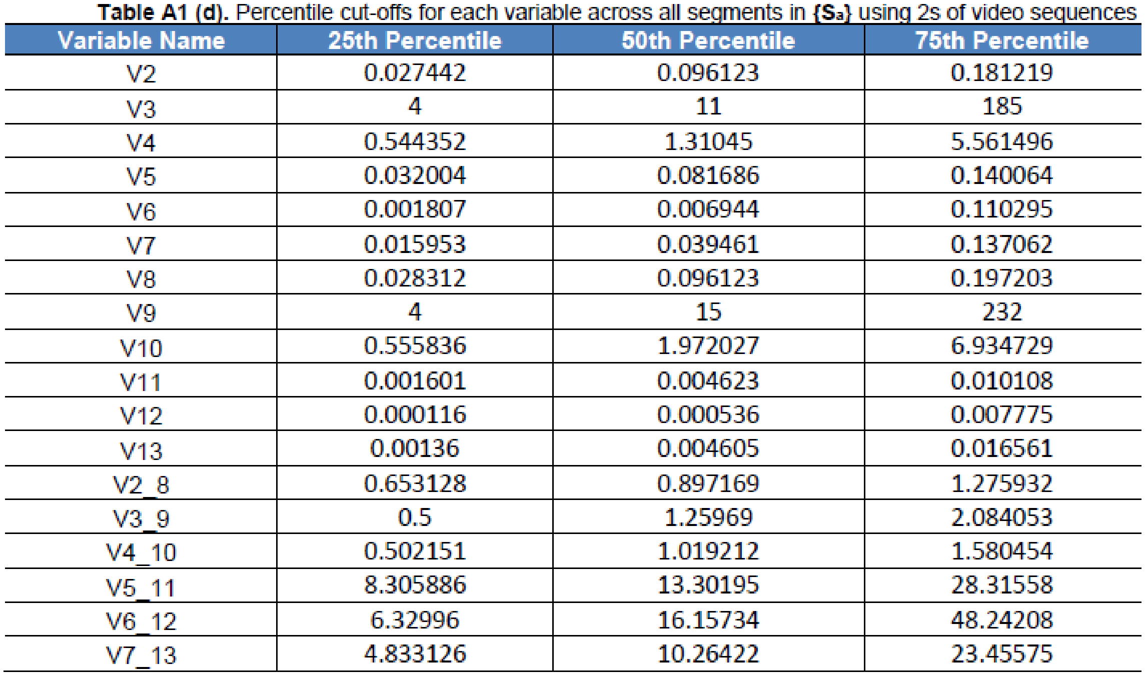
Variable Name	25th Percentile	50th Percentile	75th Percentile
V2	0.028521	0.096291	0.181219
V3	4	13	175.5
V4	0.552183	1.605571	5.200332
V5	0.036251	0.094939	0.158282
V6	0.002502	0.011834	0.130142
V7	0.017525	0.055982	0.15279
V8	0.028882	0.092357	0.197203
V9	4	14	258.5
V10	0.555836	1.951793	6.336658
V11	0.001904	0.006055	0.013018
V12	0.000128	0.000523	0.008301
V13	0.001747	0.00508	0.017826
V2_8	0.645632	0.89624	1.350195
V3_9	0.5	1.12129	2.333333
V4_10	0.560464	1.005624	1.50856
V5_11	6.285207	12.07338	27.94023
V6_12	7.657875	15.97658	56.00498
V7_13	5.056071	9.226469	21.33621

Table A1 (c). Percentile cut-offs for each variable across all segments in {S_a} using 3s of video sequences



Variable Name	25th Percentile	50th Percentile	75th Percentile
V2	0.03194	0.096123	0.150733
V3	4	13	159
V4	0.555836	1.566484	5.153229
V5	0.030702	0.082569	0.143622
V6	0.002227	0.01207	0.106299
V7	0.018207	0.047486	0.136789
V8	0.027022	0.096123	0.197203
V9	3	11	212
V10	0.394405	1.457435	6.193818
V11	0.001662	0.005614	0.011111
V12	0.000108	0.000351	0.007508
V13	0.001214	0.003857	0.015949
V2_8	0.588914	0.856317	1.418486
V3_9	0.5	1.402542	2.5
V4_10	0.706932	1.084431	1.927521
V5_11	6.548546	13.00316	29.72699
V6_12	8.128327	19	64.53311
V7_13	5.06461	10.99971	23.4315

Table A1 (d). Percentile cut-offs for each variable across all segments in {S_a} using 2s of video sequences



Variable Name	25th Percentile	50th Percentile	75th Percentile
V2	0.027442	0.096123	0.181219
V3	4	11	185
V4	0.544352	1.31045	5.561496
V5	0.032004	0.081686	0.140064
V6	0.001807	0.006944	0.110295
V7	0.015953	0.039461	0.137062
V8	0.028312	0.096123	0.197203
V9	4	15	232
V10	0.555836	1.972027	6.934729
V11	0.001601	0.004623	0.010108
V12	0.000116	0.000536	0.007775
V13	0.00136	0.004605	0.016561
V2_8	0.653128	0.897169	1.275932
V3_9	0.5	1.25969	2.084053
V4_10	0.502151	1.019212	1.580454
V5_11	8.305886	13.30195	28.31558
V6_12	6.32996	16.15734	48.24208
V7_13	4.833126	10.26422	23.45575

Table A1 (d). Percentile cut-offs for each variable across all segments in **{S$_a$}** using 1s of video sequences

Variable Name	25th Percentile	50th Percentile	75th Percentile
V2	0.043662	0.102924	0.197203
V3	3	8	109.75
V4	0.394405	1.099948	4.615003
V5	0.032882	0.074918	0.12968
V6	0.001575	0.006651	0.073862
V7	0.01319	0.034193	0.119747
V8	0.039327	0.111167	0.197203
V9	3	10	123
V10	0.547526	1.344413	5.361706
V11	0.001796	0.005085	0.008561
V12	0.000106	0.000323	0.004121
V13	0.001244	0.003122	0.012171
V2_8	0.043662	0.102924	0.197203
V3_9	3	8	109.75
V4_10	0.394405	1.099948	4.615003
V5_11	0.032882	0.074918	0.12968
V6_12	0.001575	0.006651	0.073862
V7_13	0.01319	0.034193	0.119747

Table A2. Regression formulae for the respective models in Fig 3.

Fig	Formula
3a	$V1 = -0.6882 * V2 + 0.8153 * V6 - 1.1143 * V7 - 0.0003874 * V9 + 13.0915 * V12 - 0.001769 * V6\_12 + 0.002818 * V7\_13 + 0.1227$
3b	$V1 = 0.01103 * V4 + 0.00107 * V15 - 0.00123$
3c	$V1 = -0.3232 * V2 + 0.0001431 * V3 - 0.1553 * V6 - 0.2502 * V8 - 0.09636$
3d	$V1 = 0.01665 * V4 - 0.1753 * V6 - 0.2300 * V8 + 0.0002441 * V9 - 7.6024 * V12 - 0.005745 * V4\_10 + 0.03580$
3e	$V1 = -0.2072 * V2 + 0.01528 * V4 - 0.1563 * V6 + 0.000243 * V9 - 0.01994 * V10 - 2.9549 * V11 - 7.4156 * V12 + 7.6710 * V13 - 0.004826 * V16 + 0.58134$

INTENTIONAL BLANK

A PREFERMENT PLATFORM FOR IMPLEMENTING SECURITY MECHANISM FOR AUTOMOTIVE CAN BUS

Mabrouka Gmiden[1], Mohamed Hedi Gmiden[2] and Hafedh Gmiden[2]

[1,2]Computer and Embedded System Lab (CES),
National Engineers School of Sfax-Tunisia

ABSTRACT

The design of cryptographic mechanisms in automotive systems has been a major focus over the last ten years as the increase of cyber attacks against in-vehicle networks. The integration of these protocols into CAN bus networks is an efficient solution for leaving security level, but features of CAN bus make the performance requirements within cryptographic schemes very challenging. In the literature most of academic researches focused on designing security mechanisms for the CAN bus. Yet, very few research proposals are interested in analyzing performances requirements by using cryptographic protocols. In this paper, we investigate effects of implementing cryptographic approaches on performance by proposing an analysis methodology for implementing cryptographic approach in CAN bus communication and measuring real-time performances. Next, we propose our system which presents a tool for determining the impact of implementing of cryptographic solutions. On the other hand we have proposed an intrusion detection system using the same platform. Our tool allows the implementation of any security strategy as well as the real-time performance analysis of CAN network.

KEYWORDS

CAN bus, In-vehicle Network, Security, Analysing

1. INTRODUCTION

Nowadays, numerous in-vehicle functionalities are insured by computer components, called Electronic Control Units (ECUs) [1]. Modern cars can contain from 70 to100 of these devices [2]. At previous years, functions aboard vehicles were developed as ECUs composed of a microcontroller, sensors and actuators. With the increase number of functions such as anti-lock braking system (ABS), Electronic Stability Program (ESP), air bag, multimedia, infotainment etc. As well as with the need of these purposes to be distributed over several ECUs, communication between calculators has become a need. In order to satisfy this requirement, automakers have developed some networks like Controller Area Network (CAN), FlexRay, MOST, and LIN [3]. Today, the CAN bus has become the most widely used network in automotive applications (thanks to an excellent stability, a considerable flexibility and a low cost).

By development of automotive networks, communication between nodes has become more efficient. CAN bus is the based protocol of in-vehicle networks. But the CAN message has a broadcasted nature [4]. Moreover, the CAN protocol does not contain any authenticator field [5]. Therefore, it is easy for any attacker to full control the network message transmission, as

Dhinaharan Nagamalai et al. (Eds) : CSEIT, NCS, SPM, NeTCoM - 2018
pp. 171–186, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81813

mentioned in previous study like [6] and [7]. Until recent years, security has not been a concern in spite this clear issue.

On the other hand, vehicles have not no more been a closed machine. In fact, modern cars can connect to wired-devices like USB and CD or wireless one like 4G, smart phone and Wi-Fi, even communicate with their similar. Therefore, vehicle becomes an open system which increases the probabilities of attacks [8]. Consequently, CAN bus's security becomes a big concern and it takes over a place between recent topics for researches as well as automobile manufacturers since it threats the security of passengers as well as the safety of networks .

To address such attacks, two main layouts of security have been appeared: detection system (IDS) of attacks or anomalies on the one hand and cryptographic mechanisms to ensure confidentiality and authentication and on the other hand. Although, several researches have been oriented towards IDPS system, they have been still not 100% robust and they could not prevent all types of attacks. To exceed limitations of detective measures, many researches aim to adopt cryptographic strategies since they have been improved, in internet networks, their efficient in thwarting attacks. The challenge of designing data encryption or signature mechanisms is to protect real-time performances from being impacted.

A security mechanism is any procedure designed to prevent an attack from taking place [9]. Since the complexity of automotive systems, the implementation of a one mechanism may not frustrate all type of attacks thus the adaptation of the 'defence-in-depth' principles, which based on using of recent security mechanisms, for minimizing risks.

Our main contribution in this paper, is the design of a tool which allows, on the one hand, the implementation of a CAN bus security mechanism and the analysis, on the other hand, of real-time performances resulting from the implementation of cryptographic mechanisms. So, we deployed the same tool to develop an intrusion detection mechanism in CAN networks. The method is based on the analysis of the time intervals of the CAN message.

The remainder of this paper is organized as follows. In section II, we give a general view about automotive security issues and requirements of security solutions related to. We introduce the related work in section III. Section IV depicts the presentation of the analysis method. Section V depicts the presentation of the detection system .In Section VI, details of the proposed platform are given. We conclude in Section VII.

2. AUTOMOTIVE SECURITY ISSUES

2.1. CAN Bus Vulnerabilities

In [10], Wolf et al. show that security in CAN bus is very challenging since it cannot guarantee the following security services:

- Confidentiality: each CAN message is accessible by all nodes connected to the bus. In fact, CAN frames are transmitted in the bus according to a broadcast nature. Then, the CAN bus cannot guarantee confidentiality since an authorized node can listen to the bus and read messages.

- Authenticity: since CAN bus frame has no authentication information about the sender, an attacker connected to the bus could use the ID of any node to send a fake message.

- Availability: due to the arbitration scheme of the CAN bus, any node can put the bus in a dominant state and prevent other from sending messages which could result DoS (Denial of Service) attacks.

- Integrity: CAN protocol uses CRC (Cyclic Redundancy Check) to verify whether a message has been modified. However, this latter cannot prevent an attacker from modifying a legitimate message. In fact, she could make a correct CRC for a forged message.

- Non repudiation: in CAN protocol, it is impossible for a legitimate ECU to prove that it has sent or received a given message.

- CAN message contain between 1 and 8 bytes. So, the security protocol cannot transmit any extra authenticated data inside the classic data field (Figure 1).

- In automotive networks, the primary focus is on real-time capabilities to support control systems, which are needed to respond within a given short time. So, predictability and reliability are the dominating factors.

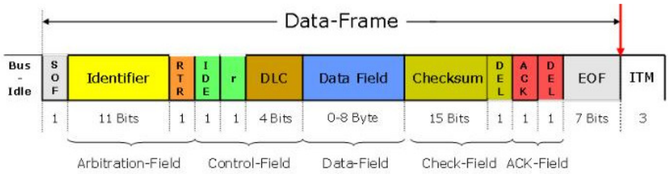


Figure 1.CAN format frame

2.2. Requirements of CAN Cus Security Solutions

- The implementation of a security mechanisms addressing CAN security issues have became urgent. However, the implementation of such solutions meets the following requirements which need to be satisfied:

- Lightweight: since in automotive system computer are very limited in computing power and memory space, heavy cryptographic functions are difficult to be performed by these ECUs. Therefore, the proposed mechanism should be as lightweight as possible.

- Respect of real-time constraints: often, applications of CAN bus are required by hard-real time constraints. Thus, security mechanism should not be impact embedded real time performances.

- Backward compatibility: the proposed mechanism should be compatible with used technologies: we are talking about retro-compatibility. On the other hand, external communications should not be prevented by the security system: we refer to t interoperability.

- Encryption: as we have seen above, a CAN data frames are easy to be eavesdropping by an attacker. So, a method of encryption should be employed in order to provide confidentiality.

- Authentication: in order to guarantee authentication of transmitted data, a hash-based message authentication code (HMAC) must be generated and transmitted along with CAN messages.

3. RELATED WORK

In [11], Nilsson et al. propose to calculate the MAC on the compounded messages then divide it into four parts and transmit them in the CRC field of the next four CAN-messages. In [12], CANauth, a lightweight authentication mechanism based on HMAC for use on the CAN bus, is proposed. The proposed authentication method is transmitted using the out-of-band CAN+ protocol, which uses 15 bytes of the CAN message as authentication data message. Both [11] and [12] give only theoretical analysis which makes it difficult to judge the performance of proposed solutions. In [13], Groza et al. propose LibraCAN, an authentication protocol based on key splitting and MAC mixing for CAN+. In Libra-CAN, the bandwidth requirements are not possible for regular CAN which makes the overhead is unacceptable. Woo et al. in [14], propose the use of AES-128 for encryption and HMAC. The proposed protocol uses 16 bits in the extended ID field and the 16-bit CRC field for transmission of 32 bits code. The implementation of the proposed protocol keeps the bus load under 50% when the CPU clock rate is 60 MHz Woo-auth provides acceptable overhead on a CAN bus. In [15], Nurnberger et al. introduce VatiCAN which enables sender and receiver ECUs to exchange authenticated data using the Keccak algorithm. Authors provide that VatiCAN guaranties a respect of real-time deadlines for safety-critical application. But it is hard to judge in case for the total system. Several security solutions proposed. However, a concrete real-time performances analysis is still limit in literature.

On the other hand, Müter et al. propose in [16] the calculation of entropy of CAN bus while the observing of traffic during a "normal" activity. If a deviation in entropy (compared to reference values) is found, an alert is then lifted. Hoppe et al. proposed IDS and demonstrated anomaly detection method by looking at frequency of messages transmitted on the bus [17].Meanwhile, authors in [18], propose an approach where each ECU has a sensor that observes the interaction of the latter with the network (sent messages but also consumed messages). Intrusion detection is based on a set of security rules based on network protocol specifications and host ECU. Intrusion detection is done in each ECU independently. Similarly, authors in [19] and [20] propose the saturation of the bus as a reaction to attacks. In [19], Miller and Valzak build a small device that plugs into the OBD-II port of a car, learns traffic patterns, and then detects anomalies. When the device detects something, it shorts circuits the CAN bus, thus disabling all CAN message. In [20], the solution presented is based on the monitoring of network traffic by each of the present ECU. When a calculator observes a message circulating on the bus, which is supposed to be its transmitter (based on the ID of the message), the ECU immediately sends an alert to crush the transmitted message. However, previous mechanisms require to be implemented in each ECU. So, they are considered as expensive solutions. Studnia et al. proposed in [21] an intrusion detection approach for an integrated automotive network. The proposed solution based on the definition of a formal language dedicated to generate a signature set for attacks aims to detect.

4. THE ANALYSIS METHODOLOGY FOR A SAFE CAN BUS COMMUNICATION

The first system, which we propose to design, aims at analyze the security performances on CAN bus network after implementing a cryptographic mechanism. In this section we want to highlight the method we used for: subsection A introduces the system model. Subsection B, explains the methodology phase and algorithms process are given in subsection C.

4.1. System Model

In this section, we introduce the system model which we adopted for implementing our method. As shown in Figure 2, our system model is composed of 2 CAN nodes connected to a CAN bus to form a network. The Node 1 with ID =0x1 send messages to Node 2 with ID =0x1.

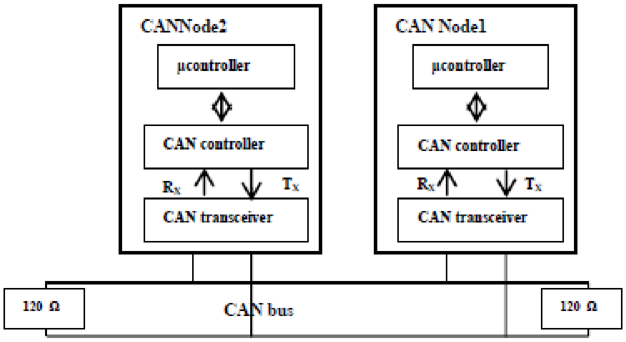


Figure 2.Synoptic diagram of system model

4.2. Fundamental Idea

The main problem on the communication side is the overhead caused by the additional data in combination with possible additional latency. Both are especially challenging when dealing with short signals requiring real time operation and low latencies. Our goal is to develop a system which can be deployed for implanting a cryptographic mechanism along with analysis real-time performances and injecting spoofed message. The proposed method allows determining the effect of security mechanism on CAN bus performances. In our work, we adapt the automotive network architecture consists of two nodes connected to CAN bus in the vehicle via a serial data communication bus. Each ECU controls a particular function of the vehicular system. The fundamental idea is to encrypt a given message in Node 1 by a cryptographic mechanism and send it to Node 2. When this latter receive the encrypted message, deploys the same mechanism to decrypt it.

4.3. Methodology Phases

Since we aim to implement cryptographic approach in the standard version of CAN protocol, the transmission process of CAN message will be different than the classic one. The whole transmission process is summarized in Figure 3. When the sender node receives a request from the receiver, it encrypts data; divides it into segments then it sends the segments via CAN bus. When the receiver gets segments, concatenates it to get complete data then it decrypts to get the original message.

4.3.1. CAN Message Encryption Phase

We need encrypt the message since we need guarantee confidentiality and integrity of automotive data network. The CAN message encryption phase is insured by encryption mechanisms and MAC methods.

4.3.2. Fragmentation Technique

As the maximum payload length allowed in the CAN data field is only 8 bytes, the available space for appending a cryptographically secure Message Authentication Code (MAC) is very limited. To solve this problem, rather than appending a MAC in one CAN frame's data field, we suggest a technique for dividing data into a size that can be stored in a message (including the sequence information) and then, each segment is transmitted.

4.3.3. CAN Message Transmission Phase

The transmission of CAN frame is carried out from the sender node to the receiver one following the CAN protocol and via CAN bus.

4.3.4. CAN message Reconstitution Phase

After the sender node receives messages, they should be reconstituted to the original form.

4.3.1. CAN Message Decryption Phase

The resulted message is decrypted to obtain the original message.

4.3.1. Calculating Clock Cycle

The last step of our methodology is calculating the clock cycle needed to perform a CAN data transmission (more detailed information can be found in the second sub-section of the next section).

5. DESIGN OF INTRUSION DETECTION SYSTEM

Our goal in this paper is to design an IDS aims at detecting attacks on CAN bus network and based on analyzing of message frame. To reach our goal we adopt three steps: analyze CAN messages, inject malicious frames on bus network and implement the proposed algorithm. This section details the design of this IDS: Subsection A describes the system model, in subsection B, we give the threaten model and the third subsection details the fundamental idea of our approach.

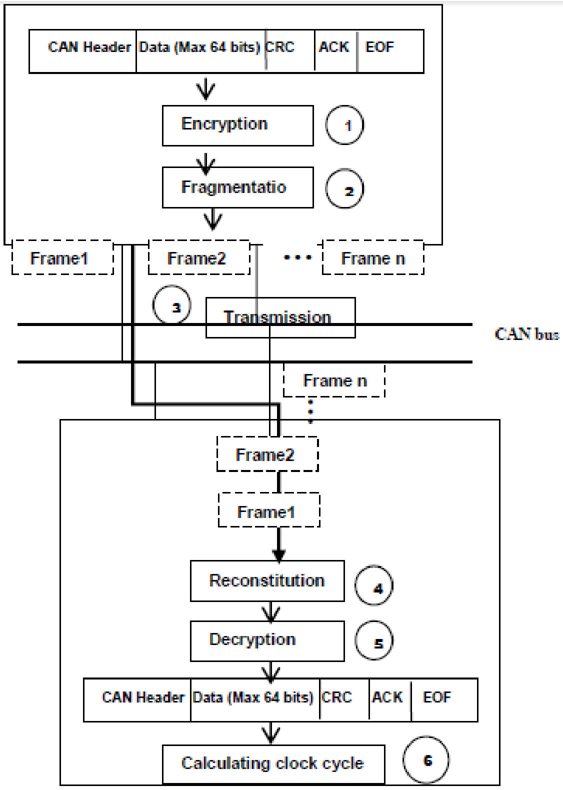


Figure 3. Overall process of analysis Methodology for a Secure CAN Bus Communication

5.1. System Model

We adapt the automotive network architecture consists of three nodes connected to CAN bus in the vehicle via a serial data communication bus. Each ECU controls a particular function of the vehicular system. As shown in Figure 4.

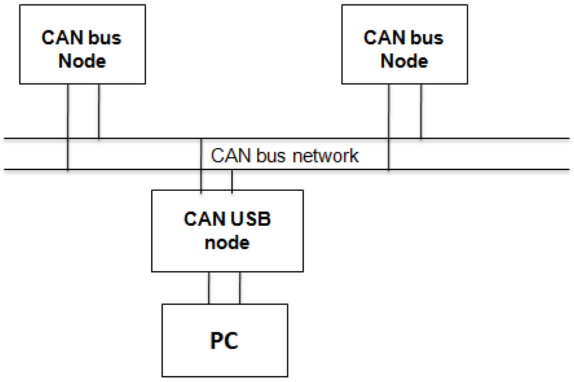


Figure 4. System Model

5.2. Threaten Model

If we consider the way over it the attacker could accede to the network, we assume this attack models: the adversary access to the CAN network by compromising an existing ECU. The attacker compromise one ECU to send frames with correct ID but from different ECU compared to its legitimate one. So, authorized ECUs believe that is a legitimate message and it is sent by an authorized one. The goal of our work is the detection of intrusions regardless to their origins.

As mentioned later, CAN bus has not any type of authentication. Therefore, if an attacker succeeds to access to the bus, he could get code running on an ECU (via an attack over Bluetooth, telemetric, tire sensor, physical access…). Also, she could full control the vehicle by injecting spoofed messages. As the attacker tries to send a malicious message to an ECU, as well as authorized ECUs still send their normal messages periodically. So, the target ECU will receive messages from the authorized ECU and from the attacker. Thus, the attacker reaches his goal to transmit injected message, unless she sends it faster than the original ECU. Previous researches like [19] and [22] mentioned that an attacker should send messages from 20-100 times faster than the original ECU to make the target ECU listens to the injected messages. Finally, the rate of messages on the network will be increased more than two times (20 – 100 times) higher than the normal

5.3. The Fundamental Idea

In the following subsection, we describe the different features of our IDS, as well as the working process.

5.3.1. IDS Description

We adapt the Intrusion detection system with this aspect:

- Data source: the proposed IDS is a network intrusion detection systems (i.e.it analyzes incoming network traffic).
- Method of detection: as its ability to detect new attack as well as its easy implementation than the Signature- based IDS, we adapt Anomaly-based IDS.
- Frequency of analysis: the detection is in real time
- Concerning its behavior after detection, our IDS is dedicated to alert the user if suspicious frame is detected
- In our work the IDS dedicated to detect frames including incorrect ID and malicious frames generated periodically while the transmission of a normal traffic.
- As each authorized ECUs send their normal messages periodically, the time interval of each CAN ID is unique. Therefore, our IDS detects messages which their IDs do not respect their own interval time, as the procedure in the next section.

5.3.2. Process Principal

After introducing the main aspects of our IDS, we continue with presenting the procedure according to it our system detects messages: each ECU connected to CAN bus sends its message regularly. So, each message ID (0x1, 0x2 ,…) has its own regular frequency or interval. The IDS checks the arrival time of CAN ID. It calculates the time interval of the arrival message compared to last message. If the interval message is less than the normal one, the alert will be lifted. The entire process of the IDS is summarized in Figure 5.

6. TEST ENVIRONMENT

This section is dictated to detail the test environment of the proposed IDS: we give the hardware architecture in subsection A. Subsection B describes the experimental setup. Last subsection details algorithms process of the analysis method.

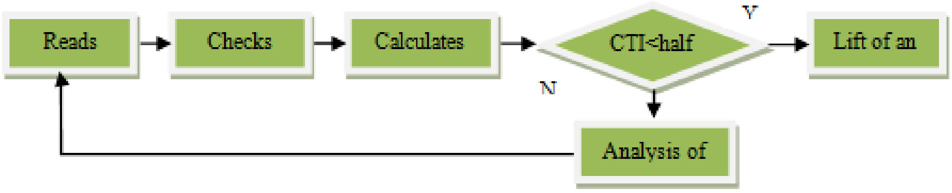


Figure 5. Flowchart of the proposed intrusion detection system

6.1. Hardware Architecture

In Figure 6, the block diagram of the proposed analysis methodology is shown (system 1). This system consists essentially of two CAN nodes which are all connected to a transmission medium (medium) looped by two termination resistors.

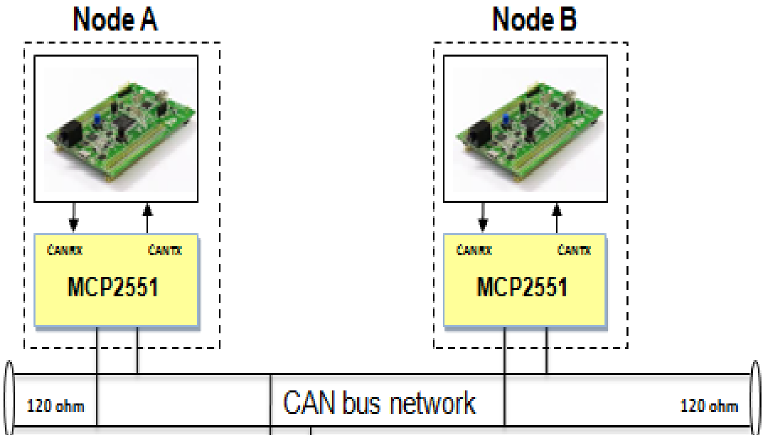


Figure 6. Block diagram of System1

The block diagram of the proposed IDS (system 2) is shown in Figure 7.This system consists essentially of two CAN nodes and a CAN-USB node which is all connected to a transmission medium (medium) looped by two terminating resistors.

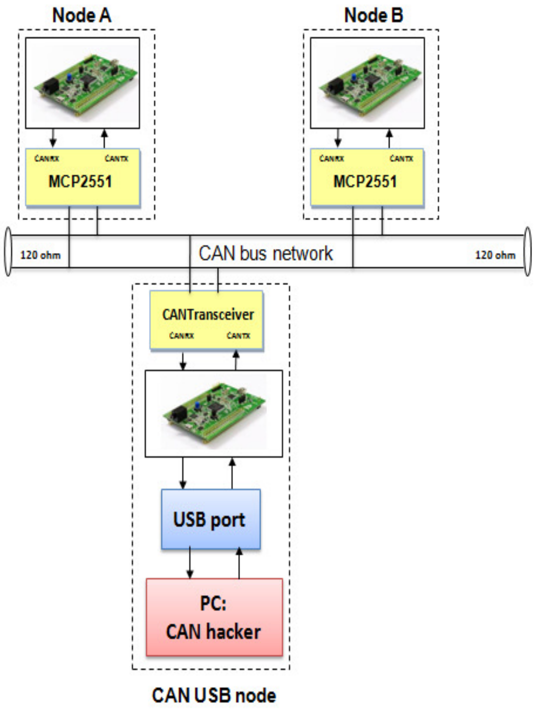


Figure 7. Block diagram of System2

6.2. Description of Platform

To design our methodology which allows implementing cryptography protocols and IDS, we proposed a platform compound of CAN nodes as shown in Figure 8. We chose ST Micro electronics'32F407 microcontroller board [23] with a 32 bit ARM Cortex-M4 core clocked at 16 MHz and an adaptive real-time accelerator since it is characterized by features could help as in our application. As CAN transceiver, we chose MCP2551 .We made the transmission in twice to remove any type of parasite terminal by two 120W resistor to provide CAN bus communication capabilities. For the implementation of algorithms, we proposed the Keil MDK 5 as an integrated development environment (IDE) to program STM32 and the STM32CUBEMX tool for configuration.

To adopt security into the CAN bus network, we included the STM32 cryptographic library package (X-CUBE CRYPTOLIB) in particular AES-128 in CMAC mode which has a 128-bit long key and a 128-bit message in output. Since the CAN data message could contain 108 bits in totally, we choose to append MAC to the data field and truncated it to 2 bytes then concatenated the result after be decrypted. The AES-CMAC library is taken from the [24]. The total code size for AES computation was about 2 244 bytes and CAN communication was about 2500 bytes. AES modes CMAC do not have a proper decryption mode like ARC4. So, decryption works exactly like encryption. The tests were executed on STMF4 which their CPU is running at 168MHz. The number of cycles needed is calculated according to equation (2) depending on [25].

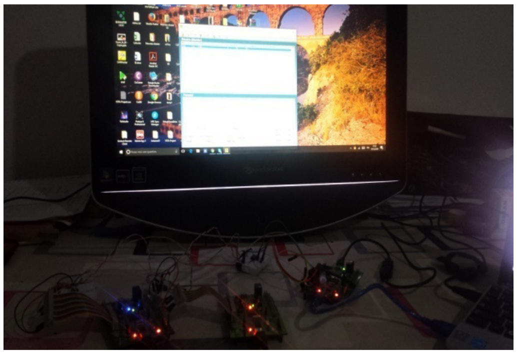


Figure 8. Components of experimental setup

6.2. Algorithms Process of the Analysis Method

In this subsection, we give flow diagrams of different phases

Main Program

The Figure 9 above shows the flow diagram of the main program. At the beginning, we start by the configuration of the stm32. Then we initialize the different devices to use such as USB, CAN and ADC ... Finally, the program is ended by the activation of interruptions if they are triggered.

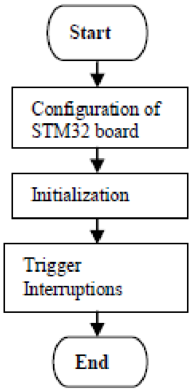


Figure 9. Flow diagram of the main program

AES-CMAC Encryption Algorithm

The following flowchart describes the AES_CMAC Encryption algorithm. Referring to Figure 10, the sender starts the initialization for AES-CMAC Encryption and checks the error status. If the error statutes value is “AES_ERR_BAD_CONTEXT” and “AES_ERR_BAD_ PARAMETER”, the sender node ends the process. Else if the error statutes value is” AES_ SUCCESS”, the sender encrypts data in CMAC Mode and checks the error status. If the error statutes value is “AES_ERR_BAD_PARAMETER”, “AES_ERR_BAD_OPERATION” and “AES_ERR_BAD_INPUT_SIZE”, the sender node ends the process. Else if the error statutes value is” AES_SUCCESS”, the sender finalizes of CMAC Mode and checks the error status. In the both value of the error statutes the sender node ends the AES encryption process.

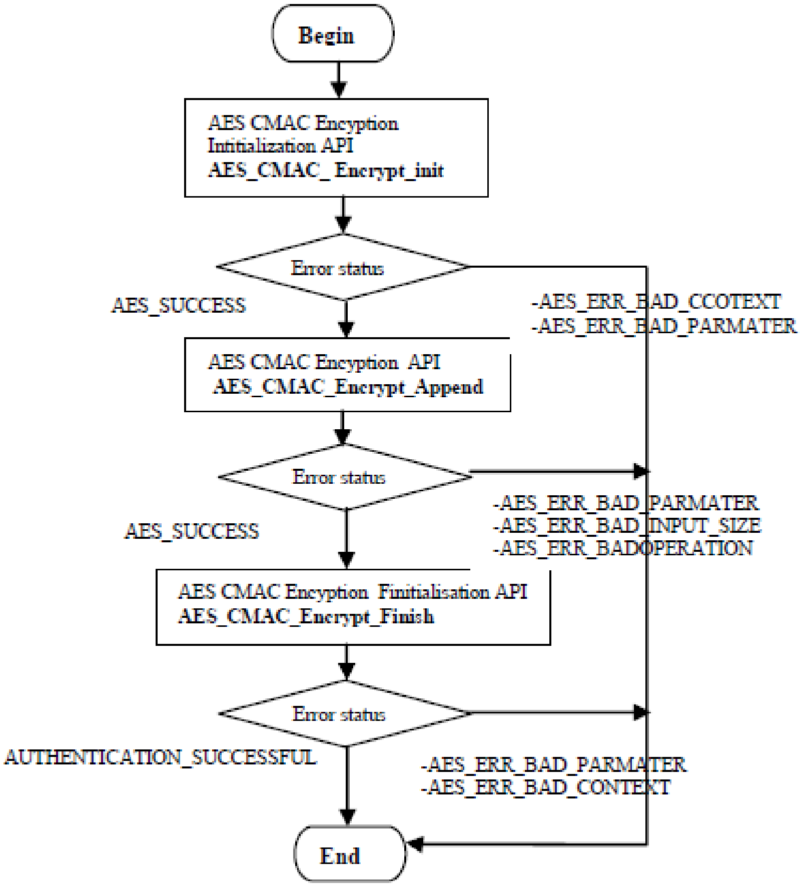


Figure 10. Flow diagram of AES_CMAC algorithm Encryption

AES-CMAC Decryption Algorithm

The next flow diagram describes the AES_CMAC Decryption algorithm. Referring to Figure 11, the receiver starts the initialization for AES-CMAC Decryption and checks the error status. If the error statutes value is “AES_ERR_BAD_CONTEXT” and “AES_ERR_BAD_PARAMETER”, the receiver node ends the process. Else if the error statutes value is” AES_SUCCESS”, the receiver decrypts data in CMAC Mode and checks the error status. If the error statutes value is “AES_ERR_BAD_PARAMETER”,“AES_ERR_BAD_OPERATION” and “AES_ERR_BAD_ INPUT_SIZE”, the receiver node ends the process. Else if the error statutes value is” AES_SUCCESS”, the receiver finalizes of CMAC Mode and checks the error status. In the both value of the error statutes the sender node ends the AES decryption process.

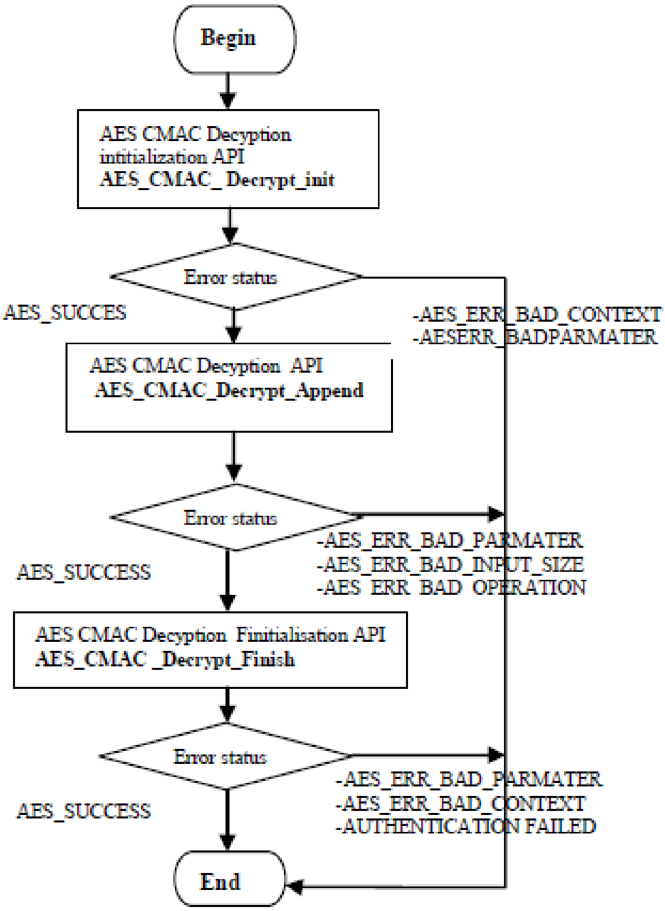


Figure 11.flow diagram of AES_CMAC algorithm Decryption

To determine the impact of using a cryptographic algorithm in CAN bus communication, we need to calculate the number of cycles clock transmit a CAN data. At first we have the number of cycles needed to perform each process is defined as follows:

$$\begin{gathered}\mathit{Cycles} = \mathit{Init\ key\ cycle} + \mathit{Init\ message\ cycle} + \\ \mathit{Process\ block\ of\ data\ cycle} * \mathit{number\ of\ blocks}\end{gathered} \qquad (1)$$

So the number of cycles needed to perform a CAN data transmission is calculated as follow

$$\begin{gathered}\mathit{Cycles}_{\mathit{CAN}} = \mathit{Init\ key\ cycle} + \mathit{Init\ message\ cycle} \\ + \mathit{Process\ block\ of\ data\ cycle} * \mathit{number\ of\ blocks} \\ +2*(\mathit{min\ of\ CAN\ data\ transmission\ cycle})\end{gathered} \qquad (2)$$

7. CONCLUSION

Our main contribution in this paper was the design of a tool that allows on the one hand the calculation of real-time performances resulting from the implementation of cryptographic mechanisms. On the other hand, the proposed system is dedicated to implementing an intrusion detection mechanism for CAN networks that we have designed. The method is based on the analysis of the time intervals of the CAN message. Also, in this work we have developed an efficient experimental platform for the analysis, the implementation of a secure communication on the CAN bus and the injection of the usurped messages. .As perspective of this work, we intend to evaluate proposed methods by the implantation and the comparison between them.

REFERENCES

[1] C. Miller, C. Valasek, (2015) “Remote exploitation of an unaltered passenger vehicle”, BlackHat USA.

[2] R. N. Charette, (2009) “This car runs on code,” IEEE Spectr.,vol. 46, no. 3, p. 3.

[3] R.B.GMBH, (2014) “Bosch Automotive Electrics and Automotive Electronics”, 5 ed. Bosch Professional Automotive Information. Springer Vieweg.

[3] TEXAS INTRUMENTS, (2016) “Introduction to the Controller Area Network (CAN)”, Application Report, SLOA101B–August 2002–Revised May 2016.

[4] C-W. Lin, A. Sangiovanni-Vincentelli, (2012) “Cyber Security for the Controller Area Network (CAN) Communication Protocol”.

[5] S. Checkoway, D. McCoy, et al., (2011) ”Comprehensive experimental analyses of automotive attack surfaces”, Proc.20th USENIX Security, San Francisco, CA.

[6] C. Miller, C. Valzek, (2013)“Advanture in automotive networks and control units”.

[7] K. Koscher, A. Czeskis, et al., (2010) “Experimental Security Analysis of a Modern Automobile, IEEE Symposium on Security and Privacy”.

[8] Prescott.E.Small, (2011) “Defense in Depth: An Impractical Strategy for a Cyber World"

[9] M. Wolf, A. Weimerskirch, & C. Paar, (2004) “Security in automotive bus systems“, Workshop on Embedded Security in Cars.

[10] D.K. Nilsson, U.E. Larson, and E. Jonsson, (2008) “Efficient In Vehcile Authentication Codes”, Vehicular Technology Conference VTC.

[11] A. Van Herrewege, D. Singelee, I. Verbauwhede, (2011)“Canauth - a simple, backward compatible broadcast authentication protocol for can bus”, ECRYPT workshop on Lightweight Cryptography.

[12] B.Groza, S.Murvay, et al., (2012)“LiBrA-CAN: A Lightweight Broadcast Authentication Protocol for Controller Area Networks”, International Conference on Cryptology and Network Security CANS 2012: Cryptology and Network Security pp 185-200.

[13] S.Woo, H.J.Jo, and D.H.Lee, (2014) “A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN “, In IEEE Transactions On Intelligent Transportation Systems.

[14] S.Nurnberger and Ch. Rossow,(2016) “VatiCAN -Vetted, Authenticated CAN Bus“, International Conference on Cryptographic Hardware and Embedded Systems(CHES)’2016.

[15] M. Müter, N. Asaj, (2011)“Entropy-based anomaly detection for in-vehicle networks”, Intelligent Vehicles Symposium (IV), Baden Baden, Germany, IEEE.

[16] T. Hoppe, S. Kiltz, and J. Dittmann, (2009) “Applying Intrusion Detection to Automotive IT - Early Insights and Remaining Challenge“, Journal of Information Assurance and Security (JIAS), pp. 226-235.

[17] U. E. Larson, D. K. Nilsson, and E. Jonsson, (2008)” An Approach to Specification-based Attack Detection for In-Vehicle Networks”.

[18] C.Miller and C.Valasek, (2014)“A survey of remote automotive attack surfaces”. Last Accessed from http ://illmatics.com/remote attack surfaces.pdf.

[19] T. Matsumoto, M. Hata, et al., (2012)“A method of preventing unauthorized data transmission in controller area network”, Vehicular Technology Conference (VTC Spring), pages 1–5, Yokohama, Japan, IEEE

[20] I. Studnia, E. Alata, et al., (2015)“A language-based intrusion detection approach for automotive embedded networks”, The 21st IEEE Paci_c Rim International Symposium on Dependable Computing (PRDC 2015), Nov 2014, Zhangjiajie, China. Proceedings of the 21st IEEE Paci_c Rim International Symposium on Dependable Computing (PRDC 2015).

[21] H. M. Song, H. R. Kim and H. K. Kim, (2016)“Intrusion Detection System Based on the Analysis of Time Intervals of CAN Messages for In- Vehicle Network”.

[22] (2017) “STM32F407VG”, http://www.st.com/en/microcontrollers/stm32f407vg.html.

[23] (2015) “UM1924 User manual STM32 crypto library”, www.st.com.

[24] (2013) “UM0586 User manual STM32 Cryptographic Library”, www.st.com.

Authors’ Information

[1]National Engineers school of Gabes ENIG, Tunisia, Avenue Omar Ibn Alkhattab, Zrig Gabes 6029

[2,3] Engeneering School of Sfax ENIS Tunisia, Route de Soukra, Km 3.5 BP W, 3038 Sfax

[1]**Mabrouka Gmiden** received the engineering degree in electric and automatic from the national Engineers school of Gabes (ENIG), Tunis in 2012. She is currently working toward the Ph.D. degree at National Engineers school of Gabes (ENIG). She is a member of Computer Embedded Systems Laboratory (CES Lab) in the national Engineers school of Sfax (ENIS). His research interests include automotive, security, cryptography, CAN bus security. E-mail: mabroukagmiden@hotmail.fr

[2]**Mohamed Hedi Gmiden** received the B.S. degree in Electrical Engineering, the M.S degree and Ph.D. degree in automatic and industrial Computing from in the national Engineers school of Sfax (ENIS), University of Sfax, in 1996, 2004 and 2011 respectively. He joined the Tunisian University in 2007. He is currently an assistant professor in Higher Institute of Industrial Systems (ISSIG), University of Gabes. He is a member of Computer Embedded Systems Laboratory (CES Lab).
E-mail: mohamedhedi.gmiden@enis.rnu.tn

[3]**Trabelsi Hafdh** received the B.S. degree from Sfax Engineering School (ENIS), University of Sfax, Sfax, Tunisia, in 1989, the M.S. degree in the Central School of Lyon, France, in 1990, the Ph.D. degree from the University of Paris XI Orsay, France, in 1994, and the "Habilitation Universitaire" in the National Engineering School of Sfax (ENIS), University of Sfax, Sfax, Tunisia, in 2008, all in electrical engineering. He is working toward the Research Management Ability degree in the field of electrical machine design at SES. He joined the Tunisian University, Tunisia, in 1995. He moved to the ENIS in 2000. He is currently a Professor of Electrical Engineering. He is a member of the Research Unit on Renewable Energies and Electric Vehicles of the University of Sfax, where he is the chair of the Electric Machine Design Team. He is a member of the Organizing Committee of the IEEE International Conference on Signals Systems Decision and Information Technology. E-mail: hafedh.trabelsi@enis.rnu.tn

RANDOMIZED DYNAMIC TRICKLE TIMER ALGORITHM FOR INTERNET OF THINGS

Muneer Bani Yassein, Ansam Alnadi, Asmaa Bataineh

Computer Science Department, Jordan University of Science and Technology,
Irbid, Jordan

ABSTRACT

Routing Protocol for Low Power and Lossy Networks (RPL) is one of the most utilized routing protocols. It designed to adapt with thousands of nodes in energy-constrained networks. It is a proactive distance vector protocol which has two major components objective function and trickle algorithm. Our work focus on the trickle timer algorithm, it is used to control, maintain and follow the control messages over the network. Short listen problem is the main blot in trickle algorithm. Several studies focused on enlarging the listen period. However, as it was suffering from node starvation when the period is short, it suffers from time and energy wasting when the period is enlarged. Notice that the time and power consumption are sensitive factors in Low Power and Lossy Networks. In this paper, we propose a randomized dynamic trickle algorithm, it contributes in the improvement of trickle and solving the above-mentioned problems by controlling the t variable in a dynamic randomly way, where t is the border line between listening and transmitting period. The performance of the proposed algorithm is validated through extensive simulation experiments under different scenarios and operation conditions using Cooja 2.7 simulator. Simulation results compared with the standard trickle timer algorithm based on convergence time, packet delivery ratio (PDR) and power consumption performance metrics. The results of the simulations denote a high improvement in term of convergence time, power consumption and packet delivery ratio

KEYWORDS

Routing Protocol for Low Power and Lossy Networks(RPL), Internet of Things (IoT), Trickle Timer Algorithm.

1. INTRODUCTION

Internet of Things (IoT) is an enthusiastic topic in our era. The concept of IoT referred to a set of real world objects that communicate with each other through wireless sensors networks (WSN) [1, 5,16]. A communication means that we can transfer the information and knowledge between components through a media [3, 5]. Many routing protocols are used to achieve this goal [2,14,15]. In order to employ and use IoT functions, we need machine to machine protocols [3]. Daily, large number of devices emerges and creates a huge communication links between each other in every time unit [4]. The emergence of smart things makes our world smarter [5]. Using IoT, many applications in real life will be better in the future like education, healthcare, industry and others [6, 8]. In wireless sensor networks, there are two types of nodes: a source node that

Dhinaharan Nagamalai et al. (Eds) : CSEIT, NCS, SPM, NeTCoM - 2018
pp. 187–197, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81814

transmits the data and a sink node that receives the data [1]. a source node sends a packet to the destination node through a path. There are many routing protocols used to explore the best path, each one has a specific algorithm to get a discovery path to arrive a destination node [1]. One of the most important protocols is the Routing Protocol for Low Power and Lossy networks (RPL) [7, 8]. RPL uses algorithm called Trickle Timer Algorithm to deliver a packet from a source to a destination [7, 8]. When we study the RPL protocol, we focus on three issues: power consumption, packet delivery ratio (PDR) and convergence time. Because of the limitations of the resources [8, 6] like a battery, always our target is minimize a power and time and to maximize the number of delivered packets [8]. The main problem in trickle timer algorithm is short listen period problem, so this leads some nodes to be starved or suffered from a long latency time [7, 1]. In trickle algorithm nodes are always on [9], so this consumes a high percentage of the power. a lot of researchers work to reduce the limitations of this algorithm. They proposed enhancement algorithms such as: Elastic Trickle Algorithm for Low- Power Networks and Internet of Things (Trickle-Plus) [7], fair broadcast suppression (Trickle-F) [8], a new elastic trickle timer algorithm [1], A New Dynamic Trickle Algorithm for Low Power and Lossy Networks [10], Adaptive-k algorithm [11], Trickle-D algorithm [12] and others.

In this paper, we propose an enhancement algorithm of standard trickle timer algorithm called randomized dynamic trickle timer algorithm (RD-Trickle) to meet the problems in standard trickle algorithm in term of three parameters: power consumption, packet delivery ratio (PDR) and convergence time. The rest of the paper is divided as the following: section 3 talks about literature review, section 4 talks about methodology, section 4 talks about conclusion, and section 5 talks about references.

2. TRICKLE TIMER ALGORITHM

Each node in Trickle timer algorithm has many intervals [1]. Major interval begins from I_min value and ends with I_max value [7]. Both I_min and I_max values are determiners variables of the major interval. Major interval contains subintervals; each interval begins from I_start value and ends with I_end value. Both I_start and I_end values are determiners variables of each subinterval. Subinterval begins with I_start value, so I_star0074 = I_min and ends with I_end = I_start*2 [1]. At starting point, the first subinterval is executed until the end, then a next subinterval starts and the same thing for all subintervals until reaches I_max value [10], which indicates that a major interval is ended. The standard trickle algorithm consists of following parameters:

1. I_ min: minimum length of the interval

2. I_ max: maximum length of the interval

3. K: redundancy factor

Also, the following parameters are maintained in trickle algorithm [13]:

1. I: current interval length.

2. C: counter.

3. T: random time within the current interval.

3. RELATED WORK

In IoT, the RPL protocol primarily uses a trickle algorithm to control a flow of messages in term of power consumption, packet delivery ratio and convergence time [7]. Problems in the standard trickle algorithm are considered by multiple researchers. They applied many improvements to enhance trickle limitations. In [7] proposed an enhancement algorithm over a standard trickle algorithm to meet a problem of getting high convergence time with lower power consumption and vice versa. They proposed an Elastic Trickle Algorithm for Low- Power Networks and Internet of Things (Trickle-Plus). Their simulations approved that trickle-plus algorithm made a protocol more flexible. They improved a convergence time and power consumption in an observable way. Advanced Metering Infrastructures (AMIs) consist of a huge number of devices like home devices and education devices, that spread in our real word neither in urban nor in rural environments [8]. C. Vallati et al. [8] proposed a new algorithm named fair broadcast suppression (F-Trickle) to meet the limitations of standard trickle algorithm. F-Trickle chooses a better route from the available routes with insurance of preserving the same number of packets in standard algorithm. Their simulations showed that F-Trickle is effective to choose an efficient route with preserving of the same power consumption value in standard algorithm. M. Bani Yassein et al. [10] proposed a new algorithm called new Dynamic trickle timer algorithm. This algorithm deals with listen only period problems in standard trickle algorithm that effects on convergence time and power consumption [1]. When they applied a new Dynamic trickle timer algorithm through random topology simulations, an enhancement results are observed in term of convergence time, power saving and performance. Also, M. Yassein et al. [1] proposed an algorithm called A new elastic trickle timer algorithm for Internet of Things to deal with listen only period problems in standard trickle algorithm and their effects on power consumption and convergence time[10]. They applied simulations with different number of nodes, and the results indicate that a new algorithm is better than the original algorithm in term of performance, power saving and convergence time. T. Meyfroyt et al. [11] proposed an enhancement algorithm above standard trickle called adaptivek algorithm. Their algorithm made every node adapted its suppression mechanism to local node density. The Adaptive-k algorithm has many advantages over a standard trickle: distribute a load between nodes, adapting the suppression mechanism among different network densities in network topologies and clearly guarantee of the functionality of applying suppression mechanism. A result of simulations showed that a proposed algorithm leads to better performance, easily discovery process of the routes by curb control messages that are considered as redundant. M. Vuˇcini´ et al. [12] proposed a Trickle-D algorithm to distribute a load between nodes in fairly way and reduce the number of messages, so reduce the transmissions through a network. By simulations, Trickle-D achieved its goal in term of load distribution in good manner and improvements on performance in an observable way.

4. RANDOMIZED DYNAMIC TRICKLE TIMER ALGORITHM

According to standard trickle algorithm, if a subinterval does not have enough period for listening and transmitting the data a new subinterval doubled to achieve the remaining work. In trickle, always a double value (I_double = 2) regardless to the situation of the network, node density, number of direct one hop neighbor or others. We must know if the node places in dense network, so it requires a high double value. When a node has low density because of doubled subinterval by 2 problems appeared like low utility problem and loss of time and power. From this point, a problem appeared in standard trickle algorithm. In order to suppress this problem and give each node the required time to complete all its work, after doing simulations, we proposed an enhancement above a standard trickle algorithm that is related to t value. As we observed, there is random time implemented in standard trickle algorithm inside each subinterval. In our proposed algorithm, we determine a time for listening period and transmitting period based on t value within a subinterval. t variable is random time used as listening and transmitting determiner. So our work primarily focuses on choosing t value. We follow a mechanism for choosing t value according to the network density. In order to achieve this, we implement four cases to choose better t value in subinterval as explain in Fig.1 below. Every time, we check a number of neighbors (C) to determine in which range we should choose a random time (t). As we observe from these four cases, if the density is low the range of choosing t value is small, but if the density is high the range of choosing t value is large. The Same thing applies to all cases. As a rule, whenever a density increases a range of choosing t value also increases.

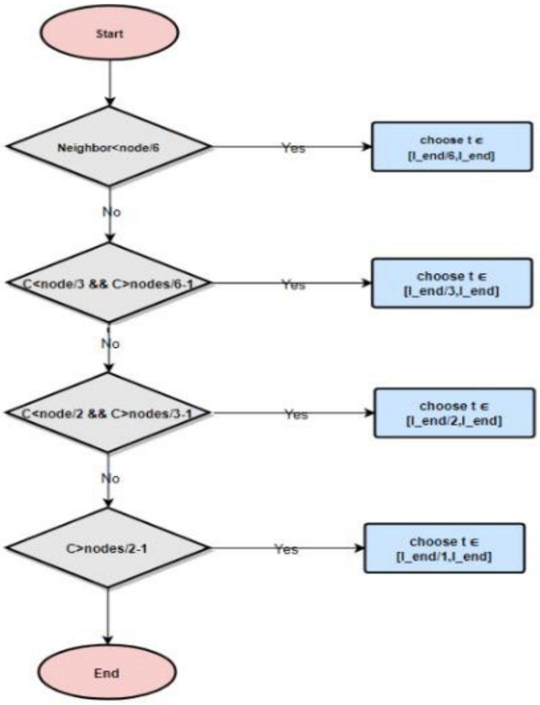
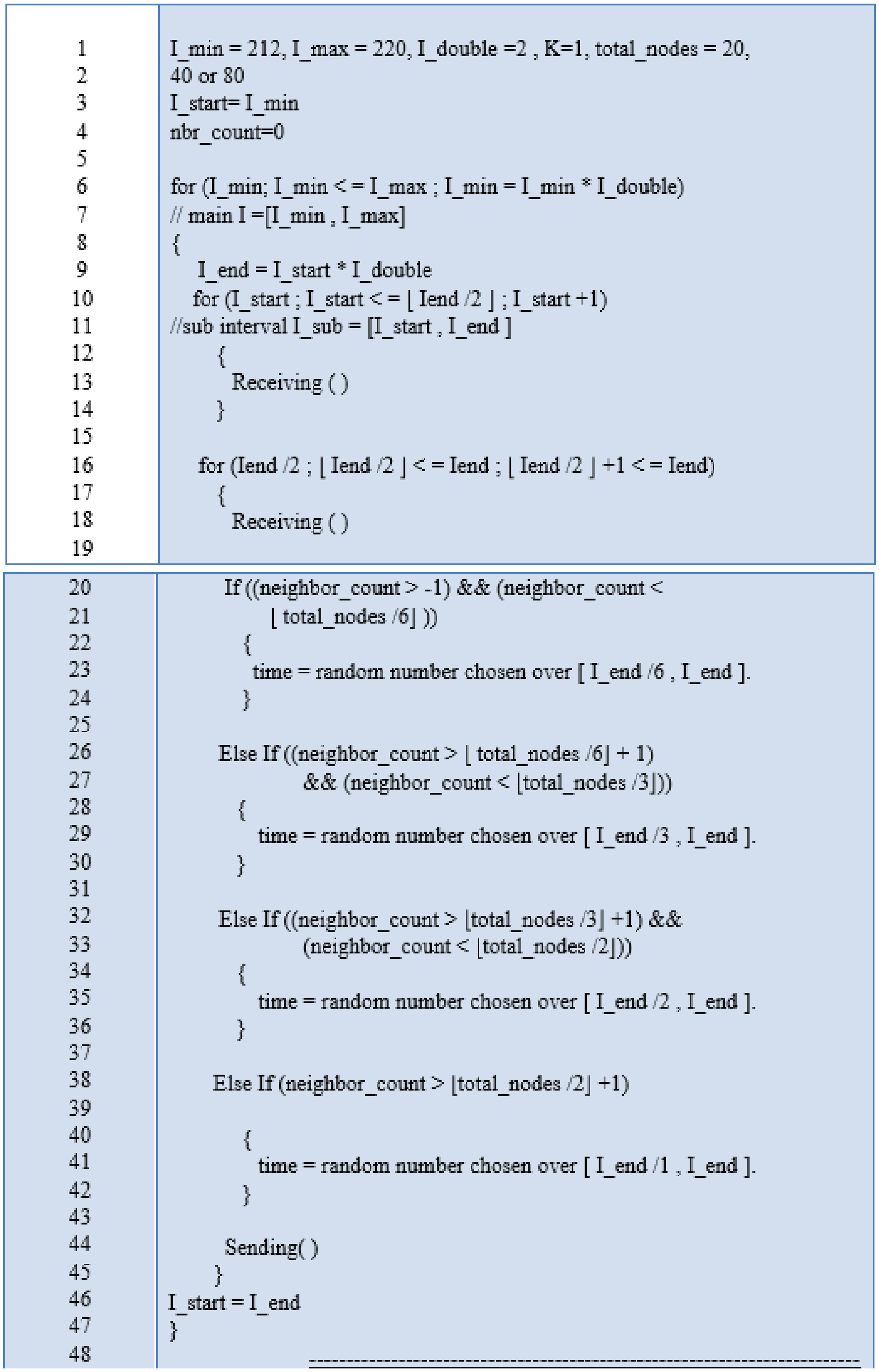

Start
Neighbor<node/6
Yes
choose t ∈ [I_end/6,I_end]
No
C<node/3 && C>nodes/6-1
Yes
choose t ∈ [I_end/3,I_end]
No
C<node/2 && C>nodes/3-1
Yes
choose t ∈ [I_end/2,I_end]
No
C>nodes/2-1
Yes
choose t ∈ [I_end/1,I_end]
End

Figure 1. our proposed method to choose (t) value.

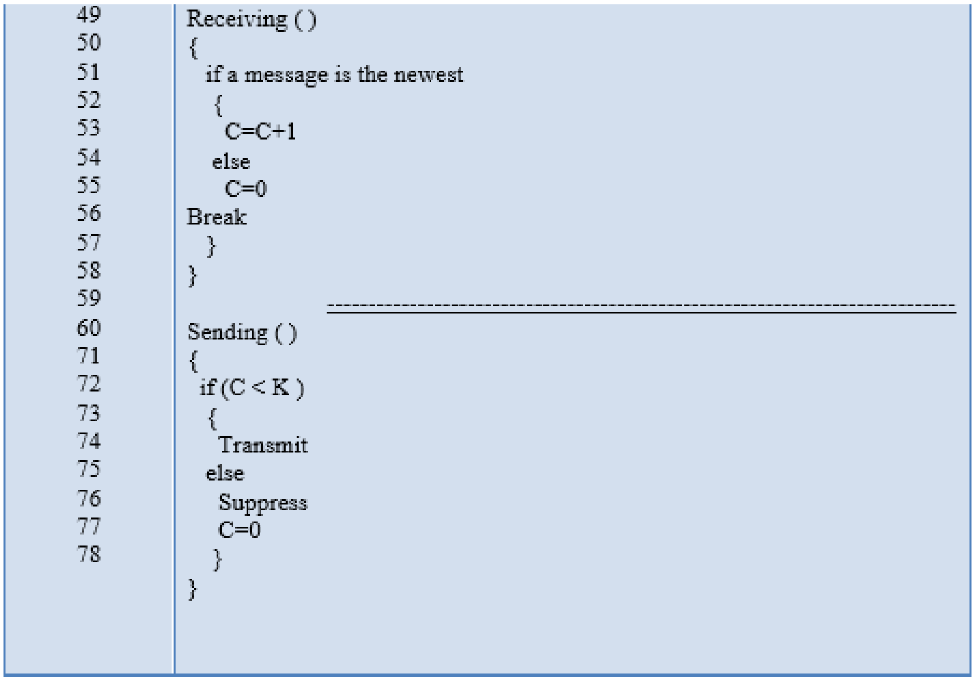
Below is the proposed randomized dynamic trickle timer algorithm:

Randomized Dynamic Trickle Timer Algorithm for each node

Input: Imin, Imax, threshold value (K), nodes.
Output: control message flow



```
I_min = 212, I_max = 220, I_double =2 , K=1, total_nodes = 20,
40 or 80
I_start= I_min
nbr_count=0

for (I_min; I_min < = I_max ; I_min = I_min * I_double)
// main I =[I_min , I_max]
{
    I_end = I_start * I_double
   for (I_start ; I_start < = ⌊ Iend /2 ⌋ ; I_start +1)
//sub interval I_sub = [I_start , I_end ]
       {
         Receiving ( )
       }

    for (Iend /2 ; ⌊ Iend /2 ⌋ < = Iend ; ⌊ Iend /2 ⌋ +1 < = Iend)
       {
         Receiving ( )

        If ((neighbor_count > -1) && (neighbor_count <
               ⌊ total_nodes /6⌋ ))
          {
           time = random number chosen over [ I_end /6 , I_end ].
          }

        Else If ((neighbor_count > ⌊ total_nodes /6⌋ + 1)
                   && (neighbor_count < ⌊total_nodes /3⌋))
          {
            time = random number chosen over [ I_end /3 , I_end ].
          }

        Else If ((neighbor_count > ⌊total_nodes /3⌋ +1) &&
                   (neighbor_count < ⌊total_nodes /2⌋))
          {
            time = random number chosen over [ I_end /2 , I_end ].
          }

       Else If (neighbor_count > ⌊total_nodes /2⌋ +1)

          {
            time = random number chosen over [ I_end /1 , I_end ].
          }

        Sending( )
       }
I_start = I_end
}
                      ---------------------------------------------------------------------------
```

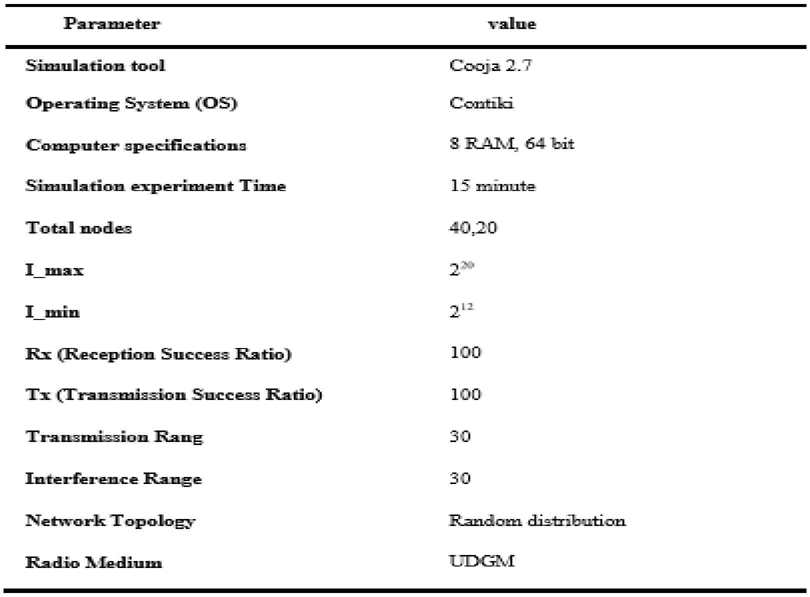


```
Receiving ( )
{
  if a message is the newest
   {
     C=C+1
   else
     C=0
Break
   }
}

Sending ( )
{
 if (C < K )
  {
    Transmit
  else
    Suppress
    C=0
   }
}
```

5. PERFORMANCE EVALUATION

This section will show the performance evaluation of RD-Trickle algorithm in terms of packet delivery ratio (PDR), convergence time and power consumption, comparing with the standard trickle algorithm. Simulation experiments were executed using cooja 2.7 simulator based on Contiki operating system. We perform a randomly deployed topology with two different network densities. For more accuracy result, we repeat each experiment around 10 times taking in the account the average of these experiments with getting rid of some of the thumping experiences. Table I shows the detailed simulation parameters used in our experiments.

Table 1. Simulation parameters.

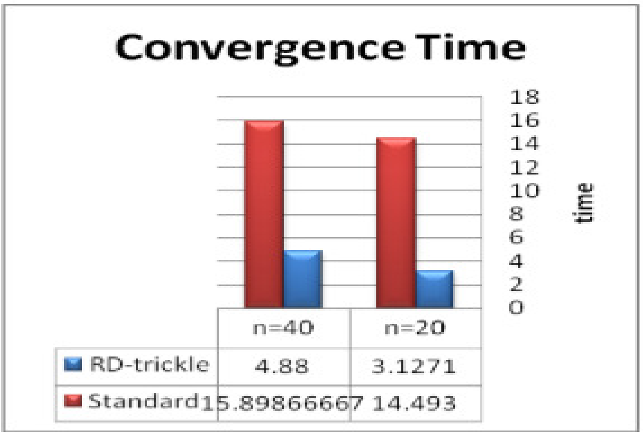


Parameter	value
Simulation tool	Cooja 2.7
Operating System (OS)	Contiki
Computer specifications	8 RAM, 64 bit
Simulation experiment Time	15 minute
Total nodes	40,20
I_max	2^{20}
I_min	2^{12}
Rx (Reception Success Ratio)	100
Tx (Transmission Success Ratio)	100
Transmission Rang	30
Interference Range	30
Network Topology	Random distribution
Radio Medium	UDGM

5.1 CONVERGENCE TIME

5.1.1 RANDOM TOPOLOGY

Fig. 2 shows the average convergence time of our proposed RD- trickle algorithm and the standard trickle algorithm on a different number of nodes deployed on random topology. As the figure shows, our RD- trickle algorithm significantly enhances the time comparing with the standard algorithm on both number of nodes 20 and 40.

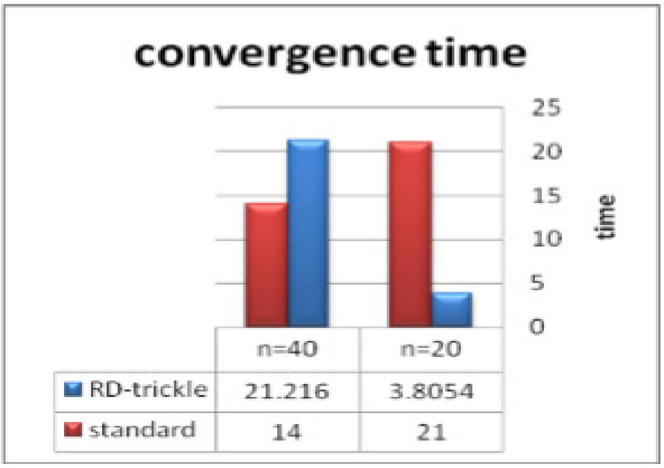


	n=40	n=20
🟦 RD-trickle	4.88	3.1271
🟥 Standard	15.89866667	14.493

Figure 2. convergence time of randomly deployed nodes: 20 and 40.

5.1.2 GRID TOPOLOGY

Fig. 3 shows the average convergence time of our proposed RD- trickle algorithm and the standard trickle algorithm on a different number of nodes deployed on a grid topology. As shown, our RD- trickle algorithm also significantly enhances the time comparing with the standard algorithm when the number of nodes =20. But when the number of nodes increased to 40, RD-trickle goes on a worse way which increases the amount of consumed time comparing with the standard algorithm.



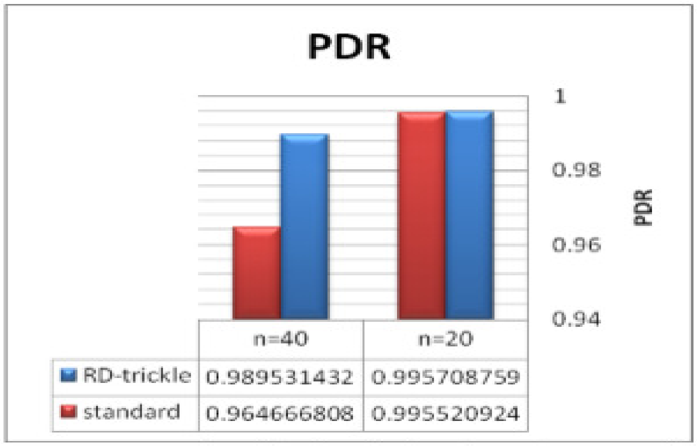
	n=40	n=20
🟦 RD-trickle	21.216	3.8054
🟥 standard	14	21

Figure 3. convergence time of grid deployed nodes: 20 and 40.

5.2 PACKET DELIVERY RATIO (PDR)

5.2.1 RANDOM TOPOLOGY

Fig. 4 shows the average packet delivery ratio (PDR) of our proposed RD- trickle algorithm and the standard trickle algorithm on a different number of nodes deployed on random topology. The figure shows that PDR is not affected when the number of node equals to 20, however, it is enhanced when the nodes increased to 40.

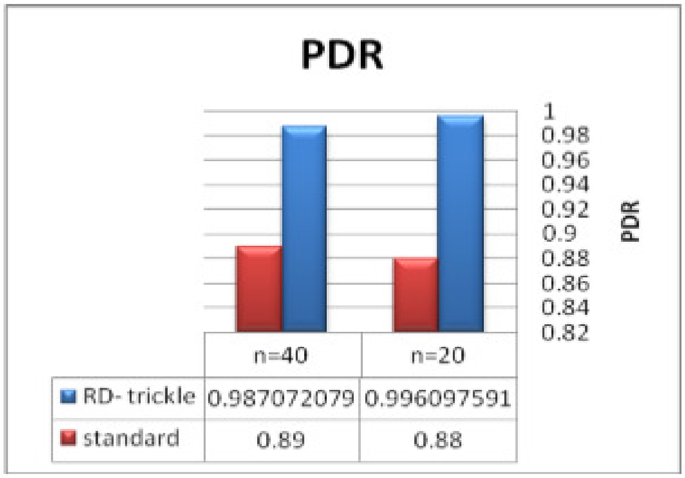


	n=40	n=20
🟦 RD-trickle	0.989531432	0.995708759
🟥 standard	0.964666808	0.995520924

Figure 4. PDR of randomly deployed nodes: 20 and 40.

5.2.2 GRID TOPOLOGY

Fig. 5 shows the average packet delivery ratio (PDR) of our proposed RD- trickle algorithm and the standard trickle algorithm on a different number of nodes deployed on a grid topology. A noticeable packet delivery ratio improvement appears in grid topology on both 20 and 40 nodes comparing with the standard trickle.



	n=40	n=20
🟦 RD- trickle	0.987072079	0.996097591
🟥 standard	0.89	0.88

Figure 5. PDR of grid deployed nodes: 20 and 40.

5.3 POWER CONSUMPTION

5.3.1 RANDOM TOPOLOGY

Fig. 6 shows the average power consumption of our proposed RD- trickle algorithm and the standard trickle algorithm on a different number of nodes deployed on a random topology. When the number of nodes equals to 20, RD- trickle almost consumes the same power that consumed in the standard algorithm. Power consumption enhancement arises when the number of nodes equals to 40.

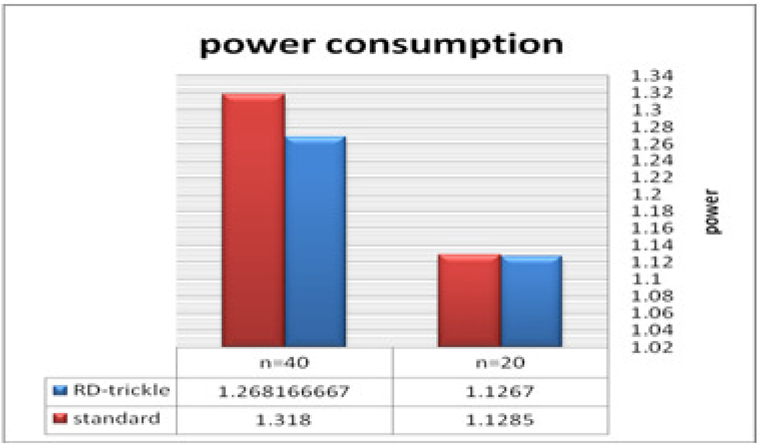


Figure 6. power consumption of randomly deployed nodes: 20 and 40.

5.3.2 GRID TOPOLOGY

Fig. 7 shows the average power consumption of our proposed RD- trickle algorithm and the standard trickle algorithm on a different number of nodes deployed on a grid topology. RD-trickle enhances the power consumption by reducing the amount of consumed power when number of nodes =20, but when the number of nodes = 40 in grid topology RD- trickle consumes power more than the standard trickle algorithm.

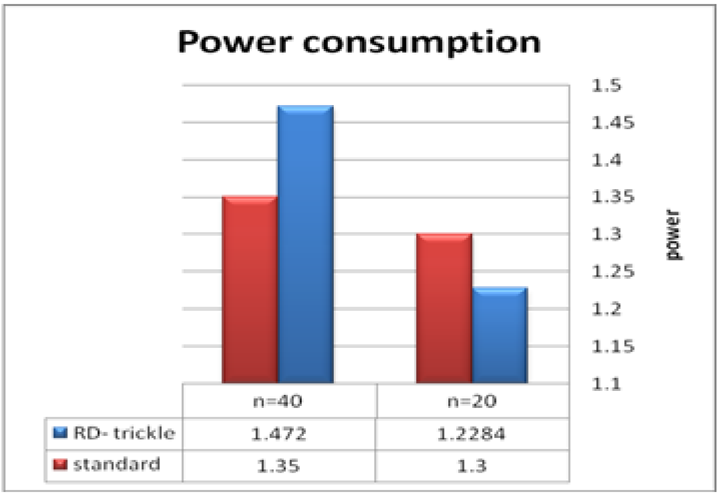


Fig. 7. power consumption of grid deployed nodes: 20 and 40.

6. CONCLUSION AND FUTURE WORK

To control and follow the messages over the Internet of Things (IoT), there is a need for routing protocols. Routing protocol for low-power and lossy network (RPL) is most commonly used routing protocol which is put on the network layer. Trickle timer algorithm is the major component in RPL which is interested in the time of the flow control messages. Trickle algorithm is suffering from short listen only period problem and latency leading to reduce its performance. Popular performance metrics used like packet delivery ratio (PDR), convergence time and power consumption for performance evaluation. If the listen only period set to be long, it will lead to resource wasting and force the nodes to wait with no ability to transmit. On the other hand, short listen only period lead to node starvation and load balancing problems. From this point, the need of a dynamically controlled period has appeared. This study proposed a randomized dynamic trickle timer algorithm (RD- trickle), RD- trickle contributes in solving the above mentioned problems. PDR, convergence time and power consumption used to evaluate its performance. Experiments disclosed that it performs better than the standard trickle in many cases especially in term of convergence time. The best performance appeared on a random topology in both 20 and 40 nodes. Our experiments have executed on cooja 2.7 simulator, Contiki OS. Moreover, some improvements appear in a grid topology, in terms of power consumption and convergence time just when the number of nodes =20, in term of PDR on both 20 and 40 nodes

In the future, we want to pursue study RD- trickle in different RX values noting its behavior and performance. Also, we will examine it to a real service application.

REFERENCES

[1] M. Yassein, S. Aljawarneh and E. Masa'deh, "A new elastic trickle timer algorithm for Internet of Things", Journal of Network and Computer Applications, vol. 89, pp. 38-47, 2017.

[2] N. Kumar, Y. Singh and P. Singh, "An Energy Efficient Trust Aware Opportunistic Routing Protocol for Wireless Sensor Network", International Journal of Information System Modeling and Design, vol. 8, no. 2, pp. 30-44, 2017.

[3] V. Kalyani, P. Gaur, and S. Vats, "IoT: 'Machine to Machine' Application A Future Vision", Journal of Management Engineering and Information Technology (JMEIT), Vol.2, No.4, pp. 15-20, 2015.

[4] A. Niruntasukrat, C. Issariyapat and P. Pongpaibool, "Authorization Mechanism for MQTT-based Internet of Things", Communications Workshops (ICC), 2016 IEEE International Conference on, 2016.

[5] S. Madakam, "Internet of Things: Smart Things", International Journal of Future Computer and Communication, Vol. 4, No. 4, pp. 250-253, 2015.

[6] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey", Computer Networks, Vol.54, No.15, pp. 2787–2805, 2010.

[7] M. Qasem, H. Altwassi, M. Bani Yassein, Ahmed Al-Dubai "Performance Evaluation of RPL Objective Functions", International Conference on Ubiquitous Computing and Communications （IUCC 2015), 2015.

[8] C. Vallati, and E. Mingozzi, “Trickle-F: Fair broadcast suppression to improve energy-efficient route formation with the RPL routing protocol”, Sustainable Internet and ICT for Sustainability (SustainIT), pp. 1-9, Palermo, 2013.

[9] P. Levis, N. Patel, D. Culler, and S. Shenker, “Trickle: A self-regulating algorithm for code propagation and maintenance in wireless sensor networks”, Computer Science Division, University of California, 2003.

[10] M. Bani Yassein, S. Aljawarneh, E. Masa’deh, B. Ghaleb, R. Masa’deh, “A New Dynamic Trickle Algorithm for Low Power and Lossy Networks”, International Conference on Engineering & MIS (ICEMIS), November 2016.

[11] T. Meyfroyt, M. Stolikj, and J. Lukkien, “Adaptive Broadcast Suppression for Trickle-Based Protocols”, IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM), pp. 1-9, Boston, 2015.

[12] M. Vuˇcini´, M. Król, B. Jonglez, T. Coladon and B. Tourancheau, "Trickle-D: High Fairness and Low Transmission Load with Dynamic Redundancy", IEEE Internet of Things Journal, 2017.

[13] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko, “The Trickle Algorithm”, RFC 6206, Internet Engineering Task Force (IETF), 2011.

[14] M. Bani Yassein, W. Mardini, A. Khalil," Smart Homes Automation using Z-wave Protocol", 2016 IEEE International Conference on Internet of Things and Pervasive System, 2016.

[15] M. Charalambous, C. Mavromoustakis, M. Bani Yassein, " A resource intensive traffic-aware scheme for cluster-based energy conservation in wireless devices", 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 2012

[16] S. Manaseer, M. Bani Yassein, "Pessimistic backoff for mobile ad hoc networks", Al-Zaytoonah University, the International Conference on Information Technology (ICIT'09),2009.

INTENTIONAL BLANK

BLACK HOLE ATTACK SECURITY ISSUES, CHALLENGES & SOLUTION IN MANET

Muneer Bani Yassein, Ismail Hmeidi, Yaser Khamayseh
Mohammad Al-Rousan, Danah Arrabi

Faculty of Computer & Information Technology, Jordan
University of Science and Technology, Irbid, Jordan

ABSTRACT

MANET (Mobile Ad-hoc Network) is simply a set of mobile hosts connected wirelessly without any centralized management, where each node acts as a packet sender, packet receiver, and a router at the same time. According to the nature of this network, the dynamic topology and the absence of a centralized management cause several security issues and attacks, such as the black hole attack, the wormhole attack, and the impersonation and repudiation attack. In this survey, we are going to introduce the Black Hole attack security issues and some of the detection techniques used to detect the black hole attack. In this kind of attack (black hole attack) the intruders manipulate the normal behavior of the network, by introducing themselves as the node with the shortest path to the destination. Intruders can do a malicious behavior over the network.

KEYWORDS

MANET, Routing Protocols, Black Hole Attack, AODV, DSR, RREQ, RREP, RERR.

1. INTRODUCTION

MANET is a group of mobile nodes, where each node has a wireless transmitter and a receiver. the nodes communicate together directly or indirectly [1]. Nodes that are in the same radio range communicate with each other through a direct wireless link; which is known as a single-hop network. In a multi-hop network, if one node wants to communicate with a node that is located out of its range, it relies on the intermediate nodes to transfer the data through it to the required destination [1] [2].

The exposed wireless transmission medium, the changing topology and the lack of main management and controlling unit makes the mobile ad-hoc network vulnerable to different kinds of attacks [1-3]. The changing scalability, the limited power supply and the lack of security boundaries that exist in MANETs make it also a subject of attacks [2]. In MANET, the attacks can be either active or passive.

In passive attacks, the attacker does not affect or modify the data transmitted between communicating nodes. it just listens to the traffic between two nodes looking for valuable data to steal it [4]. Such kind of attacks are hard to discover. As an example: traffic monitoring and releasing of message contents. Active attacks are sensitive and dangerous because it aims to change the normal functionality of the network. changing and altering the transmitted data or even sending false replies [4]. As an example: network Jamming, denial of service,

Dhinaharan Nagamalai et al. (Eds) : CSEIT, NCS, SPM, NeTCoM - 2018
pp. 199–207, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81815

impersonating, and black hole attack. From Table 1. The attacks in MANET networks occur on different protocol layers [23-27]:

Table 1. The attacks in MANET networks occur on different protocol layers.

Layers	Attacks
Multilayer Attack	DOS, Impersonation, Reply, Man in the middle.
Application Layer	Repudiation, Date corruption.
Transport Layer	Session hijacking, SYN flooding.
Network Layer	Worm whole, Black whole, Flooding, Location disclosure.
Data link Layer	Traffic analysis Monitoring, Disruption MAC, WEP weakness.
Physical Layer	Jamming, Interception, Eavesdropping.

Now, we introduce some of the most important attacks in MANETs. In Black Hole Attack, the attacking node abuses the routing protocol used in the network to introduce itself as the node that has the shortest path to the destination node. attacking node attracts all packets towards it. This malicious node discards packets without forwarding it to any other nodes[2][3]. In Worm Hole Attack, the malicious node records packets at one point inside the network and then delivers them to another location [2][3]. In Byzantine Attack, the attacking node inserts wrong routing information into the network to create routing loops. forwarding packets through wrong and non-optimal paths or dropping packets cause problems in the routing functions [3]. in this survey, we focus on the Black Hole Attack.

This paper is organized as following: section 2 discusses the MANETs' routing protocols, Section 3 discusses the concept of black hole attack, Section 4 discusses some recent detection schemes, and section 5 is the conclusion.

2. ROUTING PROTOCOLS IN MANETS

A The routing protocol is a set of rules and conventions that govern the movement of data within the network and choose the path that the data packets should travel through to reach the desired destination. A routing protocol also determines the way the router interacts with other routers. First, the routing protocol podcasts the routing information to the direct neighbors and then this information propagated through the network. Setting up the optimal route (minimum hops) between the source node and the destination node, so that the data packets reach the destination in a well-timed manner with no waste in the network bandwidth and with the least overhead is the main goal of routing protocols in ad-hoc networks [5]. When a node needs to communicate with other nodes to send data over the network, the current status of this node must be podcasted to the neighbors, where the routing information preserved by each node must be updated due to the nature of MANET [6]. Based on the way this information is collected [5][6], and the measures when the sending node seize a path to the destination (routing strategies) [7], the MANET routing protocols can be classified into three main categories:

2.1. TABLE-DRIVEN (PROACTIVE) ROUTING PROTOCOLS

Proactive protocols preserve up-to-date and consistent routing information related to every node that exists inside the network topology even before it is needed [5] [8]. Each node constructs its own routing table and deploys this table to find the optimal route to a specific destination [7]. This node needs to preserve an up-to-date and trustworthy information in its routing table [5] [7], not only routing information related to the adjacent nodes, but also about all the nodes that can be reached, in addition, the number of hops that need to reach another node on the network [6].

Whenever there is a change in the network topology, the entire network must be notified about this change. In this case, each node updates its routing table as much as needed so that the routing table remains reliable and consistent. This is done by each node periodically by podcasting its routing table to the neighbors. So whenever something changes the whole network must be notified [5-7] [9] [21] [22].

The disadvantages of this type of protocols are the expanding of the network size and the growing of the communication overhead.as an advantage, this protocol allows the network state to change immediately whenever a malicious node joins the network topology, so an action can be taken [5] [6] [18] [19] [20]. Some of the existing proactive routing protocols are Destination Sequenced Distance Vector routing (DSDV), Wireless Routing Protocol (WRP), Cluster Gateway Switch Routing protocol (CGSR), Fisheye State Routing (FSR), and Optimized Link State Routing (OLSR).

2.2. ON-DEMAND (REACTIVE) ROUTING PROTOCOLS

On-Demand (Reactive) Routing Protocols also known as source-initiated routing protocols, it starts when a node wants to send a message to another node in the network [5] [6], which means that a route to a destination node will be established just when it is required [5] [6] to scale down the overhead in the network [10]. When a specific node wants to send data to a new destination, the Route Discovery Process starts. this process tries to find a route to the destination [7]; the source node broadcast a route request message (RREQ) to the direct nodes connected to it. After the neighbors receive the message they again broadcast the message to their neighbors, and so on until the message delivered to the destination. The destination, in The node preserves information about the active routes to the other nodes in the network. But the discovery process is done for each new destination. the nodes that are inactive do not participate in such a process. The newly discovered route is presented in the node's routing table until the route is no longer required [5] [7]. The strength in the reactive routing protocols is reduced of bandwidth that was wasted due to the continued broadcasting of routing tables in other MANET proactive routing protocols. the communication overhead is also reduced, on the other hand. delays may occur due to the route discovery operation. where a new discovery process starts for each new destination. This process considers the main reason for attacks done by malicious nodes. some packets may be lost because of the routing techniques used [6]. Examples of existing reactive routing protocols are: Ad-hoc On-demand Distance Vector routing (AODV), Dynamic Source Routing (DSR), and Temporally ordered routing algorithm (TORA). We discuss AODV and DSR in more details.

In AODV, each node preserves information for the next hop in its routing table. The routing path from source to destination node also saved on routing table [5][6]. There are two main phases in AODV routing protocol: the route discovery and the route maintenance phase [7]. The discovery phase begins when a source node wants to send data to a specific destination node that not exist in routing table [7]. which means that the route to that destination is not known [5] [6].

In this operation, the source node broadcasts an RREQ to all of its neighbors. the neighbor nodes do the same when they receive a new RREQ message. Each node keeps a sequence number and a broadcast ID which is incremented each time the node sends an RREQ message. this process repeats until the message reaches the destination. in this case, an RREP unicasts from that destination back to the source node. once the RREP message is received by the source node, a route from the source node to the destination is built. The RREP message could also be unicasted to the source node if an intermediate node has a fresh-enough route to the destination [5-7], Figure 1 shows the propagation of RREQ and RREP message inside the network.

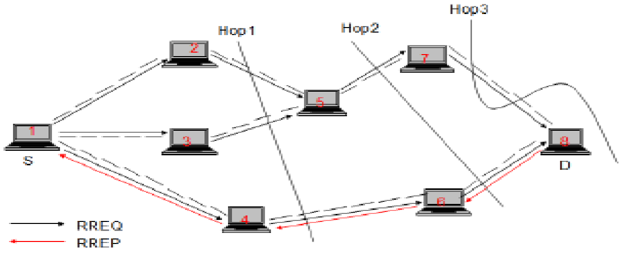


Figure 1 Propagation of Route Request packet & Route Reply packet

The route maintenance phase starts when there is a change in the distribution of the network nodes (topology) or when there is a link broken for a specific routing path between two nodes which means a connection failure[5-7].In this case a route error message (RERR) is propagated inside the network in a reverse direction to reach the source node that is related to that broken route, the intermediate nodes use this message in order to update their routing information, the source node delete the invalid routing information that is related to the broken links from their routing tables[5][11]. Once the RERR message reaches the source node, it starts looking for an alternative route, and if there were no alternative route was found, a new route discovery process starts again [6][7].

Scientists categories this protocol as a pure reactive routing protocol, because the nodes that are not located on a specific path do not preserve routing information related to that path, and do not participate in the swapping of routing tables. the performance of the network decrease as the network grows, with potential overhead caused by RREQ, RREP and RERR messages traveling inside the network during the route discovery process [7].

DSR is a source of routing protocol, which means that the source node decides the full routing path to send the data through it to destination, this is because each node here has a route cache or what it is called known routes, and this the place where each node preserves a routing information about all of the known paths from a source to different destinations [5][6][12], this route cache is altered each time a new route to a destination is known in the network [12]. Unlike AODV where each node preserves information about only the next hop node in their routing tables. Each data packet holds the full path from source to destination in its header [5][6].

the main phases: route discovery and route maintenance. When one node wants to send data packets to a specific destination, it first checks the route cache to see if it knows the destination and to see if there is a route to it. if there is a route information source node sends the data through it. otherwise, it broadcasts a route request packet to the neighbors, and they, in turn, check their route cache to see if there is a route to that destination. if not had the route information the packet is forwarded until the destination is reached. In this case, a route reply message is created. Also, the route reply message is generated if an intermediate node knows a route to a destination [12]. The disadvantage in DSR is that when the mobility of the network nodes increases, the delivery rate and the performance of the network probably decreased [6].

2.3. HYBRID ROUTING PROTOCOLS:

Hybrid Routing Protocols is a kind of routing protocols that combines the features of both proactive and reactive routing protocols in order to defeat the cons of them [6][7]. these routing protocols are designed using a layered framework [5][6]. The nodes of the network are divided into groups, based on the geographical area, and the distance between those nodes [5][7]. The proactive routing technique is used in order to collect the routing information [6] and to establish communication between the nodes that belong to the same zone [5][7]. while the reactive routing technique is used to keep the routing information when the topology of the network is altered [6] and to establish a connection between the nodes that belong to different zones [5][7]. Some of the existing hybrid routing protocols are: Temporally-Ordered Routing Algorithm (TORA), Zone Routing Protocol (ZRP), Zone-based Hierarchical Link State (ZHLS), and Distributed dynamic routing (DDR).

3. BLACK HOLE ATTACK

Black hole refers to an area in the network that drops the traffic headed to a specific destination through it, without informing the source node that the data packets was not delivered to the destination [5]. In the black hole attack, a node exploits the routing protocol to exhibit itself as the node that has the shortest path to reach a specific destination [5][14][15], after that this node receives the data packets, that supposed to be forwarded to the right destination through this node, now the node drops those packets as type of denial of service (DoS) threat [5], consumes the packets [13][14], or exploits its location in the network to advertise itself as the destination node (man-in-the-middle threat) and starts to redirect different packets inside the network [5].

In such a case, the source and the destination cannot communicate with each other. The black hole nodes here are unseen, and the network traffic must be observed to detect such nodes. In Figure 2, node A wants to send data to node F, it broadcasts an RREQ to the nodes B, M, and D, M is a malicious node, replies with an RREP message implying that it has fresh-enough route to the destination [5][13], this RREP arrives at node A before nodes' B and D RREP, node A assumes that the route discovery process has ended, ignoring all the other RREP messages, and starts to send data packets to node M, which in turn drops those packets [5][13][14][22].

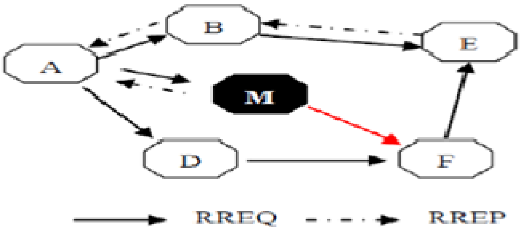


Fig 2: Black hole Attack

The black hole attack can be classified based on the strategy used by the malicious node to perform the attack. the node either drops all the packets that arrive to it which is supposed to be forwarded to the intended destination, or the node chooses some of those packets to drop, which it does not like [5].

The node that plans to attack, must find a way to put itself on the path that control packets or data packets will be delivered through it. relying on some vulnerabilities already exist in the used routing protocol, which was designed on the basis of trustworthiness between the network nodes, every node can do a wrong behavior and sabotage the network operations by destroying the data packets or misuse the control packets [5]. The dropping of packets terminates the communication and transmission between two nodes, what is worse than that is the malicious node preventing the establishing of a route between those nodes [5].

In the AODV routing protocol, the sequence number is used to indicate the freshness of the different network routes. it exists in the message that is received from the source. The more the larger this sequence number is, the fresher the route related to this number is [5] [14]. When the destination replies with a REPP message, it compares the sequence number inside the (RREQ+1) message delivered to it and the destination's current sequence number, picks the larger one and puts it in an RREP message, and then unicasts it back to the source through the shortest path. When the source receives more than one RREP message it chooses the one with the highest sequence number and sends the data through that path [5] [13] [14].

What happens exactly in AODV routing protocol, is that, when one node has no fresh-enough route to a specific destination and wants to send data to it, it broadcasts an RREQ message to all of the neighbors, if these nodes has a fresh-enough route to the destination they reply with an RREP message to the source. In turn, the source uses the RREP message that holds the highest sequence number and drops the rest of them. After that, it starts to send the data. In the case of a multiple RREP messages holding the same sequence number, the source uses the one that holds the smallest hop count and starts to send the data through that shortest path [14]. When a node intends to perform a black hole attack, when a source node broadcasts an RREQ message to nodes, the black hole node replies with an RREP message that holds the highest sequence number, this message is delivered to the source node as if it was from the destination, or from a node that has a fresh-enough route to the intended destination, as a result, the source drops all the other RREP messages, and starts sending the data packets to the black hole node. Trusting that the data will be delivered to the correct destination. So, the black hole node attracts all the data towards it and then discards or consumes them, and they will be never delivered to the destination [13-15].

In order to succeed in the attack, the node must create a route reply message with a sequence number larger than the current sequence number to absorb all the packets and then discards them [5]. Black hole attacks can be classified based on the way of the attack perform [15] into two main types: Simple or Single Black Hole Attack (ordinary)[14][15], and Collaborative Black Hole Attack, in which, two or more nodes collaborate, to manipulate the routing information to hide from the detection mechanisms [14] or to form a team that prevents the data from reaching a specific node, and its much more dangerous than the first type because it is hard to detect and easy to be performed. where one malicious node sends the data to another malicious node that, in turn, swallows the data packets without forwarding those [15].

Black hole attack degrades the network performance, causing a low packet delivery ratio, less throughput, and disturbing the route discovery process [5] [13] [14].

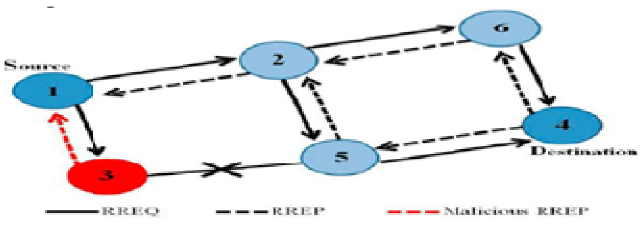


Figure 3 The single black hole problem.

4. PROPOSED DETECTION SCHEMES

In this section, we will discuss some of the black hole detection schemes that were proposed in the last few years

.

4.1. ENHANCED AODV ROUTING PROTOCOL

In 2014, Bani-Yassin et al. [16] proposed an improved AODV routing protocol to detect and avoid the black hole attack in MANETS. They suggested that the RREP message should be monitored along with its history, through the addition of a new field to its structure that contains the address of the last node that has a route to a specific destination. In addition monitoring of the node's behavior in the network by adding two tables inside each node one is called the suspect table and the other is called the blacklist table. The suspect table contains a list of nodes addresses from which they received an RREP messages, and the number of failed RREP messages arrived from each node in the list. The RREP message is considered to be failed when a specific source fails to send data through the path related to this message. Which means that the source did not receive any acknowledgment. While the Blacklist table contains the addresses of nodes that exceeds a certain number of failed RREP messages. Each node that has been moved from suspect list to this list, all the RREP messages arriving from it will be ignored by other nodes in the network. And the last modification is the creation of a 1-bit sized ACK message that is set to 1 if the data arrived at the destination otherwise they are set to 0, and they will be propagated back to the source.

They did a simulation of a MANET network to evaluate the performance of the standard AODV, MI-AODV, and evaluate the proposed AODV with the presence of 1,2 and 6 black hole nodes in the network. The evaluation metrics used are the packet delivery ratio, dropped packets ratio, delay, and network overhead. The packet delivery ratio increased by 50.9% with the presence of 1 black hole node and by 57.8% with the presence of two black hole nodes when using the proposed AODV routing protocol compared to the standard AODV, with many nodes scaling from 15 to 35 nodes. The dropped packets ratio decreased by 61.5% with the presence of 1 black hole node and by 57.8% with the presence of two black hole nodes when using the proposed AODV routing protocol compared to the standard AODV, with a number of nodes scaling from 15 to 35 nodes. But when it comes to the delay times, the proposed AODV achieves the highest delay compared to the standard AODV and MI-AODV and this because of the time is taken to process and deliver the packets through an alternative route after the first route fails to do that, because of the presence of a black hole node. Also, the proposed AODV achieved the lowest overhead compared to the other two protocols.

4.2. TIMER BASED DETECTION MECHANISM

Choudhary and Tharani [17] suggested that each node in the network set a new value to all the neighbor nodes. This value is called the maximum trust value. As we all know, the source node starts sending the data to the first neighbor node that is send the RREP message, according to the proposed method, when the source node (N) sends the data to the neighbor (N+1) that is one hop away, it sets a timer (T) in seconds, and when this timer expires the node (N) starts listening to the medium to see if it has been received the same data it has sent to node (N+1), if node (N) did not hear anything it decreases the trust value related to node (N+1) by 1, and this information is propagated inside the whole network so that the other nodes update the trust information entries related to that node in their tables, and when the trust value of a node becomes less than a predefined min trust value, it will be blacklisted and all the messages and actions coming from this node will be ignored. We should point out that the time (T) is the total packet processing in time.

They used the packet delivery ratio as a measure to evaluate their mechanism, and they have approved that their proposed solution increasing the packet delivery ratio compared to the packet delivery ratio in a black hole infected AODV. Table (2) shows a comparison between the two detection schemes.

Table 2. Comparison between the two detection schemes.

Schemes	**Enhances AODV**	**Time-Based Mechanism**
Routing Protocol	AODV	AODV
Simulator	GloMoSim	EXata-cyber
Year	2014	2015
Evaluation metrics	PDR, DPR, Delay, Overhead	PDR
Strengths	Higher PDR, lower DPR, and overhead	Higher PDR
Weaknesses	Higher delay	More evaluation metrics should have been used

3. CONCLUSION

MANET networks are networks with a dynamic topology that comes with a lot of security and attacks issues. One of the major attacks is the Black Hole Attack that exploits the used routing protocol to harm the normal operations of the network. Every day a new detection and prevention schemes are being proposed by researchers over the world to overcome this problem. By detecting this attack or at least mitigate the negative effect of it, we will help in preserving good and secure networks for exchanging knowledge and experiences around the world.

REFERENCES

[1] Suresh, M., & Shaik, S. (2016). Security Issues in MANETS. International Journal, 4(2).

[2] Ishrat, Z. (2011). Security issues, challenges & solution in MANET. IJCST, 2(4), 108-112.

[3] Priya, S. B., & Theebendra, C. (2016). A STUDY ON SECURITY CHALLENGES IN MOBILE ADHOC NETWORKS.

[4] Garg, A., & Beniwal, V. (2012). A review on security issues of routing protocols in mobile ad-hoc networks. International Journal of Advanced Research in Computer Science and Software Engineering, 2(9).

[5] Ahmed, A., Hanan, A., & Osman, I. (2016). Description of Black Hole Attack Behaviour in MANET. International Journal of Computer Networks and Communications Security, 4(12), 322.

[6] Tseng, F. H., Chou, L. D., & Chao, H. C. (2011). A survey of black hole attacks in wireless mobile ad hoc networks. Human-centric Computing and Information Sciences, 1(1), 4.

[7] Kumar, J., Kulkarni, M., & Gupta, D. (2013). Effect of Black hole Attack on MANET routing protocols. International Journal of Computer Network and Information Security, 5(5), 64.

[8] Jayakumar, G., & Ganapathy, G. (2007). Performance comparison of mobile ad-hoc network routing protocol. International Journal of Computer Science and Network Security (IJCSNS), 7(11), 77-84.

[9] Shrivastava, P., Kumar, S., & Kumar, M. (2014). Study of Mobile Ad hoc Networks. International Journal of Computer Applications, 86(3).

[10] Bai, F., Sadagopan, N., Krishnamachari, B., & Helmy, A. (2004). Modeling path duration distributions in MANETs and their impact on reactive routing protocols. IEEE Journal on Selected Areas in Communications, 22(7), 1357-1373.

[11] Hinds, A., Ngulube, M., Zhu, S., & Al-Aqrabi, H. (2013). A review of routing protocols for mobile ad-hoc networks (manet). International journal of information and education technology, 3(1), 1.

[12] Prakash, S., Kumar, R., Nayak, B., & Yadav, M. K. (2011). A Survey on Reactive Protocols for Mobile Ad Hoc Networks (MANET). In Proceedings of the 5th National Conference (pp. 10-11).

[13] Kakoty, B. S. (2013). Simulation and Analysis of Blackhole Attack in MANETs for Performance Evaluation. International Journal of Latest Trends in Engineering and Technology (IJLTET) Vol, 2.

[14] Bhattercharjee, A., & Paul, S. A Review on some aspects of Black Hole Attack in MANET. network, 1, 2.

[15] Al Dulaimi, L., Ahmad, R. B., Hassnawi, L. A., & Ahmed, I. (2016). Black Hole Malicious Behaviour via Different Detection Methods

[16] BaniYassein, M., Khamayseh, Y., & Nawafleh, B. (2014). Improved AODV Protocol to Detect and Avoid Black Hole Nodes in MANETs. FUTURE COMPUTING, 7-12.

[17] Choudhary, N., & Tharani, L. (2015, January). Preventing black hole attack in AODV using timer-based detection mechanism. In Signal processing and communication engineering systems (SPACES), 2015 international conference on (pp. 1-4). IEEE.

[18] Bader, A., Mardini, W., & Yasein, M. B. (2011). A new protocol for detecting black hole nodes in ad hoc networks. International Journal of Communication Networks and Information Security (IJCNIS), 3(1).

[19] Qasem, M., Altawssi, H., Yassien, M. B., & Al-Dubai, A. (2015, October). Performance evaluation of RPL objective functions. In Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on (pp. 1606-1613). IEEE.

[20] Yassein, M. M. B., Khaoua, M. O., Mackenzie, L. M., & Papanastasiou, S. (2006, September). Performance evaluation of adjusted probabilistic broadcasting in MANETs. In Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on (pp. 245-249). IEEE.

[21] Khamayseh, Y., Al-Salah, R., & Yassein, M. B. (2012). Malicious nodes detection in MANETs: behavioral analysis approach. Journal of networks, 7(1), 116.

[22] Yassein, M. B., Al-Dubai, A., Khaoua, M. O., & Al-Jarrah, O. M. (2009, May). New adaptive counter based broadcast using neighborhood information in manets. In Parallel & Distributed Processing, 2009. IPDPS 2009. IEEE International Symposium on (pp. 1-7). IEEE.

[23] Yassein, M. B., & Aljawarneh, S. (2017). A new elastic trickle timer algorithm for Internet of Things. Journal of Network and Computer Applications, 89, 38-47.

[24] Yassein, M. B., Mardini, W., & Khalil, A. (2016, September). Smart homes automation using Z-wave protocol. In Engineering & MIS (ICEMIS), International Conference on (pp. 1-6). IEEE.

[25] Charalambous, M. C., Mavromoustakis, C. X., & Yassein, M. B. (2012, June). A resource intensive traffic-aware scheme for cluster-based energy conservation in wireless devices. In High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 2012 IEEE 14th International Conference on (pp. 879-884). IEEE.

[26] Yassein, M. B., & Hijazi, N. (2010, July). Improvement on cluster based routing protocol by using vice cluster head. In Next Generation Mobile Applications, Services and Technologies (NGMAST), 2010 Fourth International Conference on (pp. 137-141). IEEE.

[27] Yassein, M. M. B., Khaoua, M. O., Mackenzie, L. M., & Papanastasiou, S. (2006, September). Performance evaluation of adjusted probabilistic broadcasting in MANETs. In Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on (pp. 245-249). IEEE.

INTENTIONAL BLANK

SECURITY PROTOCOL FOR POLLUTION ATTACK USING NETWORK CODING

Kiattikul Sooksomsatarn

Department of Computer Science,
School of Information and Communication Technology, University of Phayao,
Maeka, Muang, Phayao 56000, Thailand

ABSTRACT

Network coding is a technique for maximizing the use of available bandwidth capacity. We are interested in applying network coding to multimedia content distribution. This is desirable because many popular network applications for content distribution consume high bandwidth and international bandwidth; both are scarce in countries such as New Zealand. Existing work has addressed the use of network coding for content distribution, however work on network coding and security does not consider the trade-off between quality of service and security for multimedia. Network coding is vulnerable to a pollution attack or a packet modification attack. It has detrimental effect particularly on network coding because of specific characteristic of network coding that allows nodes to modify received packets at any time. Many pollution attack defence mechanisms use computationally expensive techniques leading to higher communication cost. Therefore, the focus of this work is on developing protocols to address both open problems and validate the protocols using a combination of formal and simulation techniques. More importantly, our novel contribution is reduction of complexity of algorithms appropriate for streaming content distribution with network coding.

KEYWORDS

Network Coding, Pollution Attack Detection, Security Protocol

1. INTRODUCTION

Previous work using homomorphic Message Authentication Codes (homomorphic MACs) to detect corrupted packets, such as, the work by Agrawal and Boneh [1] and Li et al. [2], leverages the observation that if a packet does not belong to the source space, then it is a corrupted packet. The detection works by firstly establishing shared secret keys between the source and the intermediate nodes. Then, using these secret keys, the source node can sign the fixed source space and the intermediate nodes can verify if their received packets belong to the source space. However, the fixed source space can cause another attack called tag-pollution attack since an attacker tries to produce a new valid tag from the fixed source space he/she has received.

In cooperative SpaceMac's detection scheme [3], Le and Markopoulou leverage the observation that a packet sent by an intermediate node must belong to the space spanned by all packets that it received from its parents. For example, consider a subset of nodes in a network shown in Figure 1. A packet sent by *C* must belong to the space spanned by the packets it received from its

Dhinaharan Nagamalai et al. (Eds) : CSEIT, NCS, SPM, NeTCoM - 2018
pp. 209–221, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81816

parents: *A* and *B*; otherwise, *C* must be polluting the network. Formally, at any moment *t* in the multi-cast session, if an intermediate node *N* sends out a vector *y* then $y \in \Pi N\ (t)$; otherwise, *y* is corrupted.

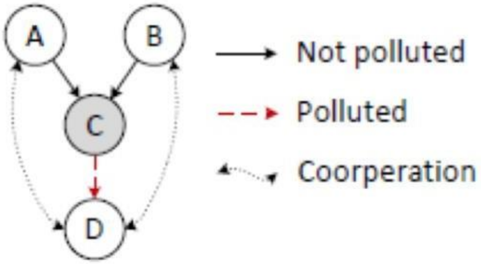


Fig. 1. Pollution Attack Detection in SpaceMac[3] (Note that "coorperation" should be "cooperation")

Figure 1 illustrates how SpaceMac helps to detect pollution attacks. Using SpaceMac, *A* and *B* are able to sign the expanding space ΠC (the received space of *C*) and *D* is able to verify any packet sent by C to see if it belongs to ΠC. If there is a packet sent by C that is not in ΠC, the attack is detected by *D*. The cooperation among *A*, *B*, and *D* helps to detect the attack from *C*. Our detection scheme uses loose synchronization by firstly establishing Kerberos ticket only shared between the source and the TCC for preventing tag-pollution and replay attack. Then, using pull-based algorithm, a downstream node can make a tag request. The downstream node must have the valid tag (*SourceSpace*) generated by the source from the original ticket to have an access for content distribution. A destination node or another downstream node do not need to interact with the source anymore if its parent has the valid tag since the parent can generate the new valid tag (*Sub-Space*). There are numbers of TCCs as replicas throughout the network. The upstream nodes can interact with the closest TCC as many times as required further down to the destination taking the role of the source to generate a new tag.

2. DEFINITIONS

2.1. Packet Identity

Size of content for distributing is definitely different. The content needs to be divided to smaller size called a *packet*. All the packets are the same in size for ease of content distribution using network coding. To establish authentication tag of packets, the packets need to be uniquely identified. The requirement of identifying packets is complicated by the fact that packets could be modified, either maliciously or as a requirement of functionality. Ordinary hash functions are no longer applicable when network coding is applied. A hash value is not robust under modifications of the packet it identifies. Any change to the packet will result in a new identity. A homomorphic hash is a function that can compute the hash of a combined packet from the hashes of the individual packets. With this construction, we can dis- tribute a list of individual hashes to nodes, and they can use those to verify incoming packets once they arrive. Homomorphic Hashing is described in the paper On- the-fly verification of rate less erasure codes for efficient content distribution by Krohn et al. [4] Therefore, we define a homomorphic hash value as a basic form of identification where homomorphic hash function *HH* is applied to the packet p to produce the identity of the packet $id_p = HH(p)$

2.2. Kerberos Ticket

Kerberos is a computer network authentication protocol which works based on tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Kerberos protocol messages are protected against eavesdropping and replay attacks. Kerberos builds on symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography during certain phases of authentication. In our protocol, to establish loose synchronization, the source creates and signs a ticket for the packet being sent out. This ticket contains information to identify the packet, as well as any extra terms of the ticket such as duration of the ticket. As the pollution attack detection protocol sends ticket information separately from the packets themselves, there is no need to embed the ticket information in the packets.

2.3. Structure Of Authentication Tag

In the pollution attack detection protocol, tags are used to represent authentication of origin and are passed from the source to the destination via intermediate nodes. A tag is defined as a tuple:

$$tag = \{A = T_{p,D}^{(n)}, B = pk_D^{(n)}\}_{sk_{TCC}}$$

The parameters of the tag are:

- $A = T_{p,D}^{(n)} = \{id_p = HH(p), Ticket_p\}_{sk_p}$: The one-time ticket signed with the secret key for the packet sk_p. This ticket contains information such as the identity of the packet $id_p = HH(p)$ and the original Ticket for the packet generated beforehand Ticket_p.

- $B = pk_D^{(n)}$: The one-time public key created by the downstream node *D* using nonce *n*.

- The parameters (*A and B*) are signed with the secret key of the TCC.

The pollution attack detection protocol uses an encryption scheme. The TCC signs tags and the public signing key of the TCC has to be well-known to verify the signed tags. The public encryption key of the TCC is also well-known so that the source can encrypt messages to send to the TCC. Before the protocol is run for the first time, the TCC generates and publishes its public encryption and signing keys. The notation A_{skB} denotes the message *A* signed using the key sk_B and A_{pkB} denotes the message *A* encrypted using the key pk_B.

2.4. Encryption Scheme

The pollution attack detection protocol requires an encryption scheme that provides indistinguishability under Chosen Plaintext Attacks (IND-CPA), which is a security definition for private- or public-key encryption schemes. At a high level, IND-CPA security means that no adversary can distinguish between different messages, even when allowed to make encryptions and decryptions of its choice.

A cryptosystem is indistinguishable under chosen plaintext attack if every probabilistic polynomial time adversary has only a negligible advantage over random guessing with probability $\left(\frac{1}{2}\right) + \epsilon(k)$, where is $\epsilon(k)$ a negligible function in the security parameter *k*.

The two most commonly used encryption schemes are the RSA encryption scheme and the El-Gamal encryption scheme. Nonetheless, both encryption schemes are not well applicable to our protocol because of stream ciphered homomorphism. Therefore, Goldwasser-Micali cyyptosystem scheme is used in our protocol.

Goldwasser-Micali (GM) cryptosystem is an asymmetric key encryption algorithm developed by Shafi Goldwasser and Silvio Micali in 1982 [5]. The GM encryption scheme is semantically secure if any probabilistic, polynomial-time algorithm (PPTA) that is given the ciphertext of a certain message m and the message's length, cannot determine any partial information on the message with probability non-negligibly higher than all other PPTA's that only have access to the message length.

Two years later, Goldwasser and Micali subsequently demonstrated that semantic security is equivalent to another definition of security called ciphertext indistinguishability under chosen-plaintext attack [6].

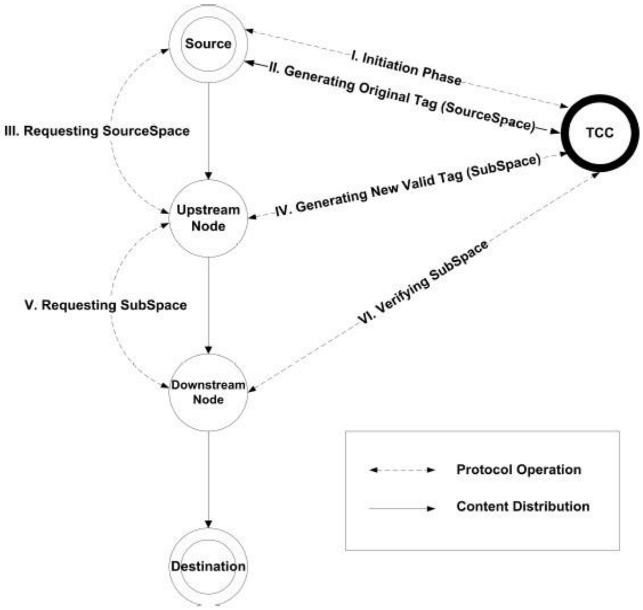


Fig. 2. Main phases of protocol for Pollution Attack Detection

3. OVERVIEW OF THE PROTOCOL FOR POLLUTION ATTACK DETECTION (PAD)

The main phases of the pollution attack detection protocol include:

3.1. Initiation Phase

The *Source* initiates dividing the content into chunks called packets and assigning their identity, cooperates with the *TCC*, creates initial secret/public keys for the packets. The *TCC* creates *Kerberos Ticket* from received information by using a trap-door function.

3.2. Sourcespace Phase

This phase includes two mechanisms:

3.2.1. Generating Original Tag (SourceSpace)

Using the Ticket for that packet, the Source generates a one-time ticket for the requesting node and the requested packet beforehand. The one-time ticket is then signed by the secret key only shared between the Source and the *TCC*. The *TCC* creates and sign a authentication tag called SourceSpace.

3.2.2. Requesting SourceSpace

The Upstream Node makes a request of original tag generated from the Source for downloading a desire packet. The Source sends the tag to the requesting node with the packet that the node desires**.**

3.3. Subspace Phase

This phase includes three mechanisms:

3.3.1. Generating New Valid Tag (SubSpace)

The Upstream Node takes the role of the Source creating a propagated new valid tag called SubSpace. If a Downstream Node wishes to redistribute the packet that they have received from the Upstream Node, they can take the role of the Upstream Node and send it to another Downstream Node(s).

3.3.2. Requesting SubSpace

This is like Requesting SourceSpace, but the Downstream Node no longer needs to interact with Source because the Upstream Node can also generate the valid tag. However, tag verification is needed in next method**.**

3.3.3. Verifying SubSpace

This provides a method for the Downstream Node to check whether the tag of the packet they received is valid.

4. DETAILED PROTOCOL FOR PAD

This section identifies the protocol for Pollution Attack Detection in more detail. The protocol consists of three phases: Initiation phase, SourceSpace phase, and SubSpace phase.

4.1. Initiation Phase

This section presents the initiation phase of the pollution attack detection protocol.

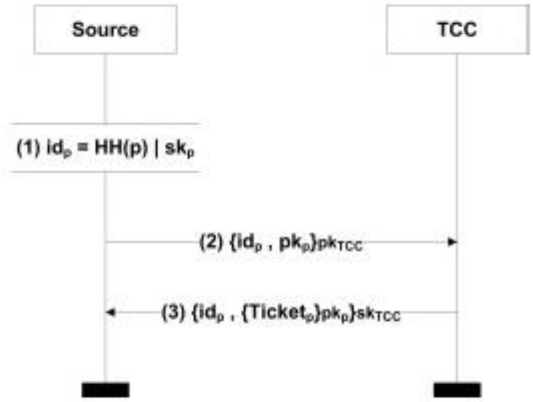

Source
TCC
(1) $id_p = HH(p) | sk_p$
(2) $\{id_p , pk_p\}pk_{TCC}$
(3) $\{id_p , \{Ticket_p\}pk_p\}sk_{TCC}$

Fig. 3. Handshake between Source and TCC

Figure 3 shows a handshake between Source and TCC for sharing public information of packets. A protocol for content distribution using network coding is defined by a set of five probabilistic, polynomial-time, multi-party algorithms: SetupKey, LooseSync, GenLicense, RegenLicense and VerifyLicense.

4.1.1. SetupKey(k)

A probabilistic polynomial time (PPT) algorithm that sets up keys and global parameters necessary for the protocol with security parameter *k*.

4.1.2. LooseSync(packet, pk_{packet})

A polynomial time algorithm where the source assigns to packet with some public information pk_{packet} where only the source knows the corresponding private information sk_{packet}. Returns 1 or 0 to indicate success or failure of the assignment.

4.1.3. GenLicense(packet, data, sk_{packet})

A PPT algorithm which returns license for packet. The algorithm generates the license using the secret information for the packet sk_{packet} and content.

4.1.4. RegenLicense(packet, $license_{old}$, $content_{old}$, $content_{new}$)

A PPT algorithm which returns $license_{new}$ for packet. The algorithm generates $license_{new}$ using content$_{new}$ as well as license$_{old}$ and content$_{old}$ from an existing license for packet.

4.1.5. VerifyLicense(packet, content, license)

A polynomial time algorithm that verifies the correctness of license for packet and content and returns 1 or 0.

The use of the GenLicense and RegenLicense algorithms will result in a set of tags license$_1$, ..., license$_n$ with corresponding content values content$_1$, ..., content$_n$. The following formula express the correctness property:

$$VerifyTag(packet, content_i, license_i) = 1$$

Where license$_1$ = GenLicense(packet, content$_1$, sk$_{packet}$) and license$_i$ = RegenLicense(packet, licensei$_1$, content$_{i1}$, content$_i$)

4.2. Sourcespace Phase

To initially generate a tag, a protocol takes place between the intermediate (downstream) node, the source, and the TCC. The generation of a new tag for a packet by the source takes place in the seven steps shown in Figure 4.

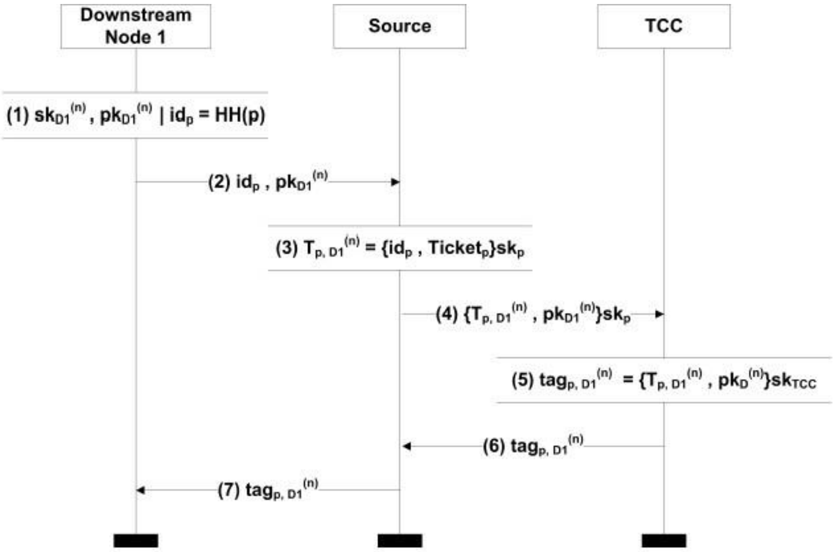

Downstream Node 1
Source
TCC
(1) $sk_{D1}^{(n)}$, $pk_{D1}^{(n)}$ | id_p = HH(p)
(2) id_p , $pk_{D1}^{(n)}$
(3) $T_{p, D1}^{(n)}$ = {id_p , $Ticket_p$}sk_p
(4) {$T_{p, D1}^{(n)}$, $pk_{D1}^{(n)}$}sk_p
(5) $tag_{p, D1}^{(n)}$ = {$T_{p, D1}^{(n)}$, $pk_D^{(n)}$}sk_{TCC}
(6) $tag_{p, D1}^{(n)}$
(7) $tag_{p, D1}^{(n)}$

Fig. 4. Source Generating Tag with TCC

4.3. Subspace Phase

Now the one-time tag for a packet has been generated, signed, and sent to the downstream node, the downstream node can take the role of the source using this tag to generate a new tag for a destination or another downstream node without interacting with the source. The generation of a new tag by the upstream node takes place in the seven steps shown in Figure 5.

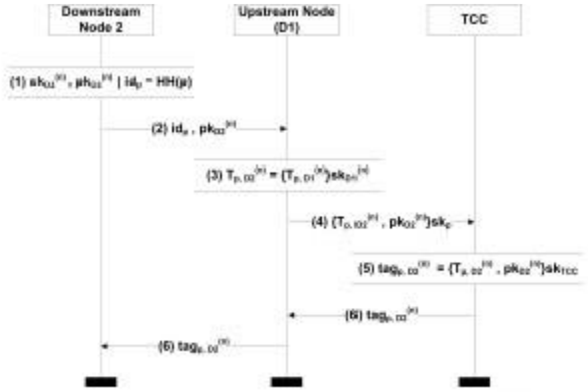

Downstream Node 2
Upstream Node (D1)
TCC
(1) sk_D2^(x), pk_D2^(x) | id_p = HH(p)
(2) id_p, pk_D2^(x)
(3) T_p,D2^(x) = (T_p,D1^(x))sk_D1^(x)
(4) (T_p,D2^(x), pk_D2^(x))sk_p
(5) tag_p,D2^(x) = (T_p,D2^(x), pk_D2^(x))sk_TCC
(6) tag_p,D2^(x)
(6) tag_p,D2^(x)

Fig. 5. Upstream Node Generating One-time Tag with TCC for Destination or Another Downstream Node On-the-fly

On-the-fly tag generation has the trade-off between computational/network overheads and security. In content distribution using network coding, homomorphic cryptography is applied to verify Message Authentication Code (MAC) tags without decrypting incoming signed, combined packets.

5. SECURITY ANALYSES

This section demonstrates two formal security analyses of the protocol for PAD. Firstly, a reduction to contradiction style of argument is used to show the PAD protocol provides security against modification, fabrication, collusion, and spoofing attacks. Secondly, a formal technique to analyse our security protocol, Communicating Sequential Processing (CSP), is used to formalise our protocol running on Failures-Divergence Refinement (FDR) model checker to show the protocol also provides security against authentication attack.

5.1. Security Proof By Contradiction

Theorem 1. *The protocol for pollution attack detection provides Secure Content Distribution using Network Coding [7] in the random oracle model provided that the signature scheme used has provable security against existential forgeries under adaptive chosen message attacks and the encryption scheme used has provable security against IND-CCA2 attacks.*

We use a reduction to contradiction style of argument to show the tagged transaction protocol provides security against spoofing, fabrication, network sniffing, and cloning attacks. then make arguments showing the security of the tagged transaction protocol against identity revelation and linkability attacks. In this security analysis, the TGC is assumed to be acting as a trusted third party. Chapter 6 removes this assumption and discusses methods to verify the actions of the TGC. For the security analysis of the identity revelation and linkability properties the following assumptions are made: a perfect anonymous communication channel, an anonymous supplier, and the parties in the protocol not revealing their identities or the identities of the parties with whom they communicate. This security analysis does not consider side channel attacks.

5.2. Formal Security Modelling Analysis

5.2.1. Modelling the Honest Agents

We now describe how we can model the honest agents running the protocol as CSP processes. We give a parameterised process *Initiator (A, kA)* to represent an agent a running the protocol as initiator and using session key *kA*. The process starts by receiving a message m from the environment, telling it with whom to run the protocol. It then sends an appropriate message 1 *m1* and receives back an appropriate message 2 *m2* containing an arbitrary value for nonce of responder *nB*.

$$
\begin{array}{l}
Initiator(A, k_A) = \\
\mathop{\square}\limits_{\substack{B \in Agent \\ k_{AB} \in Key \\ n_B \in Nonce \\ m \in Message}}
\left(\begin{array}{l}
env.A.(Env0, B) \rightarrow \\
send.A.B.A.n_A \rightarrow \\
receive.T.A.\{B.k_{AB}.n_A.n_B\}_{k_{AT}}.m1 \rightarrow \\
send.A.B.m2.\{n_B\}_{k_{AB}} \rightarrow \\
Session(A, B, k_{AB}, n_A, n_B)
\end{array}\right)
\end{array}
$$

The definition of the responder is similar: the process Responder (B, n_B) represents agent B running the protocol as responder using nonce n_B. The responder starts by receiving a message 1 m1, from an arbitrary agent a and containing an arbitrary session key k. It then sends back the corresponding message 2 m2.

$$
\begin{array}{l}
Responder(B, n_B) = \\
\mathop{\square}\limits_{\substack{k_{AB} \in Key \\ A \in Agent \\ n_A \in Nonce}}
\left(\begin{array}{l}
receive.A.B.n_A \rightarrow \\
send.B.T\{B.k_{AB}.n_A.n_B\}_{k_{AT}}.m1 \rightarrow \\
send.A.B.m2.\{n_B\}_{k_{AB}} \rightarrow \\
Session(A, B, k_{AB}, n_A, n_B)
\end{array}\right)
\end{array}
$$

As noted above, we consider a small system, comprising Alice acting as initiator, using key kA, and Bob acting as responder, using nonce nB. The two agents do not communicate directly: we arrange below for all communications to go via the attacker. We model this as an interleaving.

$$System_0 = Initiator(Alice, k_A)|||Responder(Bob, n_B).$$

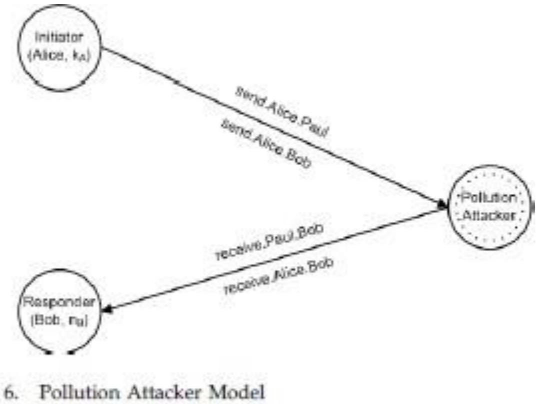


Fig. 6. Pollution Attacker Model

Of course, it is straightforward to consider larger systems, with more agents, or with particular agents running the protocol multiple times, perhaps with different roles.

5.2.2. Modeling the Attacker

We now describe how we can model the attacker. The main issue is modeling which messages the attacker can understand and to create. We need to keep track, therefore, of which submessages of protocol messages the attacker knows; we term these Facts:

$$\begin{aligned} Facts = & \{\{pk_B\}_{\{sk_A\}_k} \mid k \in SessionKey, A, B \in Agent\} \cup \\ & \{\{k\}_n \mid k \in SessionKey, n \in Nonce\} \cup \\ & \{\{sk_A\}_k \mid k \in SessionKey, A \in Agent\} \cup \\ & Agent \cup Nonce \cup SessionKey \cup \\ & SecretKey \cup PublicKey. \end{aligned}$$

If the Attacker knows a fact f and a key *k* then he can encrypt *f* with *k*; if he knows an encrypted message and the corresponding decryption key, he can perform the decryption to obtain the body; if he knows a collection of facts, he can concatenate them together; if he knows a concatenation, he can split it up into the individual components.

5.2.3. Requesting SourceSpace

The Upstream Node makes a request of original tag generated from the Source for downloading a desire packet.

5.3. Security Analysis

Showing that the pollution attacks detection protocol provides secure network coding consists of showing proofs by contradiction to show security against colluding, packet sniffing, spoofing, and fabrication attacks. If there exists an attacker that can break the security properties of the pollution attacks detection protocol, then this attacker can be used to solve a problem thought to be hard.

In CSP model, we describe the basic technique of CSP model checking of security protocols. We consider a small system running the protocol and conclude a single initiator Alice, who will use the session key *Ka*, and a single responder Bob, who will use the secret *Sb*. We also include a pollution attacker, Paul, who has complete control over the network.

We now consider authentication of the responder to the initiator, and vice versa. More precisely, we consider the following questions:

1) If an initiator *A* completes a run of the protocol, apparently with *A*, then has *A* been running the protocol, apparently with *A*, and do they agree upon the value of the nonce *n* and the session key *k*?

2) If a responder *B* completes a run of the protocol, apparently with *A*, then has *A* been running the protocol, apparently with *A*, and do they agree upon the value of the session key *k*? (Note that *A* can receive no guarantee that he and *A* agree upon *n*, because he cannot be sure that *A* even receives message 2.)

We describe how to test for the authentication property. We introduce new events, as follows:

- The event *Running.InitiatorRole.A.B.k* indicates that *A* thinks that she is running the protocol as initiator, apparently with *B*, using session key *k*.

- The event *Complete.ResponderRole.B.A.k* indicates that *B* thinks he has completed a run of the protocol as responder, apparently with *A*, using session key *k*.

We will then check that whenever the latter event occurs, the former event has previously occurred. We arrange for initiator *A* to perform the Running event when she sends message 1, and we arrange for responder *B* to perform the Complete event when he sends message 2; we hide all other events.

$$\begin{aligned}
&AuthSystem_0 = \\
&\qquad System[Running.InitiatorRole.A.B.k/ \\
&\qquad send.A.B.(m1, \{pk_B b\}_{(sk_A)_k}), \\
&\qquad Complete.ResponderRole.B.A.k/ \\
&\qquad send.B.A.(m2, \{k\}n) \\
&\qquad A, B \in Agent, k \in SessionKey, n \in Nonce] \\
&\qquad (\Sigma - alphaAuthSystem),
\end{aligned}$$

$$\begin{aligned}
&alphaAuthSystem = \\
&\qquad \{Running.InitiatorRole.A.B, \\
&\qquad Complete.ResponderRole.B.A \\
&\qquad A, B \in Honest.
\end{aligned}$$

More generally, the Complete event is performed at the last step in the protocol taken by that agent, and the Running event is performed when the agent sends a message that should be causally linked to the other agent receiving a message. Recall that we want to check that whenever a responder A performs a Complete event concerning initiator A, then a has previously performed a corresponding Running event concerning B. We therefore consider the following specification process, which allows only such traces

$$\begin{aligned}
&AuthSpec = \\
&\qquad Running.InitiatorRole?A.B.k \rightarrow \\
&\qquad Chaos(\{Complete.ResponderRole.B.A.k\}).
\end{aligned}$$

Note that this specification allows B to perform an arbitrary number of Complete events corresponding to a single Running event, and so does not insist that there is a one-one relationship between the runs of A and the runs of B. We could test for such a relationship by replacing the Chaos(Complete.ResponderRole.B.A.k) by Complete.ResponderRole.B.A.k → STOP. We can use FDR to test the renement

$$AuthSpec \sqsubseteq_T AuthSystem.$$

(The above renement test is appropriate since *AuthSystem* performs at most a single *Running* event; for a system that could perform *N* such events, we would replace the left-hand side of the renement test by an interleaving of N copies of *AuthSpec*.) FDR nds that this renement does not hold, and returns the following witness trace:

$$< Complete.ResponderRole.Bob.Alice.k_A >$$

Bob thinks he has completed a run of the protocol with Alice, but Alice did not think that she was running the protocol with Bob. We can again use the FDR debugger to nd the corresponding trace of System:

$$\begin{aligned}
&< env.Alice.(Env0, Paul) \\
&\qquad send.Alice.Paul. \\
&\qquad (m1, \{pk_P\}_{\{sk_A\}_{k_A}}) \\
&\qquad receive.Alice.Bob.(m1, \{pk_B\}_{\{sk_A\}_{k_A}}) \\
&\qquad send.Bob.Alice.(m2, \{k_{A1}\}_{n_B}) > .
\end{aligned}$$

We can test whether the responder is authenticated to the initiator (item 1 above) in a similar way. FDR nds no attack in this case. It is interesting to consider what guarantees the responder does receive from the protocol. We claim that if responder B completes a run of the protocol, apparently with A, then A has been running the protocol, and that they agree upon the value of the session key k. Note though that A might have been running the protocol with some agent C other than B, and so performed a Running.InitiatorRole.Alice.C.k event. We can test this condition using the renement check

$$AlivenessSpec \sqsubseteq_T SystemAliveness,$$

, where

$$\begin{aligned}
AlivenessSpec = {} & \\
& Running.InitiatorRole.Alice?C?k \rightarrow \\
& Chaos(\{Complete.ResponderRole.B.Alice.k \\
& |B \in Agent\}), \\
SystemAliveness = {} & \\
& AuthSystem_0 \backslash (\Sigma - alphaSystemAliveness), \\
alphaSystemAliveness = {} & \\
& \{Running.InitiatorRole.A.B, \\
& Complete.ResponderRole.B.A \\
& |A \in Honest, B \in Agent\}.
\end{aligned}$$

6. CONCLUSIONS

Using a proof by contradiction we have shown that the pollution attacks detection protocol provides protection against colluding, packet sniffing, spoofing, and fabrication attacks in the random oracle model. Further security analysis has shown that the pollution attacks detection protocol also provides protection against pollution attacks as we test authentication property of the responder to the initiator for, and vice versa. We claim that if the initiator A completes a run of the protocol, apparently with B, then B has been running the protocol, and they do agree upon the value of the session key k. Therefore, FDR finds no authentication attacks in this case.

REFERENCES

[1] S. Agrawal and D. Boneh, (2009) "Homomorphic macs: Macbased integrity for network coding," in Proceedings of the 7th International Conference on Applied Cryptography and Network Security, ser. ACNS '09. Berlin, Heidelberg: Springer-Verlag, pp. 292–305.

[2] Y. Li, H. Yao, M. Chen, S. Jaggi, and A. Rosen, (2010) "Ripple authentication for network coding," in INFOCOM, 2010 Proceedings IEEE, pp. 1–9.

[3] A. Le and A. Markopoulou, (2012) "Cooperative defense against pollution attacks in network coding using spacemac," Selected Areas in Communications, IEEE Journal on, vol. 30, no. 2, pp. 442–449.

[4] M. Krohn, M. Freedman, and D. Mazieres, (2004) "On-the-fly verification of rateless erasure codes for efficient content distribution," in Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on, pp. 226–240.

[5] S. Goldwasser and S. Micali, (1982) "Probabilistic encryption and how to play mental poker keeping secret all partial information," in Proc. 14th Symposium on Theory of Computing, p. 365377.

[6] S. Goldwasser and S. Micali , (1984) "Probabilistic encryption," Journal of Computer and System Sciences, vol. 28, no. 2, p. 270299.

[7] K. Sooksomsatarn, I. Welch, and W. Seah, (2010) "Secure content distribution using network coding," in Proc. 8th New Zealand Computer Science Research Student Conference.