

Natarajan Meghanathan
Dhinaharan Nagamalai (Eds)

Computer Science & Information Technology

9th International Conference on Networks & Communications
(NeTCoM - 2017) November 25 ~ 26, 2017, Dubai, UAE



AIRCC Publishing Corporation

Volume Editors

Natarajan Meghanathan,
Jackson State University, USA
E-mail: nmeghanathan@jsums.edu

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

ISSN: 2231 - 5403
ISBN: 978-1-921987-75-5
DOI : 10.5121/csit.2017.71501 - 10.5121/csit.2017.71509

This work is subject to copyright. All rights are reserved, whether whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the International Copyright Law and permission for use must always be obtained from Academy & Industry Research Collaboration Center. Violations are liable to prosecution under the International Copyright Law.

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

Preface

The 9th International Conference on Networks & Communications (NeTCoM - 2017) was held in Dubai, UAE, during November 25~26, 2017. The 4th International Conference on Computer Science, Engineering and Information Technology (CSEIT-2017), The 9th International Conference on Applications of Graph Theory in Wireless Ad hoc Networks and Sensor Networks (GRAPH-HOC - 2017), The 9th International Conference on Network and Communications Security (NCS 2017) and The 3rd International Conference on Signal Processing and Pattern Recognition (SIPR 2017) was collocated with The 9th International Conference on Networks & Communications (NeTCoM - 2017). 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 NeTCoM-2017, CSEIT-2017, GRAPH-HOC-2017, NCS-2017, SIPR-2017 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, NeTCoM-2017, CSEIT-2017, GRAPH-HOC-2017, NCS-2017, SIPR-2017 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 NeTCoM-2017, CSEIT-2017, GRAPH-HOC-2017, NCS-2017, SIPR-2017.

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.

Natarajan Meghanathan
Dhinaharan Nagamalai

Organization

General Chair

David C. Wyld
Jan Zizka

Southeastern Louisiana University, USA
Mendel University in Brno, Czech Republic

Program Committee Members

Abrar Abdelhaq
Addi AIT-MLOUK
Adnan Rawashdeh
Ahmed H. Salem
Ahmed J. Jameel
Ali Salem
Ammar Al-Masri
Asmaa Shaker Ashoor
Ayman EL-SAYED
Azeddine Chikh
Babar Shah
Boukenadil Bahidja
Dabin Ding
Daniel Gomes
Dimitris Kontoudis
Emad Al-Shawakfa
Emad Eldin Mohamed
Eyad Al-Zobaydi
Fatma Outay
Ghassan Qas marrogy
Goreti Marreiros
Hamid Alasadi
Hamzeh Khalili
Hari Krishna Garg
Jamal El Abbadi
Joberto S. B. Martins
John Tass
Jose Raniery
Jun Zhang
Kirtikumar Patel
Laya Ebrahimi
Lei ZHANG
Limiao Deng
Liyakathunisa Syed
Lygpapers
Mahdi Salarian
Maryam Hajakbari

Yarmouk University, Jordan
Cadi Ayyad university, Morocco
Yarmouk University, Jordan
Old Dominion University, USA
Ahlia University, Bahrain
University of Sfax, Tunisia
Albalqa Applied University, Jordan
Babylon University, Iraq
Menoufia University, Egypt
University of Tlemcen, Algeria
Zayed University, UAE
University of Tlemcen, Algeria
University of Central Missouri, United States
Estacio de Sa, Brasil
University of Macedonia, Greece
Yarmouk University, Jordan
Canadian University Dubai, UAE
Al-Isra University, Jordan
Zayed University DXB, UAE
Cihan University, Iraq
Polytechnic of Porto, Portugal
Basra University, Iraq
Universitat Politècnica de Catalunya (UPC), Spain
National University of Singapore, Singapore
Mohammadia V University Rabat, Morocco
Salvador University, Argentina
University of Patras, Greece
University of Sao Paulo, Brazil
South China University of Technology, China
Chemic Engineers Inc, United States
Islamic Azad university, Iran
University of Surrey, UK
China University of Petroleum, China
Prince Sultan University, Saudi Arabia
Sichuan University, China
University of Illinois, USA
Islamic Azad University, Iran

Masoumeh Javanbakht	Hakim Sabzevari University,Iran
Maysam Toghraee	Yasouj Science and Research Branch, Islamic
Mike Turi	California State University-Fullerton, USA
Mohamad Badra	Zayed University, Dubai, UAE
Mohamed Tounsi	Prince Sultan University,Saudi Arabia
Mohamedmaher Benismail	King saud University, Saudi Arabia
Mohammad alsarem	Taibah University, KSA
Mohammad Ashraf OTTOM	Yarmouk University,Jordan
Mohammad Hamdan	Heriot Watt University, UAE
Mohammad Qataw	University of Jordan, Jordan
Mohammad Rawashdeh	University of Central Missouri, United States
Mohammad Zarour	Prince Sultan University, Kingdom of Saudi Arabia
Mohammed Al-Sarem	Taibah University, KSA
Mohammed Ghazi Al-Zamel	Yarmouk University, Jordan
Mohammed Nabil El Korso	Paris Nanterre University, France
Mohanned Akour	Yarmouk University, Jordan
Mourchid mohammed Ibn	Tofail University Kenitra, Morocco
Mudassir Khan	King Khalid University, Saudi Arabia
Nadjia Benblidia	Saad Dahlab University, Algeria
Nahlah M. Ameen Shatnawi	Yarmouk University, Jordan
Nayeem Ahmad Khan	University Malaysia Sarawak, Malaysia
Neda Darvish	Islamic Azad University, Iran
Nicolas H. Younan	Mississippi State University, USA
Nizar	University of Carthage, Tunisia
Noura Taleb	Badji Mokhtar University, Algeria
Orhan Dagdeviren	Ege University, Turkey
Ouafa Mah	Ouargla University, Algeria
Paulo Roberto Martins de Andrade	University de Regina, Canada
Philomina Simon	University of Kerala, India
Prakash Duraisamy	University of Central Missouri, United States
Quang Hung Do	University of Transport Technology, Vietnam
Rahil Hosseini	Islamic Azad University, Iran
Ramgopal Kashyap	Sagar Group of Institutions,India
Rana Rahim	Lebanese University, Lebanon
Riccardo Pecori	eCampus University, Italy
Roberto Paiano	University of Salento, Italy
Sahar Idwan	American University of ras al Khaimah,UAE
Salem Hasnaoui	National Engineering School of Tunisi, Tunisia
Shuai Zhao	MediaTek USA Inc,USA
Veton Kepuska	Florida Institute of Technology, USA
Victor Banos	Technical University of Catalonia, Spain
Wail Mardini	Jordan University of Science and Technology, Jordan
Xuling Wei	Qingdao University of Science & Technology, China
Yao-Nan Lien	Asia University, Taiwan
Yenke Blaise Omer	University Institute of Technology, Cameroon
Yuan Zhuang	Bluvision Inc, USA
Yue Cao	Northumbria University, UK
Zeyu Sun	Luoyang Institute of Science and Technology, China
Zsolt Polgar	Technical University of Cluj Napoca, Romania

Technically Sponsored by

Computer Science & Information Technology Community (CSITC)



Networks & Communications Community (NCC)



Digital Signal & Image Processing Community (DSIPC)



Organized By



Academy & Industry Research Collaboration Center (AIRCC)

TABLE OF CONTENTS

9th International Conference on Networks & Communications (NeTCoM - 2017)

Internet of Things in Industry 4.0 Case Study : Fluid Distribution Monitoring System	01 - 11
<i>Maroua Abdelhafidh, Mohamed Fourati, Lamia Chaari Fourati and Abdessalam Chouaya</i>	
Towards a Community Based Mobile Nearby Assistance Solution : Framework and First Prototype	13 - 24
<i>Amine Boulemtafes, Dalila Hamidouche, Chayma Zatout, Chafika Benzaid and Nadjib Badache</i>	
Detection and Prevention of Black Hole Attack in VANET Using Secured AODV Routing Protocol	25 - 36
<i>Salim Lachdhaf, Mohammed Mazouzi and Mohamed Abid</i>	
Cognitive Radio and Radio Frequency Identification Technologies in Smart Environment	37 - 44
<i>Roa Alharbi</i>	

4th International Conference on Computer Science, Engineering and Information Technology (CSEIT-2017)

Distance Learning via Social Media.....	45 - 55
<i>Mohammad Derawi</i>	
Traffic Signal Control with Vehicle-To-Everything Communication.....	57 - 69
<i>Muntaser A. Salman, Suat Ozdemir and Fatih V. Celebi</i>	

9th International Conference on Applications of Graph Theory in Wireless Ad hoc Networks and Sensor Networks (GRAPH-HOC - 2017)

Performance Evaluation of Mobility and Routing Protocols for Vehicular Ad Hoc Networks Using NS-2 and VanetMobiSim.....	71 - 83
<i>Fatma Baccar, Kais Mnif and Lotfi Kammoun</i>	

**9th International Conference on Network and Communications Security
(NCS 2017)**

Denial-of-Service Attacks Against the 4-Way Wi-Fi Handshake..... 85 - 94
Mathy Vanhoef and Frank Piessens

**3rd International Conference on Signal Processing and Pattern
Recognition (SIPR 2017)**

**CFAR Detection in MIMO Radars Using Fuzzy Fusion Rules in Homogeneous
Background..... 95 - 103**
Faycal Khaldi and Faouzi Soltani

INTERNET OF THINGS IN INDUSTRY 4.0

CASE STUDY: FLUID DISTRIBUTION MONITORING SYSTEM

Maroua Abdelhafidh^{1,2,3}, Mohamed Fourati^{1,2,4}, Lamia Chaari Fourati^{1,2,4}
and Abdessalam Chouaya⁵

¹Laboratory of Technology and Smart Systems (LT2S),
University of Sfax, Tunisia

²Digital Research Center of Sfax (CRNS)

³National Engineering School of Sfax, Tunisia

⁴Higher Institute of Computer Science and Multimedia of Sfax

⁵Research Center Gafsa Chemical Group (SIAPE), Gafsa, Tunisia

ABSTRACT

Internet of Things (IoT) is an emergent technology that provides a promising opportunity to improve industrial systems by the smartly use of physical objects, systems, platforms and applications that contain embedded technology to communicate and share intelligence with each other. In recent years, a great range of industrial IoT applications have been developed and deployed. Among these applications, the Water and Oil & Gas Distribution System is tremendously important considering the huge amount of fluid loss caused by leakages and other possible hydraulic failures. Accordingly, to design an accurate Fluid Distribution Monitoring System (FDMS) represents a critical task that imposes a serious study and an adequate planning. This paper reviews the current state-of-the-art of IoT, major IoT applications in industries and focus more on the Industrial IoT FDMS (IIoT FDMS).

KEYWORDS

Industry applications, Internet of Things, Fluid Distribution System, Water loss, Oil and Gas loss

1. INTRODUCTION

Nowadays, Internet of Things (IoT) also known as Internet of Objects becomes an emergent technology that is widely used by several application domains. Thanks to its advanced services, the International Telecommunication Union (ITU) defines it as a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies [1]. Diverse fields of applications adapt IoT in their main implementation process. The most prominent areas of application include the smart home, smart energy, healthcare, manufacturing, transport, environment, smart industry and so on. Smart Industry or called also industry 4.0 is the core of IoT and smart manufacturing [2]. Intelligent techniques and flexible models used to perform a real-time monitoring make this technology a great solution for several challenges. In Other hand, the fluid monitoring is considered as a required task that must be improved in order to save environments from fluid losses and maintain a balanced system. IoT Technology is more and more investigated in this monitoring area and different researches are carried to propose,

implement and evaluate IoT-enabled solutions for Fluid Distribution System (FDS). In fact, thanks to its diverse employed devices, the data collection phase is able to sense all fluid parameters that will be transmitted wirelessly to a remote control server where the data processing and management will be done. This multi-layer architecture allows a real-time supervision and helps the operator to make the appropriate decision in case of damage in the system. This harmony of IoT subsystems is the crucial way to solve the majority of supervision problems in an efficient manner. In this paper, we will review the applications based on IoT technology. We will detail their performance and then we will focus on IoT in the FDS applications. The rest of paper is organized as follows: section II represents the Industrial IoT and its various applications. Section III details IIoT in Fluid Distribution Monitoring system. In section IV, a synthesis is carried out where we compare between the existing IoT-based applications for FDMS and evaluate their robustness. Section V illustrates the challenges of IIOTFDMS. Finally, section VI concludes this paper.

2. INTERNET OF THINGS IN INDUSTRY 4.0

Industries experience a technological revolution. Thus, at the beginning, companies and organizations employed manual monitoring methods and traditional services that required a lot of resources and led to a waste of time which can disturb the system operation. After that, by keeping pace with the industrial revolution that has largely changed the industry foundations and the economy, the industry has recognized rapid alterations from industry 1.0 to industry 4.0 [3]. In fact, in version 1.0 and 2.0, these industries used traditional monitoring ways based on non-technical methods manually making transaction report. Then, the third version introduced the deployment of digital sensors measurement leading to the control automation. Recently, an hybrid entities such as the Human Internet Of Things and the Industrial Internet are investigated with various technologies such as the Information Technology (IT) and the Operating Technology (OT). Accordingly, a change in industry's approach based on heterogeneous data provided by various objects in order to be analyzed with smart manner and operational hardware and software is used to detect and locate possible impediments [4]. With the new concept of Industry 4.0, various IoT applications are developed in different industries as highlighted in [5] [6] [7]. These applications include environmental monitoring, healthcare service, smart agriculture, food supply chain, security, manufacturing, and surveillance.

- IoT in healthcare Industry: this application domain is one of the largest and fastest-growing industries [8]. In fact, integrating IoT features into medical devices improves the quality of service, allowing a secure and efficient supervision for patients. Thus, a real-time IIOThealth monitoring infrastructure, combining various objects and defining the communication technology used for data exchanging, becomes an innovative solution for continuous patient care [9]. The potential use of various types of devices such as mobile devices, sensors, people with wireless communication via mobile internet access perform personalized healthcare services [10].
- IoT in Smart Agriculture: Due to the negative effect of industrialized agriculture on the environment and its limited productivity level, it is important to propose agriculture information based on IOT technology [11]. The smart agriculture obtained by a combination between IoT and RFID based on control platform management system and intelligent sensors enables an accurate control and real-time decision-making.
- IoT and manufacturing: IoT devices improve the productivity of manufacturing operations. It provides a tremendous growth of data volume with an accurate analyze [12]. In other hand, it is necessary to adopt IoT at production level to improve energy

consumption and to be aware about the production management. A new business model can promise a scalable monitoring system and enlarge the consumer market [13].

- IoT for industry security: Authors in [14] declare that to make a deep study about the security of difficult industrial systems is necessary to raise the quality of monitoring process and drive the pervasiveness of security. Considering security at the design phase ensures a great time management and limits the system financial loss.
- IoT for safe environment: To save the environment from several disasters is a primordial task that requires to be more and more investigated. Various environmental fields are concerned to be extremely supervised such as the fluid distribution monitoring [15], Dam monitoring [16], ocean monitoring [17] and so on. In [17], authors highlight a System of IoT based on Smart services (SIS) for Ocean Fishing Vessel Industry to share and explore services in order to create a new business model based on smart information strategy.

In the rest of the paper, we will investigate more on the IoT-enabled Fluid Distribution Monitoring System solutions.

3. IOT FOR FLUID DISTRIBUTION MONITORING SYSTEM (FDMS)

Several works are implemented to monitor the Fluid system but in the context of IoT based solutions for such issue, few works are investigated. In this paper, we will provide a literature review about IoT-based solutions for Fluid Distribution Monitoring system which includes Water Distribution networks and Oil & Gas Distribution networks as shown in figure 1. The general IOT-based Architecture for FPMS is depicted in figure 2 that presents the system architecture combined with the software modules composed by four layer (the Data layer includes data collection and data storage layers, the Network layer, the Application layer includes service layer and business layer and the Interaction layer).

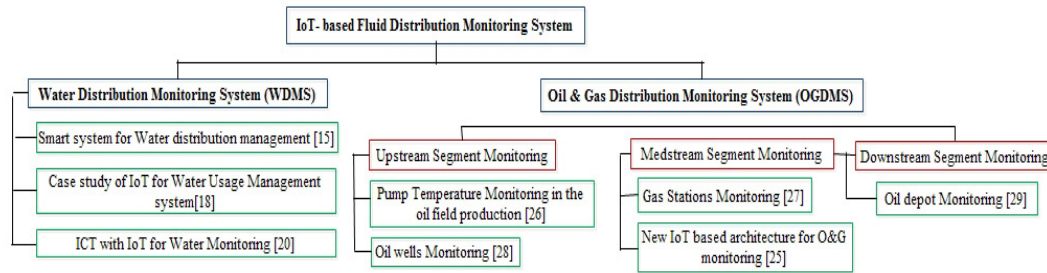


Figure 1. IOT Fluid applications in Industry

3.1. IoT-based Water Distribution Monitoring System

Authors in [18] define a case study of IoT for Water Usage Management system developed in Loughborough University in the UK and deployed in Sosnowiec in Poland and Skiathos in Greece. They report a comprehensive system based on IoT where they detail each phase of the implemented architecture by citing its main characteristics, proper configuration, used standards, software and hardware, etc. They used the water flow rate and temperature as data sources to monitor the water system. The application results and its assessments are carefully listed. The major lessons learned as they declared in their paper are:

- The necessity of an integrated system to ensure end-to-end data delivery in order to limit the human intervention in network stability.
- The use of a single data access interface as a solution to make an harmony between historical data and real-time data for the reason to guarantee a continuous data access and for a better interpreting data changes.
- A distributed Data base instead of a central one ensures the continuity of the system and provides high availability and fault tolerance.
- The importance of an on-line data management system to allow a transparent authorization to data access in-time.

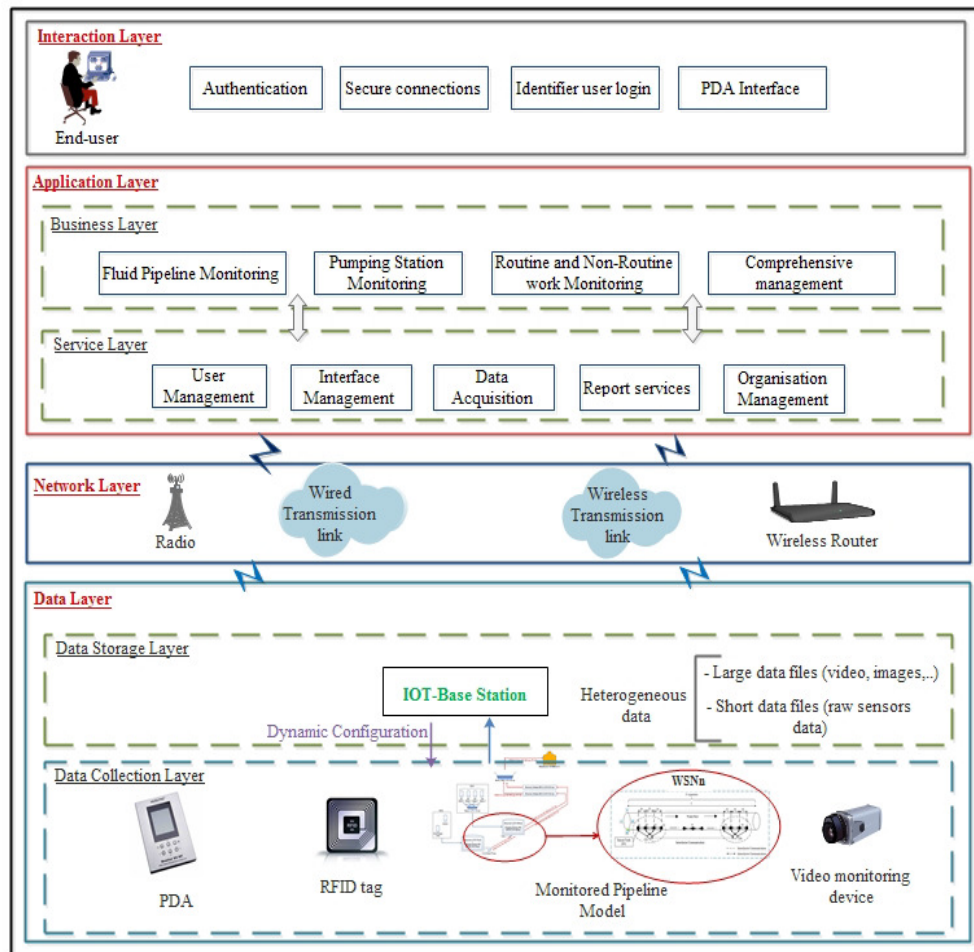


Figure 2. General IOT-based architecture for FDMS

In [19], authors suggest the automation of water supply system which is performed based on IOT. They detail the specific followed operations of the implemented round robin method. This method is applied for allocation of water in the residual areas in a centralized way. In this context, the monitoring process is based on master-slave system. The master is the central water supplier which will provide water to slave units presenting houses through Solenoid Relay nodes. To

calibrate the water consumption level, the water is supplied taking into account priority criteria. If the level is exceeded, an alert will be sent to the administrator and there will not be an additional water supply to the home concerned by this over consumption. Robles et al. in [20] reveal the lack of a reference model for the use of Information and Communication Technologies (ICT) in the field of water management. This problem is one among several described challenges that restrict the definition of industrial standards for water management. Consequently, in order to overcome these problems and implement a reliable water distribution system, authors present the MEGA [21] model as a performant reference for smart water management and detail its main layers. Then, they introduce their proposed requirements to improve the model considering its flexibility and the interoperability as main evaluation criteria.

To adapt concepts of IOT on smart environments taking into account the ICT technologies provide a real-time monitoring, scalable system that can deploy various subsystems. In addition to IOT, OPC UA (Object Linking and Embedding for Process Control) was developed as an open standard specification that allows the communication of real-time between different industries based on web services technology.

This system is improved in [22] where authors add more layers and interfaces in the deployed architecture. They consider the basic relationship between the physical and process models to define an hierarchical execution of physical elements and their better organization. Although the important role of such architecture for water management system, it still insufficient in case of other complex real problems. To solve this problem taking into account its large physical resources presents the future work to be held.

Authors in [23] present a proposed smart system to enhance the water distribution management for India using IoT. They introduce the use of the mobile phone of every Indian citizen and the valve used to calibrate water as embedded based water flow sensors to transmit data to the remote control centre. Accordingly, it will be easier to detect leakages and damage along the water pipeline.

3.2. IoT-based O&G Distribution Monitoring System (OGDMS)

The Oil and Gas companies aim to enhance reliability and optimize their operations in order to improve their business and reduce disruptions. Consequently, recently, these industries start working with data-management and integrate IoT in their applications. Oil and Gas industry value chain is divided into three main sectors: Upstream, Midstream and Downstream [24]. IoT technology can be applied either to monitor the segment where Exploration and Production of Oil and Gas i.e drilling exploratory wells (Upstream sector), the Pipelines companies that manage the pipelines that control the flow of oil (Midstream sector) or the segments where oil is cooked to make gasoline, diesel, jet fuel, etc. (Downstream sector). In [25], a novel IoT based architecture is presented to optimize the data collection from connected objects for the oil and gas industries. For each architecture layer and with each O&G sector, authors define the specificities of the implemented monitoring modules, their characteristics, equipments, used functions and technologies that support the robustness of each layer.

A design of new oil pump temperature monitoring system based on IoT is depicted in [26]. A smart real time collection of pump temperature data, during the oil production, promises useful information that allows recognizing the pump behaviour. In addition, if the temperature value surpasses a threshold value, a fault diagnosis system is implemented to alert the operator to make the appropriate action.

Authors in [27] aim to address a new IoT based system to monitor real time information of gas stations through a social network. Cloud storage is used to store collected data in order to have easy access to historical and new data remotely. This intelligent system comes to cope with the traditional gas station management based on manual monitoring and limited data resources and offer new original monitoring process with efficient data operation combined with accurate management.

Author in [28] addresses that Industrial Internet of Things use General Electric GEs Predix Software Platform to monitor and predict the performance and failure of wells. He notes that prevention of unplanned outages via the Industrial Internet of Things can save an operator up to 3 million per week which would otherwise have to be spent if a well goes out of production.

An IoT based management system is introduced in [29] to provide a remote supervision for oil depot. The proposed system is used to protect automatically the environment and to create a secure and workable system. Architecture of three layers is implemented composed by: the sensing layer consists of RFID tags and Personal Digital Assistants (PDA) employed to collect oil depot services. A communication layer used to send information gathered from the workplace to the control server where the safety management information system will be implemented.

4. SYNTHESIS

4.1. Comparative studies of existing applications

Under the concept of Industry 4.0, each IoT-based application presents its specific characteristics, material and monitoring system model. Table 1 provides a comparison between the applications detailed below and resumes their used techniques, equipments and technologies. In addition, according to the advantages noted in Table 1, it is revealed that the IoT integration enables efficient industry applications, optimizes its monitoring operations, creates new values and helps companies to transform their business. The collaboration between various smart equipments, technologies and the structured proposed systems ensure its interoperability and capability and guarantee an accurate and clear objective. Wireless networks are used by most applications in order to allow a continuous communication and an efficient data exchange between devices.

4.2. Evaluation of existing applications

The evaluation process is a crucial step permitting a relevant assessment of an achievement against various criteria and it follows different methods [30]. In this context, in order to identify the robustness and performance level of the previous detailed works, we try to evaluate and extract their main characteristics.

Researchers proposed several evaluations methods and categorized them into diverse classes such as:

- Data driven evaluation: this method determines the similarity level between obtained results and other source of data.
- Human-based evaluation: The objective is to determine the conformity between the system and the user specifications. For this, the usability technique [31] is used to develop systems interfaces especially for complex systems and to depict how much the resulted system is similar to the target one. It presents four evaluation criteria such as the flexibility, operability, learnability and understandability.

- Criteria-based evaluation: This type of evaluation considers a set of criteria to evaluate the system functionality such as: Intelligence, security.

We select the second and third approaches to evaluate the proposed systems as exposed in Table 2.

Table 1. Comparison of existing IoT- based Fluid Monitoring System Applications

	Material	Architecture/Medium	Advantages	Drawbacks
IoT-based Water Distribution Monitoring System				
[15]	-Liquid level sensor -Flow meters -Automatic weather station -Light source, PLC modules	-Service-Oriented Architecture -Layered Architecture -Wireless transmission	-Application framework based on SOA and IoT -Centralized management of massive	-
[18]	-Wireless Data collector -Wireless Gateway -Wifi Gateway -Flow rate / temperature -Flow sensors	-Star communication -3 layer architecture -Wireless	- Remote IoT –based application through real implementation -No data collision -Energy saving -Regular system -On-line configuration	-Human intervention in the monitoring system. -Central Data Base
[20]	-	-Hierarchical topology -High level architecture -Wireless	-Manageable and interoperable equipments -Open standard interface	-No integrated solutions -Coupled architecture
IoT-based O&G Distribution Monitoring System				
[25]	-Acoustic, Temperature sensors. -Flow and pressure sensors. -RFID tags.	Short/long range communication technology	-Continuous monitoring. -Minimum human intervention. -Predictive maintenance	-
[26]	-ARP- S3C2410 chip DS18B20 -Temperature Sensor	Three layer architecture	-Flexible interface. -Has a good scalability.	-
[27]	-Liquid level detection sensor -Temperature and Flow sensors -Minnow IoT Gateway	-Hierarchical network Architecture -Internet communication protocol WebSocket -Wireless Communication.	- Online services for people -Cloud Storage -Software with the advantage of portability. -Provides a huge user market.	- Centred information processing
[29]	-RFID tags - Explosion-proof PDA	-3 layer Architecture - Communication 3G - Software adopted: Oracle for storing business data, others are encapsulated as web service.	- Proven record in real depot sites	-

Table 2. Evaluation of the IIoT-FDMS applications

	Human-Based Evaluation			Criteria-Based Evaluation	
	Flexibility	Operability	Learnability	Intelligence	Security
[15]	+	+	+	+	-
[18]	-	+	+	-	-
[20]	+	-	+	+	+
[25]	+	+	+	+	+
[26]	+	+	+	+	-
[27]	+	+	-	+	+
[29]	+	+	+	+	-

5. IIOT FDSM CHALLENGES

Although, the great role of IOT in different application domains and its performance to provide accurate monitoring systems, this technology presents various challenges that would be overcome. Open challenges are discussed based on the IoT elements presented earlier. Many researchers were interested to enumerate these challenges in their works such as in [22], authors list IoT problems as follow:

- Complex interaction between water resources and environment system.
- Complicated solution based on diverse standards and methods.
- Lack of common standard for equipment internetworking.
- Insufficient knowledge for supporting ICT to understand water distribution process.
- Complicated supplier systems due to the lack of standardization.

Other authors [32] define the Industrial IoT FDMS challenges as privacy, sensing, data analytics, the standard WSN challenges including architecture, energy efficiency, security, protocols, and Quality of Service. Researchers tried to address these technical challenges in order to extend the network lifetime and to avoid any drawbacks. Authors in [33] focused on:

- Energy in IIOT FDMS: Therefore, the energetic limit is the most constraint in the IIoT FDMS design. It effects the network lifetime especially when supporting a variety of IoT entities. For this reason, to conserve the energy is the main goal. Researchers surveyed the different energy dissipation modes and sources of the overconsumption energy by the sensor node. Different mechanisms for energy conservation were overviewed such as the hierarchical topology based on clustering, the data aggregation and fusion and that directly influenced the network life time.
- Security in IIOT FDMS: A security model based on the concept of trust should be used in the system distributed surveillance. In this case, technical mechanisms must be at service of the security strategy. Therefore, too restrictive strategy enables little interaction and thus makes the system inoperative. It is the same with a very permissive strategy that eliminates the trust between users. In addition to the trust conception, the security is based on privacy of data. Then, it is a crucial task to protect the data referring to individual users from exposure in the IoT environment. Any physical or logical entity or object can be given a unique identifier and be able to communicate autonomously over the Internet or similar network.

6. CONCLUSION

In this paper, an investigation on Industrial IoT is carried on with various application domains. The wide use of such technology in various fields reveals its great importance and its efficient provided solutions to improve application results. The Fluid Distribution Monitoring System is also concerned by IoT services which improve the monitoring process and allow a real time management and data processing. Recent researches are investigated and described in order to prove the important role of this new smart technology and to evaluate their proposed architectures and systems. The main recapitulated insights are that IoT is an adequate solution to benefit smartly from IT services and operate under harmonious data access and data management. Therefore, companies that are responsible for Fluid transportation or requiring it in their production cycle are able to face considerable upside in improving pipeline safety and to handle a design of workable system. This development can guarantee the future success of industries and create new clear business objectives. IoT becomes a source of Big quantity of data obtained from heterogeneous and dynamic connected objects. For that, as future work, we will focus on managing and storing this data in a scalable way.

REFERENCES

- [1] F. Wortmann, K. Fluchter " et al., "Internet of things," *Business & Information Systems Engineering*, vol. 57, no. 3, pp. 221–224, 2015.
- [2] O. Monnier, "A smarter grid with the internet of things," Texas Instruments, 2013.
- [3] K. Schwab, *The fourth industrial revolution*. Penguin UK, 2017.
- [4] S. Wang, J. Wan, D. Li, and C. Zhang, "Implementing smart factory of industrie 4.0: an outlook," *International Journal of Distributed Sensor Networks*, 2016.
- [5] C. Perera, C. H. Liu, S. Jayawardena, and M. Chen, "A survey on internet of things from industrial market perspective," *IEEE Access*, vol. 2, pp. 1660–1679, 2014.
- [6] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.
- [7] M. Zarei, A. Mohammadian, and R. Ghasemi, "Internet of things in industries: a survey for sustainable development," *International Journal of Innovation and Sustainable Development*, vol. 10, no. 4, pp. 419–442, 2016.
- [8] Y. C. Wang, K. McPherson, T. Marsh, S. L. Gortmaker, and M. Brown, "Health and economic burden of the projected obesity trends in the USA and the UK," *The Lancet*, vol. 378, no. 9793, pp. 815–825, 2011.
- [9] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internet of things (IIOT)–enabled framework for health monitoring," *Computer Networks*, vol. 101, pp. 192–202, 2016.
- [10] I. Plaza, L. Martin, S. Martin, and C. Medrano, "Mobile applications in an aging society: Status and trends," *Journal of Systems and Software*, vol. 84, no. 11, pp. 1977–1988, 2011.
- [11] F. TongKe, "Smart agriculture based on cloud computing and IOT," *Journal of Convergence Information Technology*, vol. 8, no. 2, 2013.

- [12] F. Shrouf, J. Ordieres, and G. Miragliotta, "Smart factories in industry 4.0: A review of the concept and of energy management approached in production based on the internet of things paradigm," in *Industrial Engineering and Engineering Management (IEEM)*, 2014 IEEE International Conference on. IEEE, 2014, pp. 697–701.
- [13] A. Khan and K. Turowski, "A survey of current challenges in manufacturing industry and preparation for industry 4.0," in *Proceedings of the First International Scientific Conference Intelligent Information Technologies for Industry (IITI16)*. Springer, 2016, pp. 15–26.
- [14] C. Alcaraz, R. Roman, P. Najera, and J. Lopez, "Security of industrial sensor network-based remote substations in the context of the internet of things," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1091–1104, 2013.
- [15] X. Liu, H. Liu, Z. Wan, T. Chen, and K. Tian, "Application and study of internet of things used in rural water conservancy project," *Journal of Computational Methods in Sciences and Engineering*, vol. 15, no. 3, pp. 477–488, 2015.
- [16] N. Mohod, "Usability of internet of things [iot] for dam safety and water management."
- [17] C. M. Chen, L. J. Yu, P. L. Ling, J. S. Yang, and S. Q. Cao, "The architecture of iot smart service system of ocean fishing vessel and its application based on petri net," in *Applied Mechanics and Materials*, vol. 385. Trans Tech Publ, 2013, pp. 1771–1775.
- [18] S.-H. Yang, X. Chen, X. Chen, L. Yang, B. Chao, and J. Cao, "A case study of internet of things: A wireless household water consumption monitoring system," in *Internet of Things (WF-IoT)*, 2015 IEEE 2nd World Forum on. IEEE, 2015, pp. 681–686.
- [19] R. Ukkali and D. Geetha, "Automated water distribution system based on iot."
- [20] T. Robles, R. Alcarria, D. Martín, A. Morales, M. Navarro, R. Calero, S. Iglesias, and M. Lopez, "An internet of things-based model for smart water management," in *Advanced Information Networking and Applications Workshops (WAINA)*, 2014 28th International Conference on. IEEE, 2014, pp. 821–826.
- [21] "Mega project homepage: <http://www.gestiondelagua.es/en/>."
- [22] T. Robles, R. Alcarria, D. Martín, M. Navarro, R. Calero, S. Iglesias, and M. Lopez, "An iot based reference architecture for smart water management processes," *J. Wirel. Mob. Netw. Ubiquit. Comput. Dependable Appl.*, vol. 6, no. 1, pp. 4–23, 2015.
- [23] S. Ezhilvanji and S. Malarkodi, "An efficient water distribution system for india using iot."
- [24] A. Slaughter, G. Bean, and A. Mittal, "Connected barrels: Transforming oil and gas strategies with the internet of things," 2015.
- [25] W. Z. Khan, M. Y. Aalsalem, M. K. Khan, M. S. Hossain, and M. Atiquzzaman, "A reliable internet of things based architecture for oil and gas industry," in *Advanced Communication Technology (ICACT)*, 2017 19th International Conference on. IEEE, 2017, pp. 705–710.
- [26] D.-x. Wang, Y.-j. Xu, Z. Li, and Y.-p. Zhu, "Design of the oil pump temperature monitoring system based on internet of things," in *Advanced Research and Technology in Industry Applications (WARTIA)*, 2014 IEEE Workshop on. IEEE, 2014, pp. 831–833.
- [27] H. Cui, T. Xu, X. Jiang, and L. Fang, "Gas stations oriented internet service system based on intel minnowboard," in *Computational Intelligence and Design (ISCID)*, 2016 9th International Symposium on, vol. 1. IEEE, 2016, pp. 290–293.

- [28] P. Kendon, "5 innovative technologies changing maintenance management in the oil and gas sector," in Available via: <http://www.solufy.com/blog/5-innovativetechnologies-disrupt-maintenance-management>. [Accessed: 29.01.2017], 2016.
- [29] Z. Du, Y. Mao, and M. Lu, "Design and implementation of safety management system for oil depot based on internet of things," in Green Computing and Communications (GreenCom), 2012 IEEE International Conference on. IEEE, 2012, pp. 249–252.
- [30] M. Kim, "A quality model for evaluating iot applications," International Journal of Computer and Electrical Engineering, vol. 8, no. 1, p. 66, 2016.
- [31] M. O. Thomas, B. A. Onyimbo, and R. Logeswaran, "Usability evaluation criteria for internet of things," 2016.
- [32] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," Future generation computer systems, vol. 29, no. 7, pp. 1645–1660, 2013.
- [33] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.

AUTHORS

Maroua Abdelhafidh

Obtained her Bachelor degree in Management computer and Electronic Commerce and her masters in Computer Science and Multimedia from SFAX University, TUNISIA. Currently, she is a PhD Student at the National Engineering School (ENIS). She is a researcher at the Research Laboratory of Technology and Smart Systems (LT2S), Digital Research Center of Sfax (CRNS). Her current doctoral research area is in wireless communication, wireless sensor network, hydraulic pipeline monitoring and signal processing.



Mohamed Fourati

He obtained the engineering degree in electrical and electronic engineering from Higher Normal School Technical Studies, Tunisia in 1992, and master thesis degree from Sfax National Engineering School, Tunisia in 2008. Currently, he is an assistant professor in Multimedia and Informatics Higher Institute, Sfax. He is researcher in Laboratory of Technology and Smart Systems (LT2S), Digital Research Center of Sfax (CRNS). His scope of research is channel coding.



Lamia Chaari Fourati

She received the engineering and PhD degrees in electrical and electronic engineering from SFAX National Engineering School (ENIS) in TUNISIA. She received in 2011 HDR telecommunications from ENIS. Currently, she is an associate professor at multimedia and informatics higher institute, SFAX University, TUNISIA. She is also a researcher at Research Laboratory of Technology and Smart Systems (LT2S), Digital Research Center of Sfax (CRNS). Her scope of research are new generation networks, communications, wireless networking, multiple access and MAC design, QoS provisioning, IoT, M2M, SDN, ICN.



INTENTIONAL BLANK

TOWARDS A COMMUNITY-BASED MOBILE NEARBY ASSISTANCE SOLUTION: FRAMEWORK AND FIRST PROTOTYPE

Amine Boulemtafes¹, Dalila Hamidouche², Chayma Zatout², Chafika
Benzaid² and Nadjib Badache^{1,2}

¹CERIST Research center, Algiers, Algeria

²USTHB University Algiers, Algeria

ABSTRACT

In some cases, being able to appeal to a nearby assistance could be a determining factor possibly saving lives. In fact, a person can at any time encounter a problem or a danger, such as getting lost, falling, having a cardiovascular accident, facing a danger of aggression or theft or having a road accident, which becomes more critical if the person is being far from the eyes. From this perspective, this work aims to study the design of an effective mobile solution focusing on community involvement, cost and reactivity factors -with the help of a set of today's technologies in particular Smartphone, Cloud and sensors- allowing notifying users as well as competent services neighboring a person in need of help.

KEYWORDS

Nearby assistance, mobile, cloud, sensors, smartphone

1. INTRODUCTION

Some time ago, media talked about a motorcycle that recorded a video of a man losing the control of his car after having a stroke; fortunately, the motorcycle could follow the driver while assisting him in order to stop the car. Such situations could happen at any time and anywhere but unfortunately there's not always a motorcycle behind us. In fact, at any time, while being far from the eyes, a person could get lost, fall, have a cardiovascular accident, face a danger of aggression or theft or have a road accident.

Within this perspective, being able to appeal to a nearby assistance in case of a problem or danger even being far from the eyes could be a determining factor possibly saving lives. For this, community cooperation should be promoted especially with the help of today's technologies particularly Smartphone, Cloud and sensors which are becoming more and more part of our daily life, and thus are likely to facilitate the design and implementation of an effective solution for nearby assistance supporting the involvement of everyone and optimizing the reactivity towards persons in need of help.

Taking a look at the existing solutions, various systems for mobile emergency assistance call seem to be available on the market. Generally, such systems either make use of a dedicated device with an emergency button or just take advantage of Smartphone capabilities to do the job. From this, two main categories of such systems can be distinguished:

1.1. Systems based on an external device

Through an external device, a set of systems provide an emergency button used to trigger an alert, either independently or through the user's Smartphone. However, systems relying only on external device are much more expensive than those that make use of Smartphone, probably because of the needed built-in technologies. Examples of such systems include MobileHelp [1] a medical alert system working with local emergency service, relying on cellular/GPS without the need of a Smartphone and offering in extra an automatic fall detection device; Fall detector GPS [2] relying on built-in 3G and GPS to send help text/voice messages with position to chosen contacts; CareTracker SOS Voice [3] a personal alarm system relying on GSM and GPS to email/text message a defined caretaker and allow voice communication and tracking; or SafetyAnchor [4] which combines a Safety button and the user's Smartphone and its capabilities (communication, GPS, ...) to notify through Internet, family/friends contacts, local emergency service, as well as nearby volunteers for community help.

1.2. Systems based on a Smartphone

A more cost-effective solution for emergency assistance call systems is mobile emergency applications, which directly take advantage of Smartphone capabilities. Many examples of such applications can be cited, each having its features and advantages; Allô-Chorta [5] for example is a recent initiative from the Algerian police allowing to trigger an alert through Internet and text message in case of a danger both to the their services and predefined contacts, as well as offering the possibility to report a salient or dangerous event such as a theft or road accident; bSafe [6] is a more advanced application for safety and emergency assistance, keeping the user connected with a safety network through a set of features including tracking to let permitted contacts following you, and alert button triggering an alarm, starting video record and notifying all your friends with live location sharing; Bugle [7] solution, with a different logic, lets the user set an activity plan such as walking or jogging and automatically trigger through text messages and email an alert to predefined emergency contacts if the user doesn't check-in at time from his last activity. SafeTrek [8] came with another idea through a "hold until safe" button, where the alert button should be hold if the user feels scared, once the button is released, the user is asked to enter a code, if he does not, the local police is automatically notified of his location and emergency. Many other applications with other features can also be found such as Red panic button [9] which introduces social network integration, ICEcontact [10] which introduces delayed message allowing to automatically send an alert message after a predefined time if something goes wrong even if your phone dies or loses service, iGoSafely [11] which allows to trigger an alert by plugging in your headphone, iSurvive [12] allowing to use a Smartphone as a flashlight for SOS Morse code for example, and integrate a false deactivation option in case an aggressor tried to cancel the alert, or PanicGuard [13] and Eyewatch [14] which both feature automatic raise of alert if a fall is detected.

From the above quick overview, it is noted that the first category of solutions are interesting in the way that external devices are generally easy to use especially for elderly, while a number of these are also waterproof and thus can be used even under the shower or out in the garden; however, these kind of solutions are quite expensive seemingly due to the need of an external device especially if Smartphone is not involved where external device would be required to do all the job by itself and thus would requires more features. From another hand, the second category is clearly more cost effective and even generally free apart from services like cellular or Internet.

It is also noted that, for both categories, Internet, call and text messages are generally the means used to raise an alert and that only few solutions integrate automatic triggering, but usually only for sudden fall, jerk or stop. In another hand, a number of solutions also from both categories rely

on local emergency number (such as 911), as well as solution provider own responders who unfortunately don't act world widely and might require periodical (like monthly or annually) fees; Also, most of these solutions -except some, like Safety Anchor- don't involve the community and are only limited to contacts and/or competent services which might be too far from the person in need of help.

From this point, this work aims to study the design of a cost-effective nearby assistance solution by its architecture, features and possible enhancements, focusing on reactivity optimization in terms of speed and efficiency through community involvement, triggering and notification means and automation of emergency appeal with sensing and data analysis. To this end, we first define the solution's general architecture, its components and their roles. The different communication aspects are also described. Lastly, the proposed solution brings together a set of novel and inspired features going in favor of the target goals.

The remainder of this paper is organized as follows: The next section presents the proposed solution through the description of a framework for the design of an effective mobile solution for nearby appeal to an aid. The third section presents a first prototype intended to fall detection and notification as well as a couple of notes observed during the implementation of some features. The last section discusses the functionalities and future works related to the described framework and presented prototype, and concludes the paper.

2. NEARBY ASSISTANCE SOLUTION FRAMEWORK

From what has been previously mentioned, it turns out that in order to come up with an affordable solution for an effective reactive assistance, two important factors among others should be addressed namely infrastructure and services costs, and reactivity optimization means.

Opting for the second category of solutions i.e. Smartphone-based seems to be a suitable choice knowing that these smart devices are nowadays widely popularly used even by elderly, are more and more convenient and powerful, and almost not forgettable, which make them an ideal candidate to turn from a smart device to a safety tool; the use of voice or countdown alert triggering as it will be presented later can be imagined as alternatives to waterproof previously described feature found in the first category. Therefore, from an end-user perspective, the solution should be operational with only a Smartphone and a free mobile application; however, some advanced features could need extra equipments like sensors as it will be described later. For services, the solution should be able to select between communication means if different possibilities are offered in order to raise an alert while maintaining at best a tradeoff between cost and reliability; at last, community involvement should be promoted in order to enhance reactivity and as an alternative to paid emergency responders.

2.1. Architecture

Figure 1 presents the general architecture of the proposed solution composed from four main parts namely, the user in need of help, the safety tool (his Smartphone), the central server for coordination, and the potential helpers.

2.1.1. The user in need of help can optionally wear sensors which might be interesting for two reasons: (1) Some types of alerts could be automated according to related sensors data after analysis, such as accelerometer for fall and pulse for heart rate problems; (2) Sensors data might contain important and useful information for competent services reflecting for example the health

state of the person in need of help, which could be an important decision support regarding relevant services to send and equipments or medicines needed on site.

2.1.2. The safety tool or Smartphone, whose primary role is to raise and broadcast alerts, is used through a dedicated application and with the help of its capabilities, to provide different features enhancing the reactivity towards its owner as it will be described later.

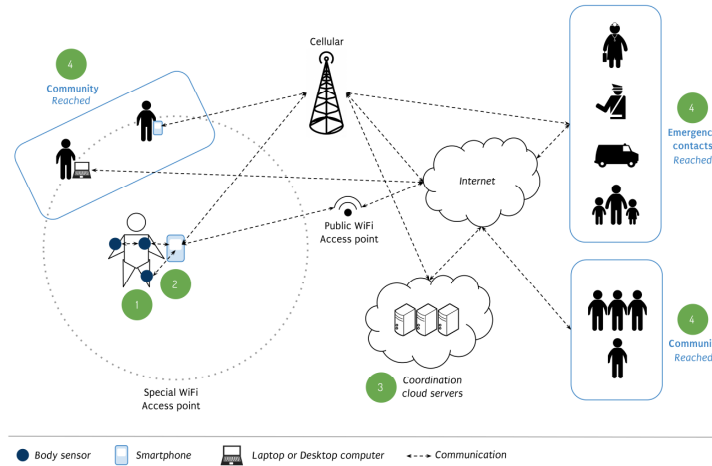


Figure 1. Nearby assistance solution framework

2.1.3. Central server, is the coordinating Cloud of the solution playing a number of roles over Internet network such as managing users, storing sensitive information, dispatching alerts, providing consultation on the web, streaming video and audio, textual communication, etc.

2.1.4. Potential helpers, include competent services such police or firefighters, user's predefined emergency contacts and registered community.

2.2. Communication

Different communication means between user's Smartphone and potential helpers are possible; the framework's scenario of communication proposal is as follows:

For direct connections between user and emergency contacts (family, emergency service, etc.) cellular network is usually used such as assistance through voice call.

For broadcast of alerts and small-medium size data like current position, Internet network if available with enough reliability should be prioritized given its cost-effectiveness; an alert can be sent to important contacts through email, social networks, ...etc. as well as to the central server which will be in charge of dispatching the alert to relevant users according to location for example as it will be described later. In case Internet is not available or not enough reliable, help request text message over cellular network can be used to reach helpers directly such as for important contacts and/or through central server for dispatching.

In order to widen scope and speed up reactivity, a costless technique for broadcasting alerts through Wi-Fi Access Point SSID can be introduced as it will be presented later in this document. Regarding live audio/video sharing, streaming could be performed through Internet if available or cellular 3G/4G video calls if available and accessible for the user but with limited participants.

From another hand, since Internet through cellular network might sometimes be intermittent, or provides low bandwidth and sometimes it is simply expensive, it seems important to optimize Internet-based text-messaging communications, such as for alerts dispatching. To this end, a suitable communication protocol taking into consideration these constraints should be used. MQTT a lightweight messaging protocol with mobile sector focus seems to be a reasonable choice due to its advantages [15]. In fact, it is reported that MQTT, with its characteristics, is ideal in case of constrained environments limitations such as network expensiveness, low bandwidth or unreliability [16]; moreover, MQTT implements a security mechanism ensuring that all messages are transmitted even in the presence of brief disconnections [15].

2.3. Features

Before describing the main features of the proposed solution, we first start by giving a brief description of how the overall solution should work.

When a person is potentially in need of help, an alert with current location is raised and a set of features are triggered or become available depending on his situation such as video streaming; the alert, via available appropriate communication means, is broadcasted to nearby potential helpers including competent services such as police, defined emergency contacts and registered community. Potential helpers if permitted should be able to track the person in need of help in order to reach him, while competent services as well as emergency contacts particularly should meanwhile also be able to interact with him for remote assistance, depending of course on the emergency situation.

Starting from the above overall steps, details of “how it works” are presented below through a set of features description. A part of these going in favor of reactivity optimization are summarized in Table I, while Table II summarizes features related to security.

2.3.1. Different alert types such as for road accident, fall, theft ...etc. can be raised; this can enhance reactivity in terms of who should come to help (police, firefighters ...) and what is expected to do and to find on site.

- Alert could be raised after a quick countdown timer to avoid accidental alerts.
- To deactivate an alert, the application could ask for a secret code before deactivating; this could avoid bad attempts of deactivation such as from an aggressor. If the introduced code is wrong, a fake deactivation can also be used to deceive the aggressor.

2.3.2. Different ways of triggering (such as shaking or long button press), one for each alert type which could enhance speed of triggering and thus reactivity.

2.3.3. Alert type dependant features; i.e., trigger or make available a set of features on the basis of the type of alert such as light and sound signals in case of lost; this could contribute in reactivity speed and simplify the use of the solution.

2.3.4. Storing alerts on central server allowing keeping track of reported assistance appeals and consultation on map.

- Alerts can also be forwarded to central server for storing through potential helpers if this was not done by the person in need of help (after verification to ensure uniqueness of stored alerts) such as in case of network service unavailability.

2.3.5. Involve social networks, through dedicated accounts where alerts can be posted in order to reach more potential helpers even non-registered community and people with Internet access restricted to social networks.

2.3.6. Delayed alerts, where an alert can be stored on the central server to be dispatched at a certain time; this allows to take precaution and ensure that an alert will be triggered in case something goes wrong even in case of out of network service or Smartphone shutdown; example of such situations include going for a walk where an alert will be automatically raised if you don't cancel it, or when feeling discomfort and you don't want to bother anyone since it's a slight malaise but at the same time you are afraid you will not be able to raise an alert if things goes worse.

2.3.7. Broadcast alert through Wi-Fi access point, because sometimes the person that could quickly help is just behind a wall, in the next street or in a near store or house, it's seems therefore interesting to be able to reach very near persons even if they are not connected or the service network is unavailable; this could be done through creating a Wi-Fi access point and integrate a help request into its SSID which could widen the appeal scope to nearby houses, stores and streets; alert received can even be rebroadcasted to neighbors of neighbors through recreating the access point, and also dispatched by forwarding the message via the central server if a receiver has an Internet access.

- In order to avoid false alerts, information provided by SSID should have a special format or be encoded; however, since SSID only authorizes a maximum of 32 characters, information included should be minimalist and techniques to reduce message length could be used such as defining acronyms for possible situations for example, THF for theft and FAL for fall.
-

2.3.8. Integrate data from biosensors in order to ensure alerts' raising and speed-up reactivity by automating assistance appeals with the help of data analysis algorithms such as fall or no movement detection using accelerometer.

2.3.9. Sound & light signals in order to ease localization as well as reach more nearby people such as in case of lost.

2.3.10. Use targeted broadcasting using location, such as nearest competent services; registered community can also be targeted through location request from central server; such feature could be optional for potential helpers giving them the possibility to adjust assistance appeals scope avoiding receiving too far requests for example, if this reduces their willingness to help by the time.

2.3.11. Keep at best a tradeoff between communication speed and cost for sending alerts, such as prioritizing Internet messaging over service network messages.

2.3.12. Offline map for tracking allows faster reactivity of potential helpers for localization and tracking of persons in need of help even with low bandwidth or unavailability of Internet.

2.3.13. Navigation to nearest competent services using offline map itinerary, which might speed up reactivity towards the person.

2.3.14. Remote assistance and information through video, audio and textual communication, instant photos sharing ..., which might enhance reactivity.

Table 1. Summary of reactivity optimization features.

Feature	Description
Different alert types	Provides information about appropriate services to send on site and what is expected to find there
Different alert triggering ways	Eases the use and allows quick triggering
Social networks involvement	Reach more people even with restricted to social networks Internet as well as people not using the application
Wi-Fi access point broadcasting	Reach more nearby potential helpers even those not using the application or without Internet
Biosensors data	Automate alerts and ensure their sending even when it is not possible manually
Sound & light signals	Speed up localization and reach more nearby potential helpers
Offline map	Localization even with low bandwidth or unavailability of Internet
Remote assistance & information	Start assistance before arriving on site or reaching the user

Table 2. Summary of security features.

Feature	Description
Countdown before alert	Prevents accidental alert raising
Code for deactivation	Prevents accidental alert canceling as well as bad attempts such as aggressor wanting to cancel an alert
Fake alert deactivation	Prevents (through deceit) from bad attempts
Access point SSID information format or encoding (user ID, situation, location, date/hour)	Protection against false alerts
Broadcast and tracking permission	Public or private (competent services and emergency contacts)
Store on server information about identity of approaching potential helpers	Protection (through discouragement) against misusing such as a bad person taking the opportunity for attacking a lost person
Store on server information about identity of help appeal receivers	For investigation like interviewing people close of an accident

It should be pointed out that such system should be under the supervision of competent services and registered users should be aware about possible information stored on central server such as their Id in case of approaching or receiving a help appeal, as well as possible communication costs such as for retransmission of help appeals to central server.

3. FIRST PROTOTYPE & OTHER PRELIMINARY TESTS

A fall detection solution's prototype still in its infancy is described showing some of the framework features described in the previous section.

A first mobile application (BFall, see Fig. 2) running in background of the user's Smartphone can detect falls and send accordingly an alert to the user's family and/or medical staff allowing them to locate him and take necessary measures.

Fall detection relays on data collected from two Smartphone built-in sensors namely accelerometer and gyroscope; with the help of a data analysis algorithm, the application continuously check if a fall has been occurred; once detected, the localization mechanism is triggered and a verification process (see Fig. 2) is launched giving the user 5 seconds in order to

cancel the alert in case he is doing well or it is just an accidental alert; if the user reacts positively, the localization mechanism is stopped, otherwise, a communication phase between the user and his emergency contacts is started.

If Internet is available, an alert message containing the user's location is sent through MQTT messaging protocol to emergency contacts; otherwise, the alert is sent as a simple text message (SMS) including GPS coordinates (if available) through cellular network service.

MQTT through publish/subscribe scheme allowed designing a one-to-many alert transmission architecture in order to be able to notify all emergency contacts at the same time including caregiver and family members. From another hand, among the three quality of service modes offered by MQTT, the third one i.e. QoS=2, considered as the safest transfer mode but also the slowest, was used since alert reception is mandatory.

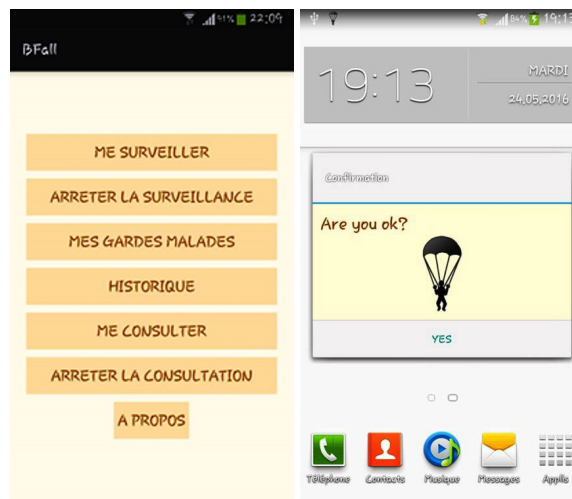


Figure 2. BFall: Main screen (left) and verification process screen (right)

A second application (CFall, see Fig. 3) running in background on the emergency contact Smartphone is used in order to handle alerts.

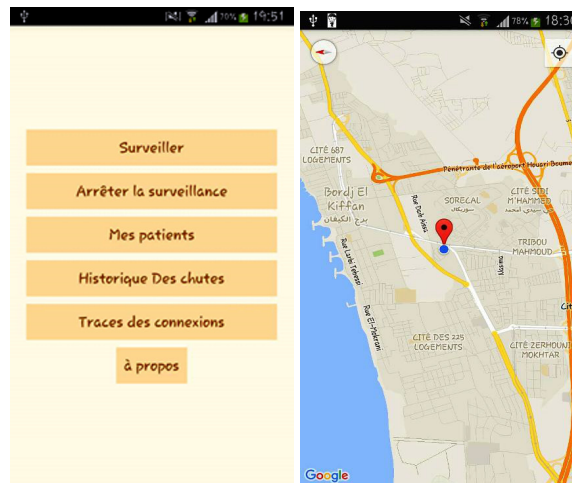


Figure 3. CFall: Main screen (left) and Localization on the map (right)

Once received, alerts are displayed with the identifier of the sender on the screen and through a simple tap a map is opened showing the location of the person in need of help (see Fig. 3).

In case an alert was received through an SMS, the application automatically and seamlessly retrieves location coordinates and displays it on the map (see Fig. 4). History of received falls is stored on a database in order to help doctors in their diagnostics (see Fig. 5).

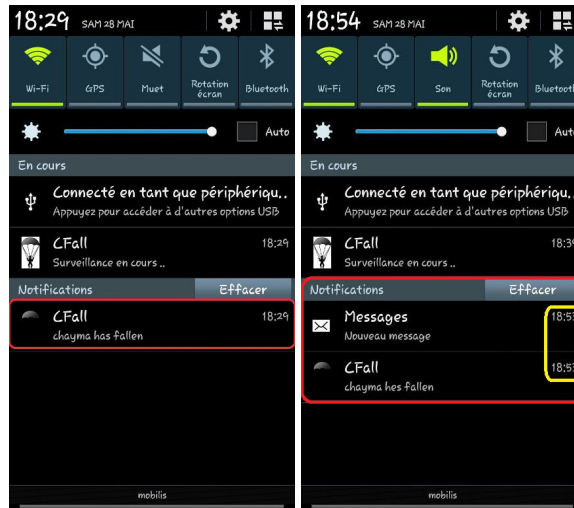


Figure 4. CFall: Alert notification using Internet (left) and SMS (right)

It should be noted that if an MQTT server doesn't receive any message after a certain time interval from a client, this latter is considered as disconnected and will no longer receive notifications; for this, MQTT Keep Alive option was used to ensure the connection between client and server through a regular sending of pings.

At last, in order to allow information exchange between the monitored person and his emergency contacts, a chat feature (see Fig. 5) was also implemented through MQTT messaging protocol.

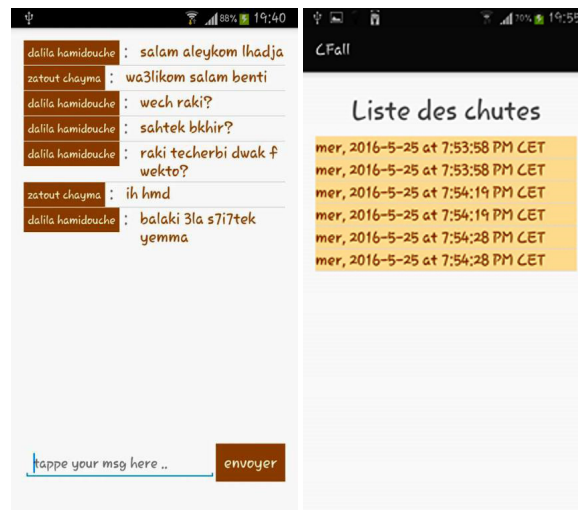


Figure 5. Chat feature (left) and Received falls history (right)

Some other features preliminary tests were also done i.e. alert triggering and notification means (see Fig. 6). From tests done on an old Smartphone running Android 2.3.4, it was noted that some actions -in order to trigger an alert- could be used even when the application was in background such as shaking the Smartphone, while some other actions could be used only when the application was in foreground such as catching volume (up/down) or other Smartphone keys which might limit the number of possibilities regarding triggering means.

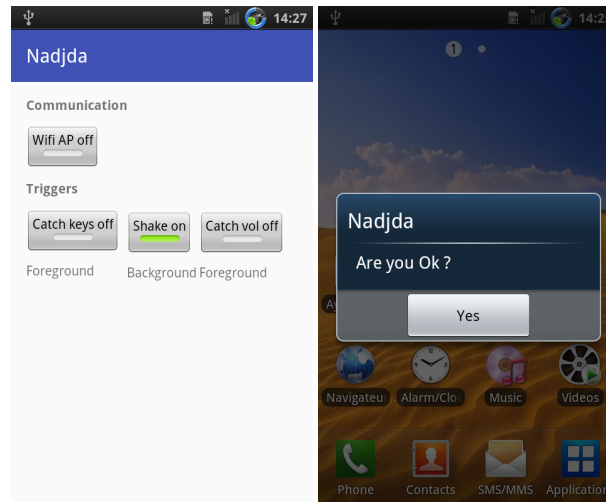


Figure 6. Preliminary tests (left) and confirmation dialog after shaking action while application is in background (right)

4. DISCUSSION AND CONCLUSION

The presented work described an assistance framework through its architecture and features. The framework aims, ultimately, to lead to a mobile nearby assistance solution taking into consideration three important criteria, namely: reactivity for reaching its main goal, affordability for wide public access and security for preventing misuse. To this end, the proposed framework conceptualizes a simple solution relying essentially on user's Smartphone, and combining security mechanisms and a set of interesting features mainly for promoting community cooperation, enhancing alert triggering and notification while ensuring its reception, and supporting reaching the user; the overall with a view to optimize reactivity towards persons in need of help.

Relying only on user's Smartphone for alerts' triggering, unlike the first category of solutions previously described, not only contributes to cost-effectiveness but also generally allows to offer more ways for triggering while enabling customization.

Varying alert types as well as notification and triggering ways including social networks, WiFi broadcast and automatic triggering through delayed alerts or biosensor data analysis allows -unlike a number of existing solutions- to address a large variety of danger and emergency cases and situations while ensuring alert delivery and enhancing reactivity towards people in danger from different ways as previously described like increasing triggering speed or reaching more neighboring community.

Unlike a number of exiting solutions which only relies on competent services such as police or solution provider own responders, the described framework promotes the involvement of community which supports cost-effectiveness as well as reactivity, while a number of security

features were also proposed to mitigate possible danger from potential community's malicious members.

Other presented features, some of which have also already been implemented by existing solutions, such as sound and light alerts or offline map with itinerary were brought together in the proposed framework for an increased optimization of the intended solution.

On the other hand, despite the presented prototype is still in its infancy and requires a lot of work to meet the goals set for the described framework, some of the core features were already implemented and a couple of observations were noted during the study and design.

Indeed, in comparison with the framework, the prototype already implements one-to-many alert sending mechanism to reach multiple receivers, automated alert triggering through Smartphone' sensors data analysis, localization of user on map, auto-switch to text message alerts via cellular network service if Internet is not available and remote assistance through chat feature. However, localization on map feature needs to be enhanced to work offline and allow navigation to nearest competent services while remote assistance should be widen to voice and video.

Regarding messaging communications, and more precisely MQTT compared to HTTPS, it was reported that according to test results of sending and receiving messages through both 3G and Wi-Fi connectivity, MQTT used less battery, was more reliable as well as faster [17], which consolidates and supports the MQTT choice; however, since Keep Alive option should be used in order to maintain connectivity between server and users, cost of such option as well as energy consumption should be more studied. Concerning MQTT server, it was noted that various brokers exist such as HiveMQ, Mosca, RabbitMQ, ActiveMQ or Mosquitto on which the choice fell for the implementation of the prototype; this latter is free and offers suitable quality of service option i.e. QoS=2, as well as SSL for secure access. However, benchmarks within the application context between messaging protocols such as MQTT, AMQP or KAFKA, ... should be considered in future works in order to come out with a more practical and validated choice.

Next prototype versions should, in addition to implement remaining features, incorporate the two current applications into one single application since a user can either be a helper or a person in need of help, especially with the involvement of community.

REFERENCES

- [1] <https://www.mobilehelp.com/> (Last access: 26/01/2017)
- [2] <https://www.medialarm.com.au/shop/fall-detector-gps/> (Last access: 26/01/2017)
- [3] http://ilcaustralia.org.au/products/21019?search_tree=631 (Last access: 26/01/2017)
- [4] <https://safetylabs.org/> (Last access: 26/01/2017)
- [5] <http://www.dgsn.dz/?-Allo-Chorta-> (Last access: 26/01/2017)
- [6] <http://help.getbsafe.com/> (Last access: 26/01/2017)
- [7] <http://www.gobugle.com/> (Last access: 26/01/2017)
- [8] <https://www.safetrekapp.com/> (Last access: 26/01/2017)
- [9] <http://redpanicbutton.com/> (Last access: 26/01/2017)

- [10] <http://icecontact.com/about-us/> (Last access: 26/01/2017)
- [11] <http://www.igosafely.com/> (Last access: 26/01/2017)
- [12] <http://www.isurviverescueapp.com/about-isurvive> (Last access: 26/01/2017)
- [13] https://panicguard.com/?page_id=652 (Last access: 26/01/2017)
- [14] <https://www.eye-watch.in/> (Last access: 26/01/2017)
- [15] J. E. Luzuriaga, M. Perez, P. Boronat, J. C. Cano, C. Calafate and P. Manzoni, "A comparative evaluation of AMQP and MQTT protocols over unstable and mobile networks," 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, 2015, pp. 931-936.
- [16] J. E. Luzuriaga, J. C. Cano, C. Calafate, P. Manzoni, M. Perez and P. Boronat, "Handling mobility in IoT applications using the MQTT protocol," 2015 Internet Technologies and Applications (ITA), Wrexham, 2015, pp. 245-250.
- [17] Why HTTP is not enough for the Internet of Things – https://www.ibm.com/developerworks/community/blogs/mobileblog/entry/why_http_is_not_enough_for_the_internet_of_things?lang=en (Last access: 26/01/2017)

DETECTION AND PREVENTION OF BLACK HOLE ATTACK IN VANET USING SECURED AODV ROUTING PROTOCOL

Salim Lachdhaf¹, Mohammed Mazouzi², Mohamed Abid³

¹Department of Informatics, Faculty of Sciences of Gabes,
University of Gabes, Gabes, Tunisia

²Assistant Professor at Higher Institute of Business Administration of Sfax,
Member of CES-Laboratory, University of Sfax, Sfax, Tunisia

³Professor at National School of Engineering of Sfax,
Director of CES-Laboratory, University of Sfax, Sfax, Tunisia

ABSTRACT

Vehicular ad hoc networks (VANETs) are becoming popular and promising technologies in the modern intelligent transportation world. They are used to provide an efficient Traffic Information System (TIS), Intelligent Transportation System (ITS), and Life Safety.

The mobility of the nodes and the volatile nature of the connections in the network have made VANET vulnerable to many security threats. Black hole attack is one of the security threat in which node presents itself in such a way to the other nodes that it has the shortest and the freshest path to the destination.

Hence in this research paper an efficient approach for the detection and removal of the Black hole attack in the Vehicular Ad Hoc Networks (VANET) is described. The proposed solution is implemented on AODV (Ad hoc On demand Distance Vector) Routing protocol one of the most popular routing protocol for VANET. The strategy can detect both the single Black hole attack and the Cooperative Black hole attack in the early phase of route discovery.

The simulation is carried on NS2 and the results of the proposed scheme are compared to [14] and the fundamental AODV routing protocol, this results are examined on various network performance metrics such as packet delivery ratio, throughput and end-to-end delay. The found results show the efficacy of the proposed method as throughput and the delivery ratio of the network does not deteriorate in presence of the back holes.

KEYWORDS

VANET, Black hole attack, Security, AODV

1. INTRODUCTION

Recently, with the improvement in the wireless communication technologies and the high number of road accidents, vehicular ad hoc network (VANET) are used to provide an efficient Traffic Information System (TIS). According to the National Highway Traffic Safety Administration (NHTSA), vehicle-to-vehicle (V2V) has a high lifesaving potential that address approximately 80 percent of multi-vehicle crashes. [1].

Natarajan Meghanathan et al. (Eds) : NeTCoM, CSEIT, GRAPH-HOC, NCS, SIPR - 2017

pp. 25– 36, 2017. © CS & IT-CSCP 2017

DOI : 10.5121/csit.2017.71503

VANET is a subclass of Mobile Ad-hoc Network (MANET) which consists of number of nodes (vehicles) with the capability of communicating with each other without a fixed infrastructure [19]. However, compared to MANET, VANET has an extremely dynamic topology due to high mobility of vehicles. the nodes tend to move in an organized pattern. Besides, VANETs have a potentially large scale which can comprise many participants and the capacity to extend over the entire road network [2]. Therefore, Routing protocol & Attacks: Lack of centralized management in VANET puts extra responsibilities on vehicles. Hence each vehicle is a part of the network and also manages and controls the communication on that network. Due to the high mobility of nodes the links between vehicles connect and disconnect very often which make routing process challenging. Hence, many researchers have focused on routing in VANET. The main aim of these proposed routing protocols is to maximize Packet Delivery Ratio (PDR) and throughput while minimizing controlling overheads and packet lose ratio. In this direction many routing protocol has been proposed which has important role in organizing the network safety. However, ad hoc routing protocols can be divided into proactive, reactive and hybrid protocols [3], Proactive protocols are typically table driven. Destination Sequence Distance Vector (DSDV), Global State Routing GCR are examples of this type. On the contrary, reactive protocols do not periodically update the routing information. It finds the route only when needed like Ad Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR). Hybrid protocols make use of both reactive and proactive approaches. Example of this type includes Zone Routing Protocol (ZRP).

AODV is the most frequently used reactive routing protocol in VANET [4]. But this protocol is not designed to tackle the security threats. So it's prone to black hole attack, gray hole attack, warm hole attack, Sybil attack, etc. [5].

In this paper, we will concentrate on well-known and Intelligent black hole attack in AODV base VANET. An intelligent black hole attack it's used by a malicious node that intelligently adapt and vary their behavior to avoid the detection and to bypass security solutions. However, as it is mentioned above, AODV is a reactive routing protocol; nodes will only send the control data only when is necessary. The node which has data to send, it generates Route Request (RREQ) packet and broadcasts it. If malicious node (black hole attack) is present in the network, the attacker node, on receiving RREQ message, sends Route Reply (RREP) without even having an actual route to the destination, and will entice all other to route packets through it. The attack becomes more severe if more than one node colludes in attack. Many research works focus on a single black hole attack but are less effective in cooperative and intelligent black hole attacks.

The remaining of this paper is organized as follows: In section II we introduced background of AODV protocol and black hole attack. Relevant related work and their limitations are discussed in section III. Section IV describes the proposed methodology and related algorithm. The simulation experimental outcomes along with the analysis of performance are presented in the Section V. Finally, Section VI contains our conclusions and the future work of our research.

2. AODV ROUTING PROTOCOL AND BLACK HOLE ATTACK

The Ad hoc On-demand Distance Vector (AODV) routing protocol [5][3] uses on-demand approach to find routes, thus, a route is established only when it is needed by a source node to send data packets. There are two mechanisms used in AODV, first is route discovery and second is route maintenance. When a node needs to forward a data packet, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the data packets to the destination. If a route is not available or the previously entered route is inactivated, it buffers the packet and broadcasts a Route Request message (RREQ). The source node and the intermediate nodes store the next-hop information corresponding to each flow of

data transmission.

When an intermediate node receives a RREQ, it either forwards it or generates a Route Reply (RREP) and it does not forward the RREQ any further if it has a valid route to the destination. RREP is a unicast message routed back along the reverse path to the source node. Only the destination node itself or an intermediate node that has a valid route to the destination are allowed to send a RREP to the RREQ's source node, hence, RREQ messages may not necessarily reach the destination node during the route discovery process. This enables quicker replies and limits the flooding of RREQs. This process continues until a RREP message from the destination node or an intermediate node that has a fresh route to the destination node is received by the source node.

However, the source node may obtain multiple routes to a destination for a single RREQ. The destination sequence number is used to identify the latest route. The highest destination sequence number means the freshest path to the destination node, which is accepted by the source node for the data transmission. If two or more paths to the destination node have the same highest sequence number, the source node chooses the route with the lowest hop count.

In route maintenance, a route established between two nodes is maintained as long as needed by the node which wants to transmit data packets. If any node identifies a link failure it sends a RERR (Route Error) packet to all other nodes that use this link for their communication to other nodes until the source node is reached. The affected source node may then choose to either stop sending data or reinitiate the route discovery process sending a new RREQ message.

AODV is exposed to a variety of attacks since it has no security mechanisms [6]. Black hole attack is one such attack and a kind of denial of service (DoS) attacks [7] where a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the freshest and the shortest path to the destination node even if no such route exists since in AODV, any intermediate node could respond to RREQ message if it has a fresh route.

The main goal of black hole attack is rerouting the network traffic through a specific node controlled by the attacker. During the Route Discovery process, the source node sends RREQ packets to the intermediate nodes to find a fresh route to the intended destination. Malicious nodes respond immediately to the source node without even checking its routing table by claiming that it has the freshest and the shortest route to the destination on the route reply packet sent to the source node. The source node assumes that the route discovery process is complete, ignores other RREP messages from other nodes and accepts the path through the malicious node to route the data packets. The attacker now drops the received data packets instead of forwarding them to the destination as the protocol requires.

For example, in Fig. 1, the source node (S) needs to send a data packet to node (D), so it broadcasts a route request packet RREQ to its neighbors to find a route to that node. It is assumed that node B is a black hole in the network and the intermediate node A has a fresh route to the destination node (D). The nodes (A, B, C, F) receive the RREQ packet from the source node (S), the node B replies directly using a fake RREP and it claims that it has the highest sequence number and lowest hop count to the destination node (D) without checking its routing table. So, the malicious RREP reaches fastest to the node (S) compared to other replies from other nodes in the network. As a result, node (S) accepts the freshest and the shortest route through the black hole node (node B) and sends data packets to the node (D) via this node, the other received RREP packets are rejected (in this example, the RREP packet from the node A is rejected). The source node (S) assumes that the data would reach safely to the destination node but, in fact, the black hole node drops all data packets instead of forwarding them to the destination.

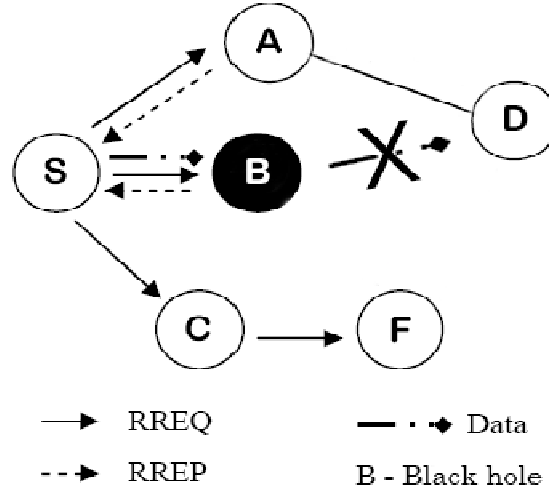


Figure 1. Routing discovery in AODV under black hole attack

This paper provides routing security to the AODV routing protocol by detecting and preventing the threat of Black Hole attacks.

3. LITERATURE REVIEW

Lately, black hole detection has been an active area of research and many solutions have been proposed. However, most of the solutions can detect and prevent only the single black hole attacks and requires high overhead to detect collaborative and intelligent adaptive attacks. Several solutions have been proposed for MANETs can be implemented in VANET. This section discusses some of these works.

In [8], R. Khatoun et al. proposed a reputation system for the detection of the black hole attacks, a watch dog is used to check the modification of information in received packets. In other hand a reputation score is used to identify the nodes that drop packets frequently. This mechanism fails in the presence of cooperative black hole attacks, since, the calculation of the reputation score for a vehicle is based on the reports sent by its neighbors.

Roshan et al. have presented a routing strategy to detect and prevent malicious nodes in [9], the idea of the proposed strategy is based on double acknowledgement packet which means every intermediate node has to inform the source node that it has sent the packet forward. This process ends when the destination is reached. This method adds heavy overhead in the network and extra delay.

In [10], Sathish et al. proposed a novel strategy to reduce the impact of the single and collaborative black hole attacks. In their scheme, a fake RREQ is broadcasted with non-existing destination address. Any node replies to that RREQ is putted in black hole list. In this solution a cooperative black hole is those nodes that have a next hop node listed as black hole. The author proposed a second approach to prevent the black hole impact using digital signature and a trust value. The simulation results show that the proposed scheme creates extra delay.

In [11], Chaker et al. proposed a mechanism for the detection of intelligent malicious and selfish nodes using threshold adaptive control. However, direct and indirect trust are computed based on the number of legal and malicious actions. Direct trust is calculated between a node and its

neighbor. In the other hand, indirect trust is calculated based on the recommendation from one hop neighbors about other vehicles. But this fails if there is a collaborative black hole attack. P.S. Hiremath et al. proposed an adaptive system of fuzzy interference to detect and prevent the black hole attack. In [12], four input used for the Fuzzy Interference System (FIS): trust, data loss, data rate, and energy (characterize the quality of next hop neighborhood). These information are sent periodically by each node to update neighbor information. The system of fuzzy interference is used in the step of selecting of the next hop neighbor. This strategy is compared to an adaptive method [13] and the simulation results shows a better performance for the proposed solution.

In [14], Sagar R Deshmukh et al. proposed an AODV-based secured routing to detect and prevent single and cooperative black hole attacks. The authors idea is to attach a validity value to the RREP and keep the basic mechanism of AODV unchanged. The simulation results show a good performance against the black hole attack with negligible overheads compared to the normal AODV. However, in the presence of an intelligent adaptive black hole in the network, this method falls flat, hence, an intelligent malicious node could easily set the validity in the same way in which it claims that it has the shortest and the freshest route to a target node.

4. PROPOSED MYTHOLOGY

In the basic mechanism of AODV, when a source node has a data packet addressed to a destination node, the source node checks its routing table first which contains the next hop to use to reach the destination node. However, if a valid route is found, the source node sends the data packet to the next hop to forward it to the target node. If no route is found, the source starts route discovery phase and to find new route to the destination. The route discovery phase is initiated by broadcasting a route request message (RREQ). A route reply message (RREP) is sent back if an intermediate node has a valid route to the destination or the RREQ message reach the destination node itself. The solution proposed in this paper makes minor change in basic mechanism of AODV as shown in flow graph of figure 2.

In proposed strategy, Cyclic Redundancy Check 32 bits(CRC-32) [15] is used as hash function. However, as shown in figure 3, the only change made on the AODV message formats is the RREQ message format. In fact, the destination address field is replaced by its CRC-32 value which have the same length (32 bits) [6] that keeps the RREQ message format unchanged and it will not result any extra overhead.

In Accordance to the proposed method, before sending the RREQ, the source node stores the intended destination address and replace it by its CRC-32 value in the RREQ and broadcast it. If an intermediate node receives the RREQ, it sends back a RREP after setting the real address of the destination node only if it's the destination by comparing the CRC32 of its IP address with the destination node address set on the RREQ or, it has a valid route to the destination by comparing the CRC32 value of each route present on its routing table with the destination node address set on the RREQ. Otherwise, the intermediate node sends the RREQ message forward.

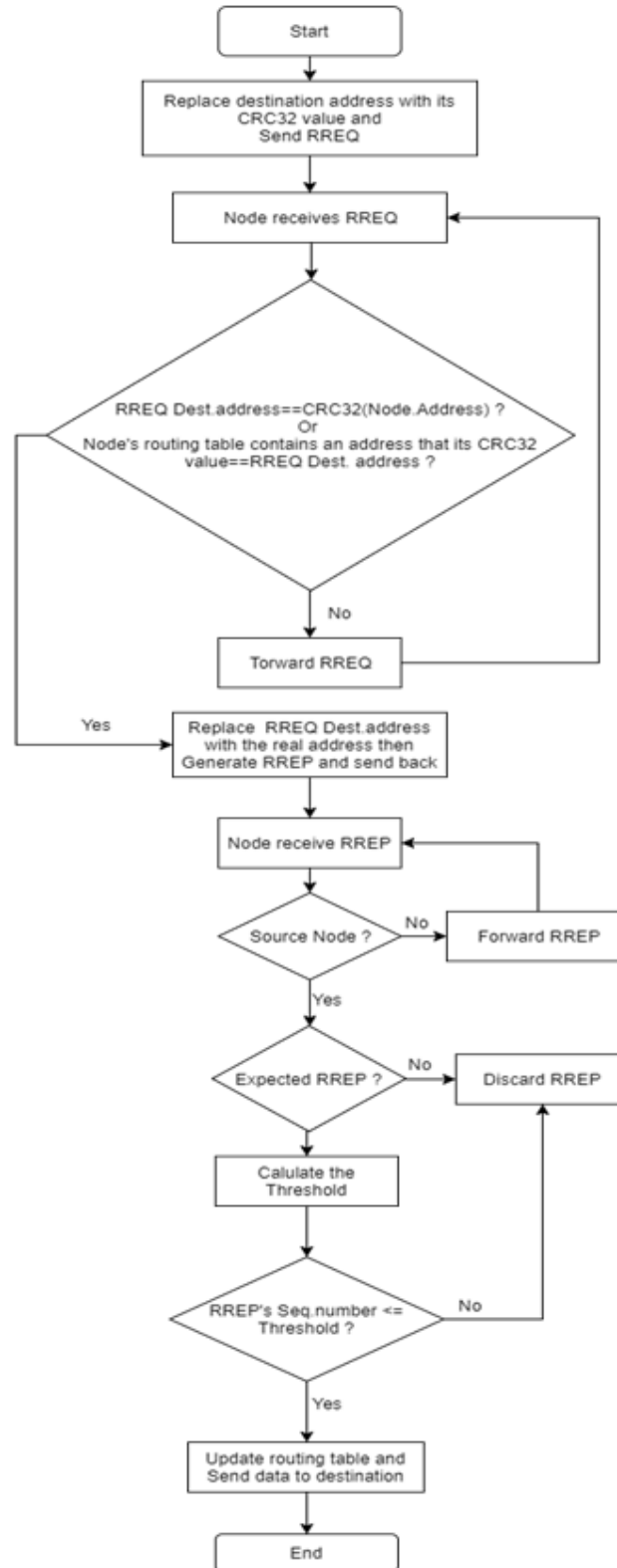


Figure 2. Flow graph of proposed method

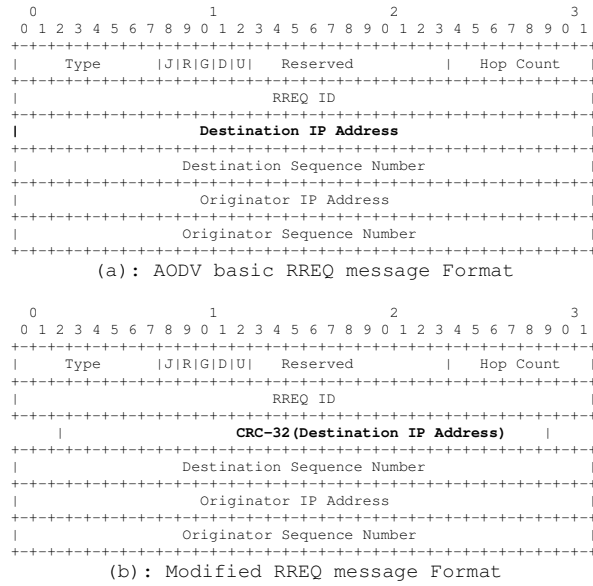


Figure 3. RREQ message format modification

However, for each RREP received, the source node applies two phases of checking:

- 1- If RREP's source address is not expected (not matching any destination address stored by the RREQ's source node), it will be rejected. Since, only malicious nodes reply for no existing target address.
- 2- If the RREP is legitimate then compare its sequence number to calculated threshold: if RREP's sequence number \leq threshold then the source node accepts the RREP and update its routing table, else, the RREP will be rejected. Where the threshold is calculated as following:

Threshold=*AVERAGE* (all received RREPs' sequence number) + *MIN* (all received RREPs' sequence number).

In the proposed scheme a well-known black hole attack will be prevented from the first phase, but an intelligent adaptive black hole can behave just like a genuine node by checking its routing table and send back a RREP with a high sequence number only if it has a route to the destination to be accepted as the freshest route to the destination which will be detected in the second phase.

This method can be used for single black hole detection and prevention as well cooperative black hole attacks, since, if a group of black hole are in collaboration, none of them can get the real address to the destination because the CRC32 is not reversible, hence, according to the proposed solution the unexpected RREP will be rejected.

5. SIMULATION RESULTS AND DISCUSSION

To evaluate the proposed solution, we relied on the NS-2 simulator [16] with the simulation parameters chosen as mentioned in the Table 1. To make further study, and simulation process and analysis we used Network Animator (NAM) [20] as shown in figure 4.

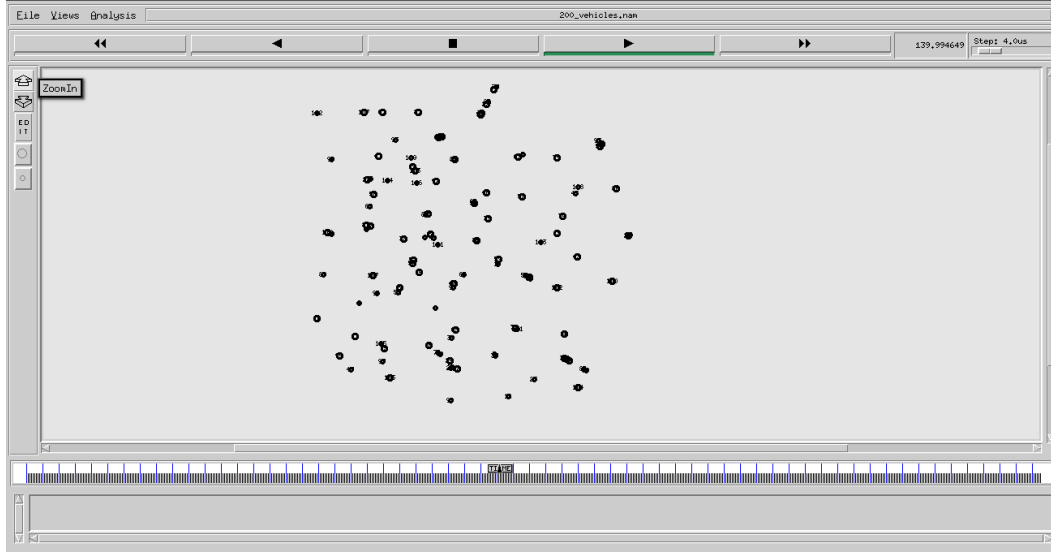


Figure 4: NAM output for the excerpt of the generated NS-2 trace

To generate vehicular traffic, we used SUMO [17] to create mobility traces based on real map (in our case Manhattan map) extracted from OpenStreetMap [18] as shown in figure 5.

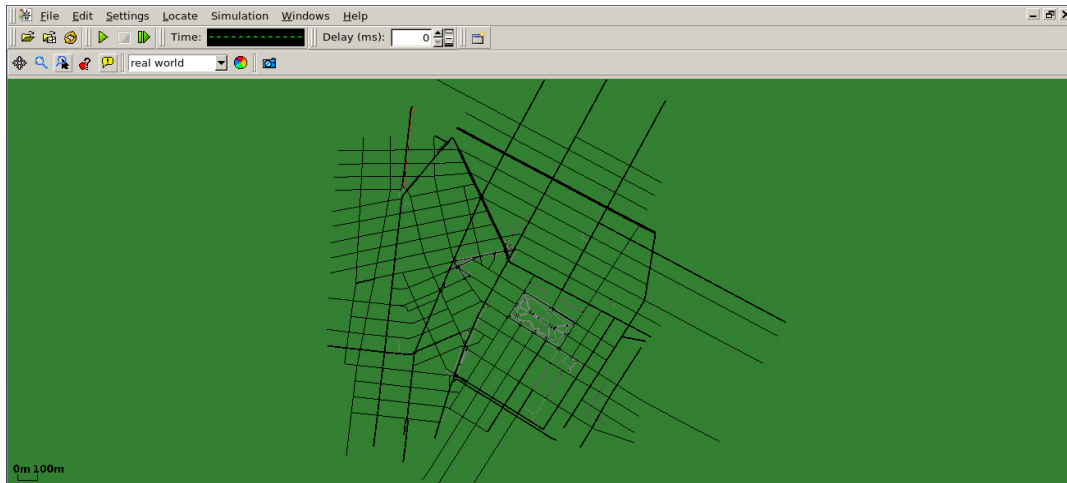


Figure 5: Extracted map from OpenStreetMap for the simulated scenario

Table1: Simulation Parameters

Parameters	Values
Simulator	NS2 (Version 2.34)
Simulation area (km x km)	2.5 x 2.5
Simulation time	300 s
Network interface type	WirelessPhyExt
MAC Layer	802.11
Movement Model	Manhattan Grid/Random way Point
Transmission range (m)	250
Permissible lane speed (km/h)	[0,80]
Number of vehicles	[100, 200]

Packet size (byte)	512
Traffic type	CBR
Packet Generation Rate	5 Packets per Second
Routing protocols	AODV, Proposed, [14]
Malicious Node	1

The efficiency of the proposed method is analyzed on the basis of four performance metrics, namely, throughput, packet delivery ratio (PDR), end-to-end delay (ETE) and routing overhead. In our simulation, the proposed scheme and [14] are simulated under an intelligent black hole attack and the results are compared with the fundamental AODV routing protocol.

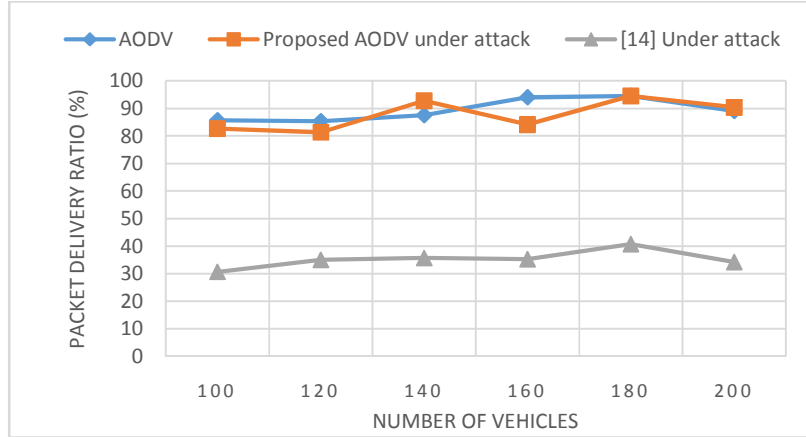


Figure6: PDR for varying number of vehicles under an intelligent black hole attack

As shown in figure 6, the packet delivery ratio of the proposed scheme is highly better than proposed solution in [14], moreover our proposed scheme has a PDR nearly equal to the fundamental AODV without attack.

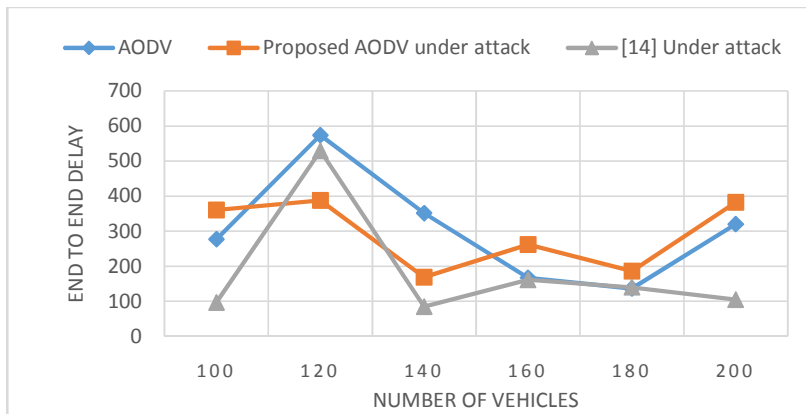


Figure 7: Average delay for varying vehicles density under an intelligent black hole attack

The figure 7 shows that based on our scheme, the end to end delay is comparable to AODV when there is no attack. The proposed solution in [14] shows the lowest end to end delay since the end to end delay is computed only for the received data packets, while the only received data packeted in [14] under an intelligent adaptive black hole attack are those when the source node and the destination are too close or neighbors otherwise these packets will be deleted by the black hole node.

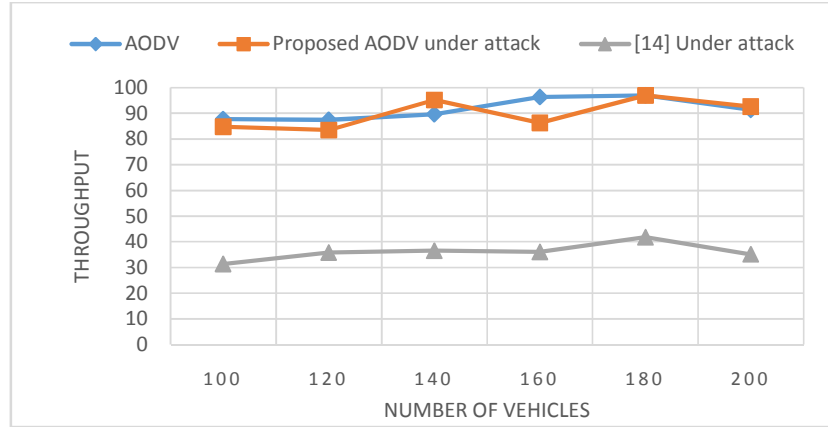


Figure 8: Throughput for varying number of vehicles under an intelligent black hole attack

The throughput of our scheme is nearly equal to the AODV and better than [14] as shown in figure 8.

The figure 9 shows that the routing overhead of our proposed scheme is comparable to AODV under normal condition (without attack) which is not the case with [14] in the majority of node density.

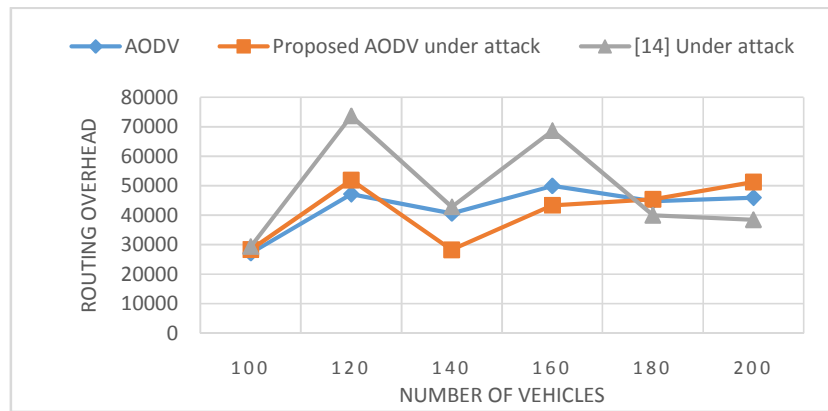


Figure 9: Routing overhead for varying number of vehicles under an intelligent black hole attack

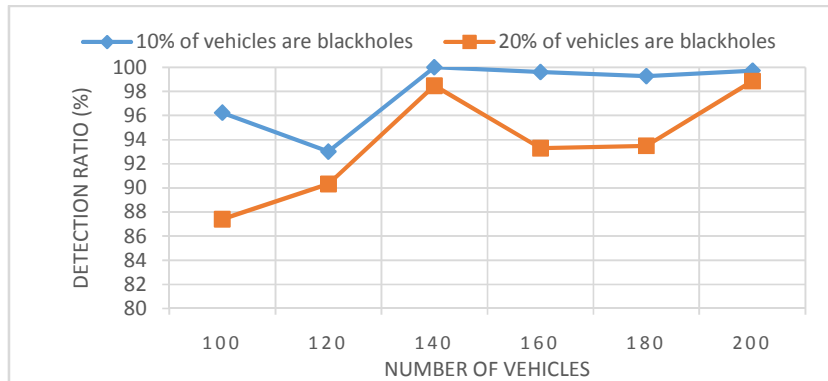


Figure 10: Proposed strategy detection ratio

The figure 10 represent intelligent black hole attacks detection abilities by our proposed scheme. Resulted curves shows that even in the presence of a high number of intelligent adaptive black hole attacks our proposal can ensure a high detection ratio exceeding the 85%.

So, from previous Figures and according to the positive simulation results it can be observed that, in the case of an intelligent adaptive black hole attack our scheme works well against the intelligent adaptive black hole attacks in vehicular networking.

3. CONCLUSIONS

With the emergence of newer security solutions, different kind of threats emerge as well. In this paper, Intelligent Black hole attack is discussed and prevented via our proposed strategy. The simulation results proved the efficacy of the proposed solution since it has the ability to ensure high packet delivery ration and throughput with nearly the same end to end delay and routing overhead compared to the fundamental AODV. Moreover, a high detection ratio is offered by the proposal in low and high vehicles density.

Furthermore, the proposed strategy is compatible with other reactive routing protocols, so, for future work we plan to implement and evaluate the performance of our scheme for other reactive protocols such as Dynamic MANET on demand (DYMO) routing Protocol and evaluate its performance under similar attacks such as the Grey hole attack.

REFERENCES

- [1] Vehicule to vehicule communication. Available online: <https://www.nhtsa.gov/technology-innovation/vehicle-vehicle-communications> (accessed on April 2017).
- [2] Elias C. Eze, Sijing Zhang and Enjie Liu, "Vehicular Ad Hoc Networks (VANETs): Current State, Challenges, Potentials and Way Forward", Proceedings of the 20th International Conference on Automation & Computing, Cranfield University, Bedfordshire, UK, 2014.
- [3] Surmukh, S.; Kumari, P.; Agrawal, S. Comparative Analysis of Various Routing Protocols in VANET. In Proceedings of 5th IEEE International Conference on Advanced Computing & Communication Technologies, Haryana, India, 21–22February 2015.
- [4] Sabih ur Rehman, M. Arif Khan, Tanveer A. Zia, Lihong Zheng, "Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges", Journal of Wireless Networking and Communications, 2013, pp. 29-38.
- [5] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing", Proceedings of IEEE Workshop on Mobile Computing Systems and Applications 1999, February 1999, pp. 90-100.
- [6] C. Perkins, E. Belding-Royer and S. Das, "Ad Hoc On-Demand Distance Vector (AODV)Routing", Network Working Group, Request for Comments, 2003.
- [7] Halabi Hasbullah, Irshad Ahmed Soomro, Jamalul-lail Ab Manan, "Denial of Service (DOS) Attack and Its Possible Solutions in VANET", International Scholarly and Scientific Research & Innovation 4(5) 2010, World Academy of Science, Engineering and Technology, Vol:4 2010-05-25.
- [8] R. Khatoun, P. Guy, R. Doulami, L. Khoukhi and A. Serhrouchni, "A Reputation System for Detection of Black Hole Attack in Vehicular Networking," International Conference on Cyber Security of Smart cities, Industrial Control System and Communications (SSIC), 2015.

- [9] Roshan Jahan, Preetam Suman, "Detection of malicious node and development of routing strategy in VANET," 3rd International Conference on Signal Processing and Integrated Networks (SPIN), IEEE, pp. 472-476, 2016.
- [10] Sathish M, Arumugam K, S. Neelavathy Pari, Harikrishnan V S, "Detection of Single and Collaborative Black Hole Attack in MANET," International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), IEEE, pp.2040-2044, 2016.
- [11] Sathish M, Arumugam K, S. Neelavathy Pari, Harikrishnan V S, "Detection of Intelligent Malicious and Selfish Nodes in VANET using Threshold Adaptive Control," 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA), IEEE, 2016.
- [12] P.S Hiremath and Anuradha T, "Adaptive Fuzzy Inference System for Detection and Prevention of Cooperative Black Hole Attack in MANETs", International Conference on Information Science (ICIS), pp.245-251, 2016.
- [13] P.S Hiremath and Anuradha T, "Adaptive Method for Detection and Prevention of Cooperative Black Hole Attack inMANETs", International Journal of Electrical and Electronics and Data Communication, Volume-3, Issue-4, pp.1-7, 2015.
- [14] Sagar R Deshmukh, P N Chatur, Nikhil B Bhople," AODV-Based Secure Routing Against Blackhole Attack in MANET", IEEE International Conference On Recent Trends in Electronics Information Communication Technology, India, pp. 1960-1964, 2016.
- [15] Cyclic Redundancy Check (CRC) RFC. Available online : <https://tools.ietf.org/html/rfc3385> (accessed on Mars 2016).
- [16] Network Simulator- NS-2. Available online: <https://www.isi.edu/nsnam/ns/> (accessed on 5 May 2017).
- [17] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "Sumo–simulation of urban mobility", in The Third InternationalConference on Advances in System Simulation (SIMUL 2011), Barcelona, Spain, 2011.
- [18] Open street map. Available online: <https://www.openstreetmap.org/> (accessed on Mars 2017).
- [19] Heithem Nacer and Mohamed Mazouzi, "A Scheduling Algorithm for Beacon Message in Vehicular Ad Hoc Networks",International Conference on Hybrid Intelligent Systems (HIS 2016),Marrakech, Morocco, pp. 489-497, 2016.
- [20] Sirwan A.Mohammed and Sattar B.Sadkhan, "Design Of Wireless Network Based On Ns2", Journal of Global Research in Computer Science (jgrcs), Volume 3, No. 12, December 2012.

COGNITIVE RADIO AND RADIO FREQUENCY IDENTIFICATION TECHNOLOGIES IN SMART ENVIRONMENT

Roa Alharbi

Department of Computer Engineering,
University of Western Ontario, London, Canada

ABSTRACT

In this survey, smart environment wireless networks are reviewed. The focus is on using the Cognitive Radio (CR) technology and Radio Frequency Identification (RFID) technology in these smart networks. Therefore, the reviewed research papers are studying the Cognitive Radio usage in smart homes and hospitals wireless networks. The main objectives of using CR in wireless networks are providing the flexibility in networks allocation, managing wireless networks efficiently and saving time and cost for communications. In addition, the papers include how the Radio Frequency Identification technology is merged with the Cognitive Radio to produce a smart environment. Although new technologies like CR and RFID have advantages, they also have disadvantages such as network interferences, network allocation and users' priorities management. For this reason, recent studies are describing the challenges that facing CR and RFID technologies and new ways to solve them.

KEYWORDS

SDR, Cognitive Radio

1. INTRODUCTION

The smart environment is a small world that includes all person's requirements in a fast and comfortable way. This small world has smart devices that are continuously working to get those requirements anytime and anywhere. There are three different types of smart environment: virtual computing environment, physical environment and human environment. Initially, virtual computing environment is a virtual world which allows smart devices to access specific services. Secondly, physical environment includes various types of smart devices such as tags, controllers and sensors. Thirdly, human environment where the human is included in this technology, for example using mobile phones and other devices.

Focusing on physical environment, there are several technologies to build this kind of environment. Software Defined Radio (SDR) technology is one of the technologies. To explain, SDR is defined by the Institute of Electrical and Electronic Engineers (IEEE) as a "Radio in which some or all of the physical layer functions are software defined"[1]. So that, SDR makes

Natarajan Meghanathan et al. (Eds) : NeTCoM, CSEIT, GRAPH-HOC, NCS, SIPR - 2017
pp. 37– 44, 2017. © CS & IT-CSCP 2017 DOI : 10.5121/csit.2017.71504

the communication more flexible by modifying radio devices. Moreover, using Software Defined Radio technology imports the cost efficiency in the communication business area. In general, any device that uses radio frequency (FR) spectrum to transfer and receive signals in a wireless network is called a “radio”. Radio devices are used today as cellphones, televisions and computers. Further, SDR technology leads to three related technologies which are Adaptive Radio, Cognitive Radio and Intelligent Radio. Adaptive Radio technology enables communication systems to control their performance and edit their operating features like frequency, data and power. However, communication systems that use Cognitive Radio know their location in RF spectrum and they are designed to decide the best wireless channel and change their internal state. Intelligent Radios are cognitive radios but they use machine learning technology to improve their performance. [2]

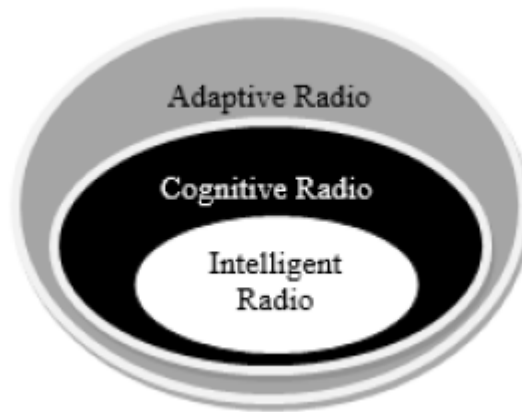


Figure 1.SDR Related Technologies [1]

Another related technology to the SDR is the Radio Frequency Identification (RFID). RFID is a wireless communication technology which enables the identification of objects with specific tags [8]. The RFID system contains of tags (electronic labels) on objects, reader (integrator) and information stored in the system's database. Each tagged object has a memory chip that saves object's identifiers such as the unique Electronic Product Code (EPC), time stamp, read count, radio frequency and received signal strength indicator [9]. In addition, the reader is connected with an antenna emits signals to the tag on the object, which distributes this signal with its ECP. In detail, tags could be active, passive or battery-assisted passive. These three kinds differ in their batteries, the active tag has its own on-board battery. The battery-assisted passive has a small on board battery that activated when it is connected with reader. However, the passive tag has no battery and it has to use radio energy to work. Further, tags could be read-only tag that are programmed from the factory and could not be changed. They could be read/write tags, which enable the end user to program specific function on these tags. RFID tags are composed of two main parts, the integrated circuit and antenna. The integrated circuit is used to process information and the antenna is used to receive and transfer signals. Similarly, readers depending on associated tags have three different types: Passive Reader Active Tag (PRAT), Active Reader Passive Tag (ARPT) and Active Reader Active Tag (ARAT). In PRAT system, the passive reader receives signals from the active tag, which transmits signals only. However, the active reader in the APRT system transmits signals and receives information from passive tags. The ARAT system has active readers activated with active tags to send and receive information [8]. Important to realize, RFID frequency bands is classified into different ranges. For example, smart

cards utilize 13.56 MHz (HF) frequency band and the range for that 10 centimetres to 1 meter. Also, Bluetooth standards use 2450-5800 MHz that range from 1 to 2 meters [3].

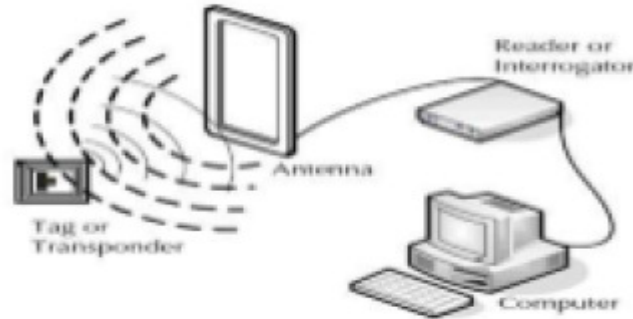


Figure 2: RFID

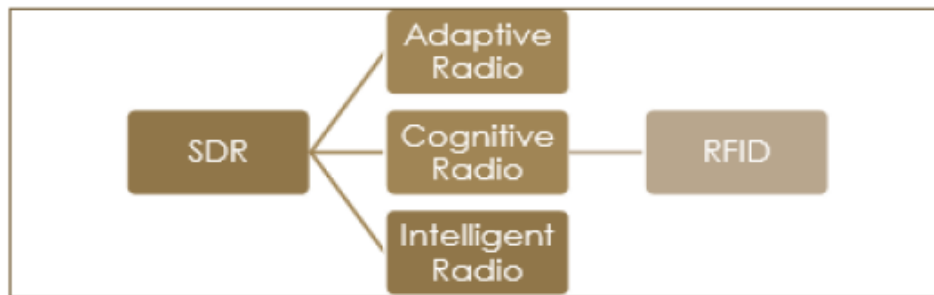


Figure 3: Survey Paper Classification

The above classification is important to understand the proposed survey paper. The SDR technology, CR technology and RFID technology are three related technologies in smart environment wireless networks. In this survey paper, I am focusing on CR study area because it is an essential technique to produce flexible wireless access, especially in large networks that are surrounding with many devices and application. This area is changing rapidly, so we as engineers must be aware of these changes and be part in introducing an improved version of these techniques.

2. COGNITIVE RADIO TECHNOLOGY IN SMART HOMES NETWORKS

The Using Cognitive Radio (CR) technology in building smart homes would produce better and more cost efficient environment. Cognitive Radio enables users to connect to several wireless technologies at the same time [10]. Also, users can move between these technologies easily. Further, CR technology helps in adapting to channel conditions, declining packets loses and changing in modulation. These features leads to increase energy efficiency in smart home network. Although Cognitive Radio technology provides flexibility in the management of wireless sensor networks in smart homes, it faces some challenges such as the emitted interferences and the indoor penetration losses. According to Per Lynggaard and Knud Erik Skouby in the article “Deploying 5G-Technologies in Smart City and Smart Home Wireless Sensor Networks with Interferences”, they state that it has been proven in previous studies that

the interference is a big challenge in smart homes' networks [4]. For instance, using the IEEE standard in the WIFI access point offers 14 channels in the 2.4 GHz and each channel is 22 MHz wide distributed by 5 MHz. In this case, an overlap is resulted. So that, CR technology is used to subdivide spectrum access intelligently to decrease overlapping. This solution has been studied by Cavalcanti, and he mentioned in his study that there is an obvious improvement in allocation channels by using CR in smart homes. To clarify, CR connects all infrastructure elements for smart home by multi-hop and pervasive techniques. These elements are able to transfer big information using band allocation which allows high bitrate transferring. As a result, emitted interferences in smart home networks could be decreased using CR technology [11]. Another key point, the indoor penetration losses challenge could be solved with the CR technology. To explain, it has been found that penetration losses depend on wall thickness and type. For example, a 12 cm thick uniform plaster wall would have penetration losses in the range of 5 to 10 dB. As a solution, there are two options, one option is to increase the transmit power by reducing the Bit Error Rate (BER). The other option, is to decrease the BER by programming error correcting coding (pre-coding); however, this technique could affect the bandwidth because the pre coding generates overhead information. In the above study, the authors proved by simulations that deploying CR technology in smart home networks decrease the mentioned challenges. These simulations compares commonly used networks in smart homes with the one using CR. They found that using CR technology saves 10% power and 7% bandwidth.

Also, battery life for the smart home network could be extended to 26% with using CR in these networks [4].

3. COGNITIVE RADIO AND RADIO FREQUENCY IDENTIFICATION IN SMART HOSPITALS

In recent years, using wireless communication in hospitals has been a popular trend. New technologies are used in hospitals in monitoring patient's status such as blood pressure, heart been and temperature [5]. These technologies must be connected to each other to transfer patient's information through trusted wireless networks. However, wireless communication in hospitals challenges two key issues. First, the electromagnetic interferences that could influence the bi medical devices' performances. Second, the wireless channel allocation depending on devices' priorities. Speaking about these issues, there are two types of the spectrum sharing in the wireless network. The first kind, is the Horizontal Spectrum Sharing, which is accessing the unlicensed band by the radio. In this type, Cognitive Radio is used to improve the usage of the spectrum by devices in an efficient way. The other kind, is accessing the licensed band by the radio, which is called the Vertical Spectrum Sharing. In this case, Cognitive Radio is used by the secondary device (low-priority device) to access a licensed spectrum assigned to a primary device (high-priority device). Moreover, medical devices could be passive or active. Passive devices do not transmit wireless signals while Active devices transmit wireless signals and they could be interfered by other device [12].

In "A Cognitive Radio System for E-Health Applications in a Hospital Environment" paper, the authors focused on two active applications real-time non-critical telemedicine and hospital information system [6]. Telemedicine applications include remote diagnosis, consultation and patients' information transformation. While hospital information system manages patients and staffs data and stores them in hospital's database. For this study, the telemedicine is treated as the primary user and the hospital information system is treated as the secondary user of the wireless

network. To clarify, the architecture of the Cognitive Radio System proposed in this paper includes an inventory system, a cognitive radio and cognitive radio clients. Initially, the inventory system is used to maintain hospital's devices information such as location, electromagnetic capability requirement and activity status. These information should be tracked using tracing system. In this case, an attached RFID tags on devices are used for the tracking system that supports the inventory system in the smart hospital. Also, RFID reader are installed among the hospital to track these tagged devices and send information to the inventory system. Secondly, the cognitive radio system uses control channel and a data channel to operate. Further, interference avoidance approach is used for the wireless access. Thirdly, cognitive radio clients, every CR client transmits its information to the CR controller. Then, the CR controller uses the information from the inventory system to control those clients. The CR controller has two interfaces, one for the control channel and the other is for the data channel. So that, it can transmit/ receive data to/from both channels at the same time. However, the CR client has one interface to transmit/receive data to/from one of the two channels (control channel, data channel) at a time. Equally important, this study focuses on improving the Electromagnetic Capability requirement, for example the device used in wireless network must limit the transmit power to decrease interferences with other devices. Moreover, the study takes in consideration the Quality of Service of the application, such as loss or delay are factors for measuring the Quality of Service. The study was performed in an area of 27 m², and it is divided into nine areas, as shown in Fig. 4.

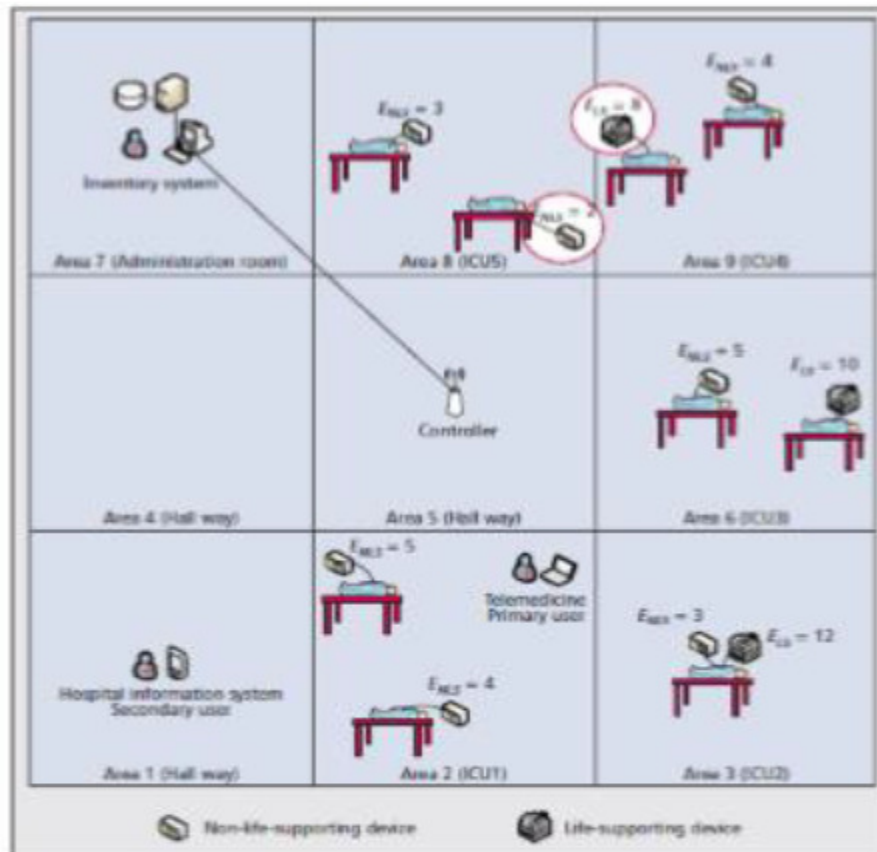


Figure 4: Cr System in Hospital [6]

In this study, the authors include two major performance measures, the outage probability and the interference probability. The outage probability is the probability of the strength of the received signal is less than -65 dBm that is the minimum level for decoding in the controller. The interference probability is the probability that an interference happens, which occurs when the transmit level is higher than the acceptable level. As a result, in the CR system proposed, they found that the interference probability decreased 99.98 % but the outage probability resulted is greater than the traditional wireless systems. Overall, the performance results of the proposed schema show that using CR technology in hospitals wireless networks protects the bio-medical devices from harmful electromagnetic interference. Also, the allocation performance improved by using this schema [6].

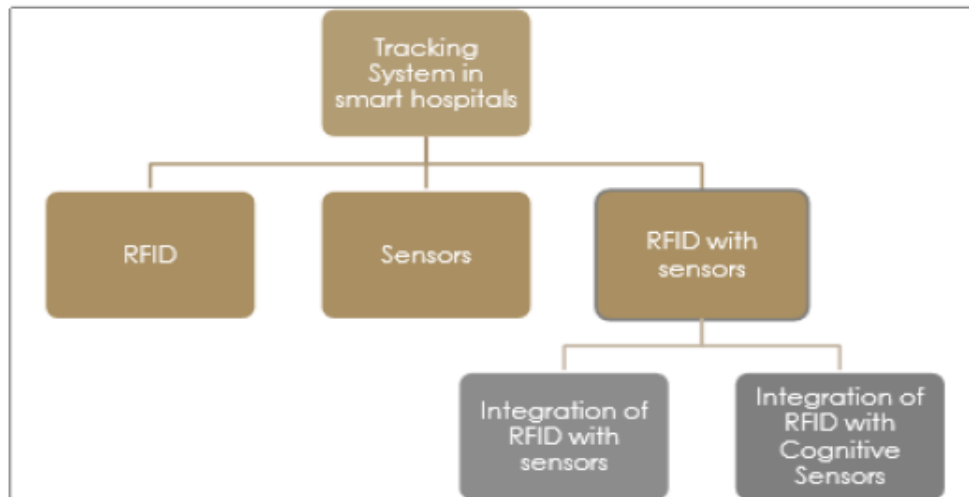


Figure 5: RFID Classification

A number of studies include integrating RFID with smart wireless networks. RFID is utilized in hospitals networks to track equipment, identify patients and improve patients care. As shown in figure 5, tracking system in smart hospitals could be done using RFID with sensors. With integrating the RFID technology with cognitive sensor, the performance of the system will be enhanced and the quality of service will be improved. Further, medical errors could be declined by using RFID. So that, each patient would be connected to his/her medicine prescription wirelessly without the need for paper prescriptions. Another important point, cloud-assisted Tracking System in smart hospitals RFID Sensors RFID with sensors Integration of RFID with sensors Integration of RFID with Cognitive Sensors integrated RFID with integrated RFID tags are useful for memory lose patients. In this technique, information is sent to doctors remotely from other places to track the patent and insure patent's safety. Also, it offers real time responses and stores patent's history with updating it each time. However, collision issue could appear with RFID technology. In this case, RFID protocol in reading tags should be developed to decrease delay as well as collision. Also, privacy could be harmed in this kind of systems. So that, restricted information security should be included. For example, a cryptography method could be used to encrypt patient's information. In this way, patient's information would be secure when transferring information among the wireless network [7].

4. CONCLUSIONS

To sum up, a Cognitive Radio technology in smart homes wireless network is proposed, with taking in consideration, two main challenges which are the emitted interferences and the indoor penetration losses. I believe that using CR technology in communication networks adds more efficient features to these networks. Also, it saves money by reducing networks deployment costs. Moreover, the survey paper includes challenges that face smart hospitals networks. These issues are the electromagnetic interferences and the network allocation depending on users' priorities. Besides the CR technology, the RFID technology is used in these networks to track devices. As a result, there is a big improvement in networks performance with using these technologies in smart hospitals. Overall, The CR technology in smart homes and hospitals manages the network usage by categorize users as primary and secondary. This approach controls the wireless network professionally with avoiding interferences. In addition, it manages spectrums efficiently and provides users more flexibility in smart environments.

For future, Cognitive Radio system can be improved by adding improved multichannel protocols. Further, prioritization of primary and secondary devices could be controlled by stronger algorithm to gain a better Cognitive Radio system. Finally, the administration unit for the Cognitive Radio systems must control and limit number of primary users to avoid interferences in the smart environment's wireless network.

REFERENCES

- [1] B. S. W. Group, "Base Station System Structure," Jan. 2010.. [Online].
- [2] V. Fabrizio, "Softwae-Defiend Radio," IEEE vehicular technology magazine, pp. 71- 82, May 2013.
- [3] R. Parada , J. Melià-Seguí, M. Morenza-Cinos, A. Carreras and R. Pous, "Using RFID to Detect Interactions in Ambient Assisted Living," IEEE Computer Society, pp. 16-22, Jul. 2015.
- [4] L. Per and K. E. Skouby, "Deploying 5G-Technologies in Smart City and Smart Home Wireless Sensor Networks with Interferences," Springer Science Business Media New York, Mar. 2015.
- [5] Y. Pu, W. Wang and Q. Xu, "Emerging Cognitive Radio Applications: A Survey,," IEEE Communications Magazine, pp. 74-81, Mar. 2011.
- [6] P. Phunchongharn and E. Hossain, "A Cognitive Radio System for E Health Applications in a Hospital Environment," IEEE Wireless Communications, pp. 20-28, Feb. 2010.
- [7] G. Prasad Joshi, S. Acharya, K. Chang-Su and K. Byung-Seo, "Smart Solutions in Elderly Care Facilities with RFID System and Its Integration with Wireless Sensor Networks," International Journal of Distributed Sensor Networks, vol. 2014, Aug 2014.
- [8] K. Finkelzeller, The RFID Handbook, 2nd ed., John Wiley & Sons, 2003.
- [9] M. Weiser, "The Computer for the 21st Century," Scientific Am., vol. 265, no. 3, 1991, pp. 94–104.
- [10] R. Want et al., "Bridging Real and Virtual Worlds with Electronic Tags," Proc. ACM SIGCHI, ACM Press, 1999, pp. 370–377.
- [11] K. Finkelzeller, The RFID Handbook, 2nd ed., John Wiley & Sons, 2003.

[12] R. Want, “Enabling Ubiquitous Sensing with RFID,” *Computer*, vol. 37, no. 4, 2004, pp. 84–86.

AUTHORS

Roa Alharbi

- Researcher at KACST
- Bachelor degree in Information technology, King Saud University
- Master of Engineering in Software Engineering, The University of Western Ontario

DISTANCE LEARNING VIA SOCIAL MEDIA

Mohammad Derawi

Smart Wireless Systems,
Norwegian University of Science and Technology, Norway

ABSTRACT

In this research work, we examine one of the most applied networking website, namely the Facebook, for conducting courses as a replacement of valuable classical electronic learning platforms. At the initial stage of the Internet community, users of the Internet used email as the main communication mean. Even though email is still the indispensable approach of communication in a appropriate but offline mode, other services were presented, such as many Instant Messaging (IM) software applications like ICQ, Skype, Viber, WhatsApp, Instagram, Musical.ly and Messenger, which let people connect in a real-time mode. Nevertheless, the communication between people was further improved to the next phase, when Facebook came to reality as a social networking homepage that supports many features. People do not only link with others, but also establish all kinds of connections between them. Facebook offers rich functionalities for forming associations. The framework of Facebook delivers without charge software that were provided by traditional electronic learning. This research work looks at how people apply Facebook for teaching and learning, together with recommendations provided.

KEYWORDS

E-Education, Distance Learning, Social Network Services, Facebook

1. INTRODUCTION

The Internet today provides software applications of the necessary communication media for computation purposes. Due to its fame, it has become a need of modern individuals for communication and information sharing purposes. For example, the usual Internet users are using email as a replacement of sending letters via postal [1]. Although emails arrive at the mailboxes of recipients instantly, emails are to be read only when the recipients check their accounts. At the early stage, computers allow instant messaging among Internet users using software talk on UNIX operation system. It enables Internet users to communicate in real-time by sending textual data character by character. However, these applications were not popular among casual Internet users, because they must access to host machines [2].

The extensive use of Facebook is not only due to its popularity, but also due to the support by various devices. Facebook is a web application that can be accessed via any web browser. Besides, many mobile phones are equipped with web browsers, such as Opera Mini (a mobile phone version of Opera web browser), and some are even equipped with dedicated software solely for accessing Facebook, such as Apple iPhone, Samsung, Ultra-mobile PC's, various netbooks and the Apple iPad. The support of Facebook by these mobile devices is a definite advantage of using Facebook for education purposes[3].

2. THE ROLE OF FACEBOOK

Facebook is a social networking web application that supports the following functions, which are for education purposes[4][5]:

- *No Cost* - The use of most social media sites including Facebook are free of charge.
- *No prerequisite* - Any Internet user with a valid email address is allowed to register
- *Group* - It supports user-defined groups so that users can be divided into groups. There are private groups and public groups. The former can only be joined by users via invitation and the latter is open to all. On the other hand, Facebook page enables any student to join the page for accessing the teaching materials and to be notified by any update of the page.
- *Page* – It enables users to create Facebook pages for particular organizations, so that other users can join the group and will be informed of all updates to the Facebook pages.
- *Privacy* - It supports the control of privacy in terms of items posted, users and groups. In other words, it is possible to set the access control privileges of individual items posted, users and groups.
- *Notifications* - It supports user notifications of all updates of items, users and groups via emails. If there is any update of an item, a user or a group, emails are sent to the related users for notifications.
- *Photo albums* - It supports user and group level photo albums.
- *Discussions* - It supports discussions with respect to a message, a photo, a photo album or an article.
- *Emails* - It supports internal emails between any two Facebook users, and it is possible to send an email to all users of a group.
- *Events* - It supports events and is possible to create events for a group. Users to indicate whether they will be present or absent from the events.
- *User main page* - The main page of a Facebook user shows all the updates to friends, the groups joined, and all the upcoming events.
- *Chatting* - Facebook support real-time chatting through the web browser.
- *User-defined software* – There is a well-defined Facebook API (Application Program Interface) so that software developers can develop software to be executed within the Facebook webpage. For example, quiz creator software enables any Facebook user to create a survey, questionnaire or quiz easily. Furthermore, applications for file sharing allows users to share their own documents with any other users. Besides, some Facebook applications are educational [10] .
- *Activity log* – All operations by any Facebook user are logged with timestamps and can be traced.

- *Live Video* – On April 6 2016 last year, Facebook started this extremely great service, where you have real-time video conversations with others. A fascinating service.

3. FACEBOOK AS AN EDUCATIONAL PLATFORM

It is conceivable to use Facebook as a social network for education purpose as follows:

- *User creations* - Teaching staff and students need to access the Facebook website for registration. Preferably, they all use their email accounts granted by the universities, so that it is easier for them to locate one another. Furthermore, each of them can keep their own personal Facebook accounts for their own casual uses, whereas the Facebook student users created by using university accounts are for teaching and learning only if they would like to prevent lectures from accessing their private life in the social networking website. The limitation is that the students may not log on their Facebook that is associated with their university email account daily.
- *Course preparations* - Teaching staff can create a Facebook page for each course with their Facebook accounts. Each Facebook page can create multiple photo albums and multiple discussions. Therefore, teaching staff can make use of the facilities provided by Facebook to enrich their Facebook page for the course, such as adding links to references materials, discussions or photo albums.
- *Teaching materials preparation* - For teaching purposes, the most important teaching materials to be distributed are lecture notes or slides. Usually, teaching staff uses Microsoft PowerPoint to prepare the PowerPoint files for students to download. Although there are free Microsoft PowerPoint viewer applications for Windows platforms released by Microsoft, there are platforms and mobile devices that cannot display PowerPoint files properly. Instead, image file format is the universal format for display purposes. It is therefore preferable to convert all PowerPoint files into sequences of images, and upload them as Facebook page photo albums. There are freeware applications that can convert Microsoft Office files into sequences of images. Then, Facebook users will be notified the existing of new slides, which can be accessed by any web-browsing enabled devices. For presentation files other than Microsoft PowerPoint, lectures can also using different applications to convert the files into images for uploading. Most mobile devices can be used for web browsing. Some mobile phones, such as Apple iPhone, are equipped with dedicated components for accessing Facebook. With the existence of mobile network technologies, such as GPRS and HSDPA, students can view the lecture notes as photo albums on the Facebook page for the course anywhere. The teaching materials in Microsoft Office formats can be uploaded to a web server and their URLs can be posted to the Facebook pages. As a result, Facebook student users can determine whether to download the original files. Besides, it is possible to post links of videos or upload video files to the course Facebook page, such as the videos for the lectures or demonstrations.
- *Conducting lectures and tutorials* - Teaching staff can use the PowerPoint or other presentation files to conduct lectures and tutorials. With Facebook, they have an alternate way to present the notes, which is showing Facebook photo albums for the presentation files. There is an extra benefit of showing a photo album compared with presenting a presentation file, which supports discussions on the entire photo albums and individual slides. Furthermore, while showing a slide as Facebook image, students can add comments to the slide which will notify the teaching staff the existence of comments for immediate feedbacks. It facilitates the discussions among teaching staff and students, especially those who are unwilling to speak in front of other students. Furthermore, if a

student has any problem on any slide, he or she can add a comment, and a notification email will be sent to the teaching staff. Then the teaching staff can simply click the link embedded in the email to locate the slide (image) the student mentioned and provide feedbacks.

- *Discussions* - Whenever there is any update to the course group or course page, all involved Facebook student users are notified and can access those changes, such as a posting of links referring to online reference materials, videos and a creation of photo albums. Then, all users can access to those items and leave comments which can be read by other users for discussions. By consolidating the reference materials which originally scattered in the Internet, students time for searching the materials by themselves can be saved. For example, lecture notes can be released as Facebook photo albums, so that all students can access these albums for viewing them. Whenever they have any comments or questions regarding any slides, they can leave comments or questions to them. Teaching staff and other students will be notified of such comments or questions by emails, and leave responses on the slide. Since Facebook is informal, users are more willing to leave messages on them. It actually motivates students to share and discuss for peer-to-peer learning. In fact, there are many interactive applications developed for Facebook. Lectures can make appropriate use of those external applications to facilitate interactions among lecturers and students.[6]
- *Assessments* - Facebook provides application programming interface (API) for software developers to develop Facebook applications. As such, there have been a lot of applications available for Facebook users. There are several Facebook applications which enable Facebook users to create quizzes, such as the Quizzes and Quiz Creator applications. By using these software, teaching staff can create a quiz, such as for each lecture, and post the link to the course page, and inform students to take the quiz to examine their understandings on the course materials. In addition, file sharing applications allow students submit assignments to teachers easily. As Facebook can be accessed by any web browser, students can increase their understanding on the course materials, anytime and anywhere. [7]
- *Personal notes and private files* - Students can make use of notes function in Facebook to keep their personal study notes. They can either keep the notes private or share the notes with others. Private files can be sent using the private message function with attachment. [8]
- *Privacy, security and legal issues* - Facebook provides customization in course account setting that protect privacy and ensure security of course access. The course creator can set the access of content to their students only by using the “add friend” function and “controlling how you share” function properly. Account and privacy setting can be performed under the “Account” session in Facebook. Regarding the legal issues of posting teaching materials in the social networking website, the lecturers should well aware of the terms and agreements listed in Facebook. By using Facebook appropriately, education functions can be delivered via this platform effectively.[9]

4. CASE STUDY

In this case study, a course is used for illustration purposes. Upon the creation of Facebook account by a teaching staff, the lecturer can create a Facebook page for the course with the given course code. For creating the course account, the teaching staff, clicked the Drop down arrow and "Create Page" to create a new page for the course as shown in Figure 1

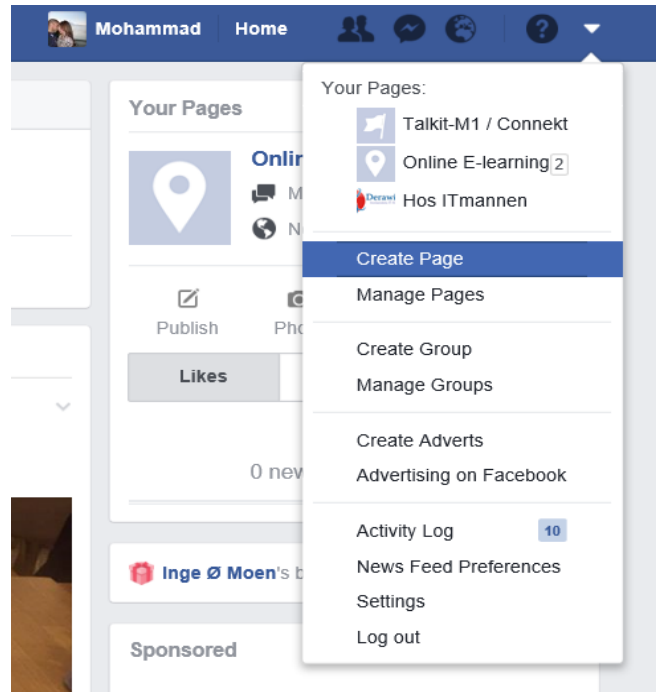


Figure 1. Facebook page for personal profile creation

By clicking “Create Page to start creating the page for the course”, the teaching staff can specified the course details on the webpage as in Figure 2 below. Finally, the teaching staff clicked “Create Page” to create the course page. Then, the lecturer could create photos albums for the lecture notes. The lecture clicked “Photos” to create a new photo album.

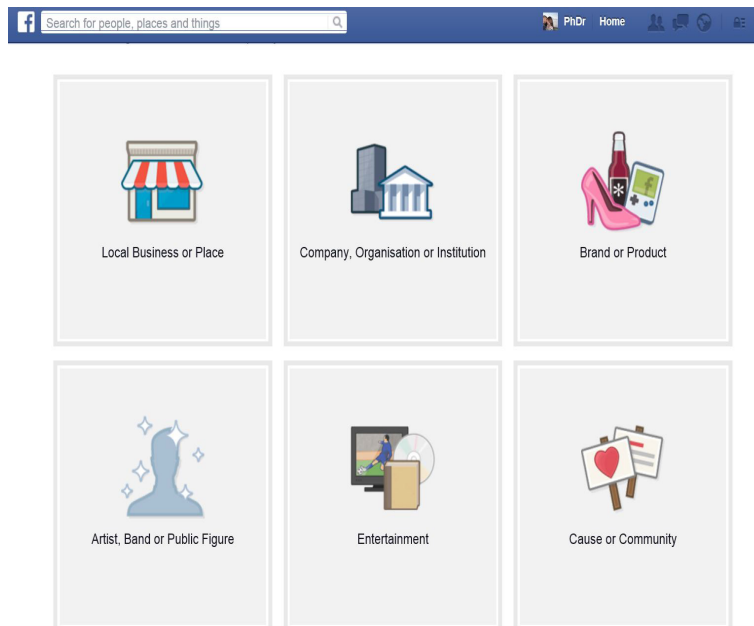


Figure 2. Facebook page for course main menu

The lecturer then started uploading the lecture notes images to the photo album. Since different web browsers support different approaches of uploading images to a photo album, for example, Microsoft Internet Explorer and Google Chrome can make use of a Facebook plugin whereas Firefox uses a Java based component, the lecturer would experience different interface when using different web browsers. Once the photo album was created, the lecturer reviewed the images and rearranged the sequence of the images as necessary. Then, the photo album with lecture notes was ready to be accessed by students.

Set up Online E-learning

1 About 2 Profile Picture 3 Add to Favourites 4 Reach More People

Add categories, a description and a website to improve the ranking of your Page in search.
Fields marked by asterisks (*) are required.

Course Wireless Systems

Add a few sentences to tell people what your Page is about. This will help it show up in the right search results. You will be able to add more details later from your Page settings.

155

*Tell people what your Page is about...

Website (e.g.: your website, Twitter or Yelp links)

Choose a unique Facebook web address to make it easier for people to find your Page. Once this is set, it can only be changed once.

http://www.facebook.com/wirlessonline

Is Online E-learning a real organisation, school or government? ☐ Yes ☐ No
This will help people find this organisation, school or government more easily on Facebook.

Save Info Skip

Figure 3. Facebook page for course description

For those students who would like to receive notification of course notes publishing, the lecturer could instruct them to use the function of adding themselves as fans of the course page. The lecturer could either rearrange the images or add new images by clicking “Organize Photos” or “Add Photo” buttons. For any further updates of the album, students with the role of fans of the course page would receive new notifications about the changes. The overview of the album is shown in Figure 4 and a screen showing the course content is shown in Figure 5.



Figure 4. Facebook page for course slides

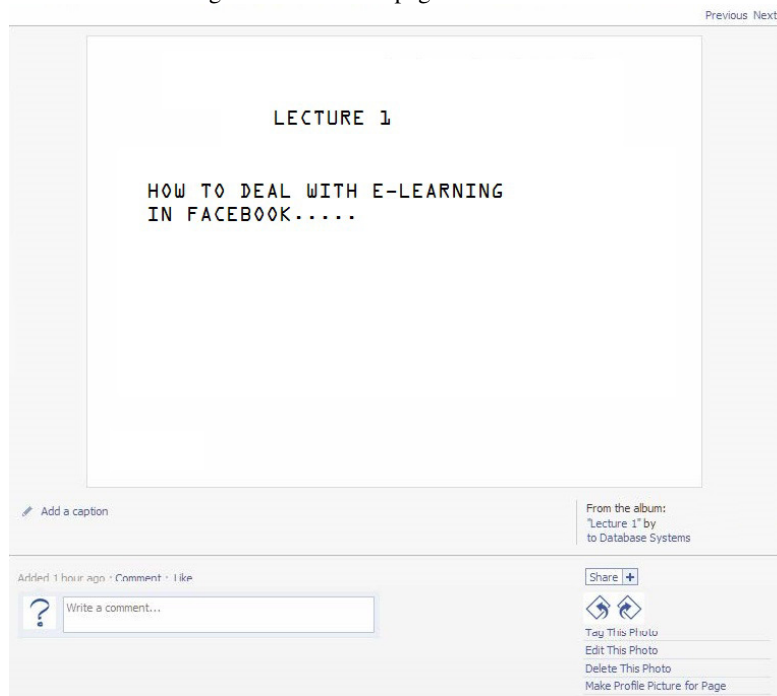


Figure 5. Facebook page for course slide presentation

The lecturer could make use of other Facebook features in the main profile of the course page to provide further support to the students:

- Link – teaching staff can add the reference materials on the web page with a link, such as reference articles, videos and so on.
- Event – teaching staff can create events for lectures and tutorials, so that student users will be notified and their main page will show the schedules of the lectures and tutorials whenever the students users log on Facebook.
- Video – if the lecture, tutorial or demonstration is recorded, it is possible to update it to the Facebook page, so that it is accessible easily by the students.

If the presentation file does not involve any transition effects, teaching staff could use the Facebook photo album web page to conduct the lecture/tutorial. The benefit was that if students wanted to raise any question and provide any feedback on the slide, they could post their comments for such slide and the teaching staff would be notified immediately. Such feature was especially useful to students who were passive in the class. The comments posted were specific to individual slide and it therefore facilitates the discussion among teaching staff and students. Students could also access to the photo album with their own mobile devices, such as mobile phones. Although the devices were small, they support zooming and enabled the students to provide feedbacks or comments similar to a computer. For example, Figure 6 shows the same lecture note slide to be shown by an Apple iPhone and a LG mobile phone respectively.

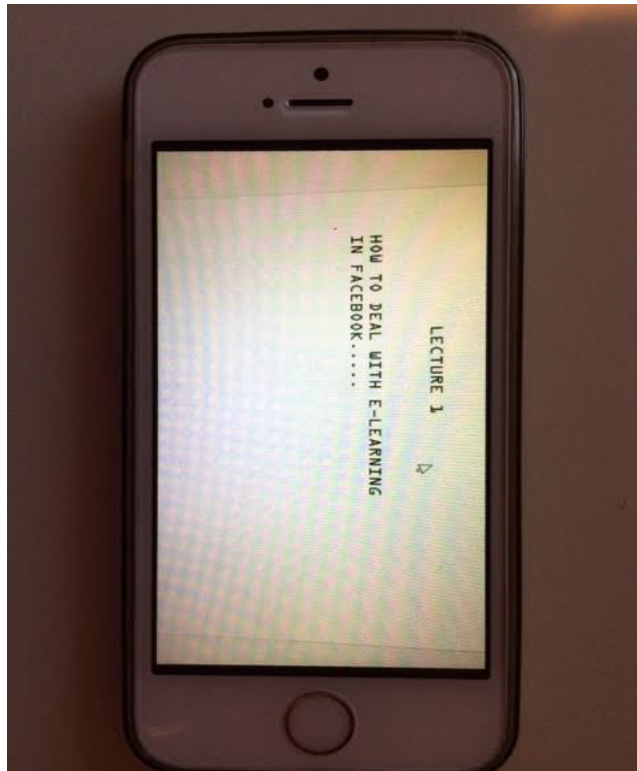


Figure 6. The image for a lecture note slide is shown by an Apple iPhone. The same will also appear in a LG mobile phone

For slide with text in smaller typeface, most mobile phones enable users to zoom the images for better readability. When students wanted to leave comments or questions regarding the slide, they used their mobile device to do so. For example, Figure 7 shows the user interfaces of an Apple iPhone and a LG mobile phone, which enables Facebook student users to post comments to a slide.

Create your own Quiz App!

Let's start by entering some basic info about your quiz. [Click here](#) to see what it looks like in the quiz.

What type of quiz do you want to make? (step 1)

☐ **Personality** Tells you what type of person you are. Example: What's your kissing style?

☒ **Trivia *new!*** Has right & wrong answers. Example: How well do you know Twilight?

Name Your Quiz:

This will be the title of your quiz app.

Quiz Description:

This shows up in the quiz directory.

Quiz Language:

This Quiz is For: ☒ Everybody ☐ Boys ☐ Girls ☐ Only my friends

Contains Alcohol: ☒ No ☐ Yes. Please restrict minors from viewing this quiz.

Upload a Picture:

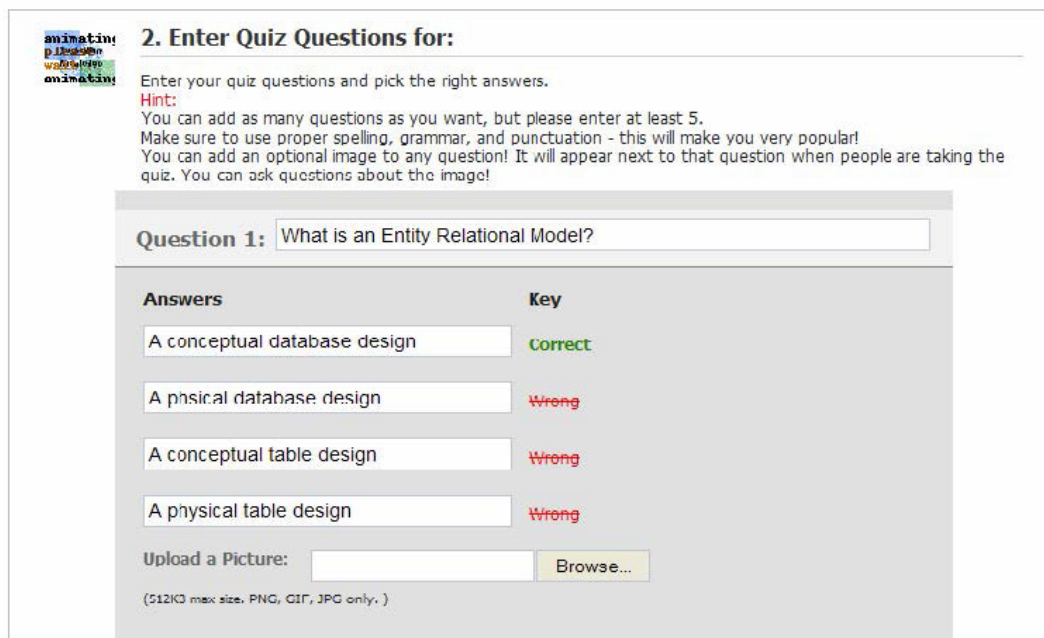
Upload a picture for your quiz to make your quiz more popular! Max 512KB. PNG, GIF, JPGs only.

Facebook guidelines: applications may not promote, or contain content (including any advertising content) referencing, facilitating, promoting or using, the following: Adult content, including nudity, sexual terms and/or images of people in positions or activities that are excessively suggestive or sexual; Obscene, defamatory, libelous, slanderous and/or unlawful content; Content that infringes upon the rights of any third party, including copyright, trademark, privacy, publicity or other personal or proprietary right, or that is deceptive or fraudulent; Sale of liquor, beer, wine, tobacco products, ammunition and/or firearms. Exception: liquor, beer and wine are permitted in apps that are marked as "containing alcohol."; Gambling, including without limitation, any online casino, sports books, bingo or poker.

By pressing Next, I certify that I have read and agree to the Quiz Creator Terms of Service and the Platform Application Guidelines, and that I have the right to distribute these pictures and that they do not violate Facebook's Terms of Use.

Figure 7. Specify the quiz name and details with Quiz Creator

In fact, mobile devices are capable of viewing the slide and enable students to leave comments or questions to particular slide. Upon receiving comments or questions, all members in the course, including teaching staff, would be notified. As soon as teaching staff received a notification emails from Facebook, they could click the embedded link that navigates the web browser to the referred slide, and leave another comment for the same slide as responses. Teaching staff could create quizzes to assess students' understandings of the lecture. For example, Figure 8 illustrate the use of Quiz Creator Facebook application by a teaching staff to create a quiz.



2. Enter Quiz Questions for:

Enter your quiz questions and pick the right answers.

Hint:
 You can add as many questions as you want, but please enter at least 5.
 Make sure to use proper spelling, grammar, and punctuation - this will make you very popular!
 You can add an optional image to any question! It will appear next to that question when people are taking the quiz. You can ask questions about the image!

Question 1:

Answers	Key
<input type="text" value="A conceptual database design"/>	Correct
<input type="text" value="A physical database design"/>	Wrong
<input type="text" value="A conceptual table design"/>	Wrong
<input type="text" value="A physical table design"/>	Wrong

Upload a Picture:

(512KB max size, PNG, GIF, JPG only.)

Figure 8. Specify the quiz questions and answers with Quiz Creator

5. CONCLUSION

The social networking site - Facebook is the most popular web site today, and students today do not need any training on its practice. In addition, any pc and smart device can effortlessly access it with web browsing competence. Thus, Facebook becomes an excellent additional education framework that can replace some features of traditional classroom learning. We also see today that more and more universities today are applying Facebook in a different level. In summary, the use of Facebook for education has many benefits. First, true cross platforms and cross devices such as pc and smart device support Facebook. Second, course-teaching materials are easily spread. Third, blog-like discussion or video chatting on individual items as well as online quizzes and assessments are supported. Fourth, it is user-friendly and no special trainings are obligatory. The points deliver some visions for one to develop a student friendly platform for information-sharing.

REFERENCES

- [1] E-learning Systems, <http://www.bapsis.com/elearningsystems.htm>, [On-line; accessed 19-September-2014].
- [2] Craciunas, S. & Elsek, I, (2009) The standard model of an e-learning platform, Bucharest, Romania, (Chapter 2).
- [3] Dobre, I., (2010) Critical Study of the present e-learning systems, Academia Romana, Romania, (Chapter 2).
- [4] Edgar, R. W., (2005) Security in e-learning, Springer. Vienna University of Technology, Austria, (Chapter 1).
- [5] Iacob, N., (2010). Data replication in distributed environments, Proceedings of International Scientific Conference ECO-TREND: Brancusi University Targu Jiu, 629-634.

- [6] Jalal, A. & Ahmad, M., (2008). Security Enhancement for E-Learning Portal, Proceedings of International Journal of Computer Science and Network Security, Department of Computer Science City University, Peshawar, Pakistan, 41-45.
- [7] Kritzinger, E. & Solms S., (2006). E-learning: Incorporating Information Security Governance, Proceeding of Informing Science and IT Education Conference, Salford (Greater Manchester), England, 319-325.
- [8] Kumar, S. & Kamlesh, D., (2011). Investigation on Security in LMS Moodle, Proceedings of International Journal of Information Technology and Knowledge Management, Kurukshetra University, Kurukshetra, India, 233-238.
- [9] Przemek, S. (2007), PHP Session Security, Poland, (Chapter 1).
- [10] Smeureanu, I. & Isaila, N, The Knowledge Transfer Through E-Learning in Business Environment, Economy Informatics, 97-98.

AUTHORS

Mohammad Derawi received his diplomas in Computer Science engineering from the Technical University of Denmark where he received both a BSc (2007) and Msc (2009) degree. In addition he received the title as the youngest engineer of Denmark in 2009. Derawi has pursued his PhD in information security at the Norwegian Information Security Laboratory (NISLab). His research interest included biometrics with specialization on gait recognition and fingerprint in mobile devices. Derawi was active in the 7th Framework European project “TrUsted Revocable Biometric IdeNtitiEs” (TURBINE, www.turbine-project.eu) and other main interests of areas include biometrics. Today he holds an full professor position and received the title as the youngest professor of Norway within Electronic Engineering and is specialised within Information Security, Biometrics, Smart Devices, Multimedia, Programming and Micro-Controllers.



INTENTIONAL BLANK

TRAFFIC SIGNAL CONTROL WITH VEHICLE-TO-EVERYTHING COMMUNICATION

Muntaser A. Salman^{1,2}, Suat Ozdemir³ and Fatih V. Celebi²

¹Department of Information Systems, University of Anbar, Anbar, Iraq

²Computer Engineering Department, Yildirim Beyazıt University, Ankara, Turkey

³Computer Engineering Department, Gazi University, Ankara, Turkey

ABSTRACT

Traffic signal control (TSC) with vehicle-to-everything (V2X) communication can be very efficient for solving traffic congestion problem. When regarding a low number of vehicles equipped with communication capability i.e. penetration rate (PR), an assumption that TSC can operate with a sufficient quality need to be studied. In this paper, this assumption was investigated with simulations using COLOMBO framework. The PR is the major factor that influences the quality of TSC, but as well the evaluation interval should be taken into account. The performance of TSC in means of sufficient period should follow the evaluations of the overall system. COLOMBO framework has been further investigated and new two approaches have been proposed (i.e. instead of swarm algorithm used in COLOMBO framework, simple and fuzzy logic have been used). To evaluate the performance of our proposal, a comparison with COLOMBO's approaches have been done. The results suggested that the duration that a vehicle remains associated with roadside unit (RSU) directly or through group leader can be used for controlling (as well as evaluating the traffic conditions) of an intersection with good accuracy even for low PR.

KEYWORDS

Traffic Signal Control, Vehicle to Everything Communication, Penetration Rate, COLOMBO Framework, Swarm algorithms & Fuzzy Logic.

1. INTRODUCTION

Traffic signals are able to self-organize and adapt to traffic conditions changing through vehicular communications monitoring and intelligent control algorithm. Vehicular communication monitoring provide extensive information of approaching vehicles as they frequently transmit a specific messages (e.g. basic safety message (BSM) in United States (US), or cooperative awareness message (CAM) in Europe countries(EU)), containing all required relevant information (e.g. speed, position, ...etc.). A convenient method to acquire data from cooperative vehicles is to receive messages with RSU. After receiving the message, the RSU extract the most important information that is suitable for TSC. Then, controlling an intersection through TSC required an algorithm that can deal with the RSU's information sufficiently.

In US and EU, several researches have been conducted for TSC of an intersection using vehicular communication protocols. Generally speaking, based on PR, two different approach for TSC can

be observed. Either full penetration rate(FPR) or partial penetration rate (PPR). This is done based on how much vehicular communication data are sufficient in the computation that achieve (full or partial) knowledge of the traffic conditions.

FPR-based approach is built upon an assumption that all vehicles are capable of communicate with each other for compressing the description about the traffic conditions. With FPR approach, it is capable to determine traffic conditions indicators without involving a RSU. Thereby, it may be applied for virtual TSC (or virtual traffic light VTL) of an intersection without real traffic signals infrastructure. In this context, VTL project [1] explored the benefits of vehicle-to-vehicle (V2V) communication for VTL using elected leader. For which, the responsibility of creating the VTL and broadcasting the traffic signal messages is assigned. The main drawback for this approach is the FPR that assumed. Although VTL project contributors in [2] show that VTLs can offer benefits in both throughput and delay with partial deployment scenarios, but they suggest an external representation for the VTL. Yet aspects such as visibility, and legislation, were not addressed. Clearly, these issues will play a major role in deciding what is the most appropriate representation and as a result a deployment issue is grown.

On the contrary, PPR-based approach is built upon an assumption that some vehicles are capable of communicate with each other and the available traffic signals infrastructure involve RSU. With PPR approach, to overcome the partial knowledge of traffic conditions, TSC can become more benefit with intelligent algorithm. In this context, the idea of self-organizing algorithm is merged in 2005 by Gershenson [3]. It was demonstrated that traffic signals are able to self-organize and adapt to changing traffic conditions by using simple rules without direct communication among intersections. The simple self-organizing traffic lights algorithm proposed in [3] gives preference to vehicles that have been waiting longer, and to larger groups of vehicles (platoons). According to that approach, platoons affect the behaviour of traffic signals operation, prompting them to turn green.

The idea of exploiting vehicular communication is merging into the field of self-organizing TSC recently. For instance, in [4] a decentralized adaptive TSC algorithm using V2I communication data was developed. Their algorithm was phase based and the objective was to minimize total queue length. The control problem considered as an optimization problem and it was solved by dynamic programming. In [5] a platoon based TSC algorithm in a vehicular communication environment was proposed. The algorithm divided a phase into two stages where the first stage served standing queue and the second stage served vehicles approaching the intersection. Based on the location and speed, the travel time of the vehicles can be obtained. Result showed that 40% PR was critical for effectiveness of the algorithm. In [6] a TSC framework for multi-modal under V2I communication was proposed. Their algorithm was platoon based and the objective was formulated to solve for an optimal signal plan based on current traffic condition, controller status, platoon data and priority requests. In [7] acumulative travel-time responsive real time intersection control algorithm with vehicular communication data was presented. The algorithm applied a kalman filter to estimate cumulative travel time under low PR. The phasing with highest combined travel time was set to be the next phase. The paper stated that at least 30% PR was required. In [8] a predictive microscopic simulation algorithm for TSC was proposed. The algorithm took data from vehicles including positions, headings and speeds and imported them to a model to predict the future traffic conditions. A rolling horizon strategy was chosen to optimize either delay only or a combination of delay, stops and deceleration. The algorithm considered several PRs as well as estimating the states of unequipped vehicles based on equipped vehicle states. Previous researches [3]-[8] showed that the PR was a critical parameter in determining the effectiveness of the TSC algorithms.

From literature review, it is clear that there are inefficiencies and trade-offs under different PR (e.g. efficient use of the communications channel versus accurate TSC and traffic conditions

estimation) that need to be focus on. In this context, the EU FP7 COLOMBO (2012-2015) project [9] exploits V2X protocols in the context of TSC. This was done in order to determine traffic surveillance information about local queue length in proximity of traffic signals. The goal of which is to use such traffic indicators to dynamically adapt TSC algorithms and timings. COLOMBO focuses on TSC algorithms using swarm algorithm with V2X cooperative data.

In this paper, simple and fuzzy logic had been investigated in COLOMBO framework instead of swarm algorithm with more detailed information that cooperative V2X protocol can offer.

The remainder of this paper is organized as follows. Section 2, presents COLOMBO project efforts in the field of intelligent TSC using V2X protocol with low PR. Section 3, describes in details the perspective of the approach proposed in this paper. Section 3 analyses the approach performance and reports the primary experimental results collected so far. Comparison with related works presented in Section 4. Discussions with on ongoing research and conclusive remarks end the paper.

2. COLOMBO's TSC

The main effort of the COLOMBO project is dedicated towards making self-organizing traffic lights an effective means for practical TSC [9]. The common underlying principle of the policies developed for the COLOMBO project is the teach TSC, controlling one or more interconnected intersections, operates independently of all other controllers and gets information only on the traffic flow on its incoming and outgoing lanes. Ideally, a birds-eye view of the traffic network with speed, position and route information about each vehicle should be available. Using this information, the TSC knows exactly how many vehicles are waiting or approaching each signal group. Both traditional detection V2X protocols and standard cooperative systems cannot deliver this even with FPR-based approach. This means that TSC algorithms rely on estimates of traffic conditions to divide the arrival flow between signal groups. With PPR-based approach, one could coarsely assume that absolute numbers (like number of vehicle and sum of stops) can be hardly determined, while averaging measures (like average speed) can be retrieved with a sufficient quality. In this context, COLOMBO project [9], developed an open source framework and confirm the previous assumption using simulations. COLOMBO framework use swarm intelligence algorithm to estimate an abstract of traffic conditions (called it pheromone) based on average speed and its derivative. Based on these pheromones, different TSC methods (i.e policies such as phase, platoon, marching and congestion policy) are developed. Each policy performs under specific traffic condition and not for others. For example, phase policy terminates the current phase as soon as another one has reached the traffic threshold after the minimum duration constraint of the current stage is satisfied. This policy was designed to handle medium-low traffic conditions, where this early termination would not make the TSC switch too often. It is worth mentioning that phase policy never ends the current stage if there are no cars opposing the currently allowed traffic flow.

Platoon policy tries to let all the vehicles in the currently green lanes pass the intersection before releasing the green light. It is worth noting that even the platoon policy will not switch phase unless another one requests the green light. The maximum phase duration is taken into account in order to pre-empt the current phase execution even if there are approaching vehicles.

In intense traffic conditions, each phase will be executed for the maximum allowed time. The definition of the maximum allowed time for a phase greatly impacts the performance of the system.

Marching policy is adequate when no vehicle is sensed or when the traffic looks too intense from all directions to take any online decision regarding the input lanes. In this case, there are two possible approaches:

- Falling back to a static duration for each stages;
- Taking into account the traffic conditions of the outgoing lanes to prevent traffic towards already heavily loaded ones.

The approach chosen by COLOMBO framework developer is the first one because they want the policies to implement simple rules.

Finally, congestion policy is used when the output lanes are congested and there may be vehicles waiting in front of the intersection. To avoid gridlocks, all input lanes are inhibited, i.e. the system terminates the current phase executing each stage for their minimum duration time. When the all red light stage is reached, no other phase is activated until the congestion has been solved.

To this aim, the goal of the policy selection procedure is to select which policy should be executed in the TSC undercurrent traffic conditions. In order to do that, COLOMBO framework has a large number of parameters that need to be appropriately set to achieve best possible performance. A parameter tuning optimization approach is required. It is time consuming and required a lot of traffic data to be aggregated in static or dynamic approach to overcome the whole traffic conditions. One drawback of this approach comes from the local traffic conditions sample aggregation areas. In static approaches the challenge is to determine the zone length that is neither too large nor too small. Dynamic approaches adjust to true traffic conditions, the challenge is to build and maintain dynamic clusters and cluster leaders.

On the other hand, in COLOMBO framework, a set of vehicles that are approaching an intersection are grouped following a common direction as an intermediate level of abstraction between the RSU and the multitude of surrounding vehicles. From this grouping; the group leader is chosen in an approximate central position, so that it can reach all other peers by simple single-hop communication and coordinate all group members. This grouping and group leader approximation chosen procedures in V2X protocols of COLOMBO framework make the dynamic cluster, with different PRs and traffic conditions, fuzzy and uncertain. Instead of using swarm algorithm to abstract traffic conditions, fuzzy logic had been used in this paper to estimate accumulative delay time with respect to the total travel time. Such indicators can be directly used for estimating the traffic conditions. This estimation, based on average speed and its derivative, is investigated with different PR for intelligent TSC design.

3. PROPOSED TSC

In this paper, we propose to follow PPR-based with different strategy. We can do that by estimating accumulative delay with respect to their total travel time as a direct indicator to the traffic conditions estimation. Our approach uses the V2X protocol that used in COLOMBO framework, mainly for average speed estimation purposes, to estimate the accumulative delay time for each edge per moment (e.g. in our simulation per second) using fuzzy logic. These conditions are monitored and accumulated locally by the RSU of an intersection. When a different edge situation is detected, the average of the individual estimations is determined in order to collaboratively detect and characterize the whole intersection traffic conditions. The relation between the averages of estimated accumulative delay time can be used directly to make a TSC adaptive. The details of our TSC algorithm is going to be explained in details in the following subsections.

3.1. Traffic conditions estimation

In PPR-based approach, PR is neither known nor can be estimated for near future. Because of that, the estimated average speed of vehicles per edge and its derivative can be use to estimate the accumulative delay time for each approaching edge, as well as for the whole edges, of an intersection per moment. Estimating the accumulative delay time (with respect to total travel time) is not just for traffic conditions estimation but also give an indicator for evaluation period for the intersection as a whole.

In general, delay time can be defined as the sum of acceleration, deceleration and stopped delay time. Where acceleration time can be defined as the time that determined with low speed and acceleration for vehicle (or group of vehicles) entered to the edge under the RSU coverage area. While, deceleration time can be defined as the time that determined with high speed and deceleration for vehicle (or group of vehicles) entered to the edge under the RSU coverage area. And finally, stopped delay time can be defined as the time that determined with zero speed and zero acceleration/deceleration for vehicle(or group of vehicles) entered to the edge under the RSU coverage area. This will be done in the RSU instantaneously per second so that the delay time per second can be determined.

Cumulative delay time can be used as a good indicator for evaluating TSC continually. For each second the information of the group is sent to the RSU that joins the intersection. The RSU use the incoming information for estimating the cumulative delay time of each edge separately. By averaging the cumulative delay time to the whole incoming edges of the intersection continuously, traffic conditions for the whole intersection can be estimated. As the vehicle travels along an intersection encounters different degrees of delay (i.e. different traffic conditions), so the value of the average cumulative delay time varies accordingly. Intuitively, the higher value of the average cumulative arriving time indicates the worse degree of traffic condition. Each RSU implementing our solution to estimates cumulative delay time based on its average vehicles speed and their derivative (acceleration/deceleration). The average vehicles speed can be easily obtained from the [1] protocol. Therefore, in each road (i.e. direction) we can estimate its cumulative delay time in terms of its average vehicles speed and their derivative through fuzzy system.

As in any fuzzy system, the input variables are first classified into different categories or fuzzy sets. The possible fuzzy sets for the speed are L for low, M for medium, and H for high. For the derivative, the defined fuzzy sets are N for negative, Z for zero, and P for positive. In addition, output fuzzy sets corresponding to estimated cumulative delay time have also been defined for one second time span, with L for low, M for medium and H for high. One of the main particularities of fuzzy logic is that a fuzzy set can contain elements with partial degree of membership, and consequently, an input value can belong to several fuzzy sets at the same time. For instance, a speed value of 9.9445 m/s (i.e. with maximum edge speed equal to 13.889 m/s) could be member, with a different degree of membership, of both medium and high speed fuzzy sets.

In order to determine the degree of membership of the input values to each of the fuzzy sets, membership functions are employed. The membership functions used in our solution, which have been implemented based on simple rating system, are illustrated in Fig. 1(a), Fig. 1 (b) (with average acceleration $a=2.8$ and deceleration $d=4.8$ [10]) and Fig. 1(c).

To finalize the definition of our fuzzy system, fuzzy rules that relate the input (speed and its derivative) and the output fuzzy sets (delay time per second) have been established and are displayed in Table I. The fuzzy rules have been designed based on the speed, its derivative and arriving/leaving time physical relationship. As Fig. 1(c) illustrates, the output of the fuzzy system is a continuous value within the interval $[0, 1]$ indicating the delay time, per second.

In this case, some policies have to be checked and select the most suitable one based on the traffic conditions of the incoming edge in an adaptation way. The details of which is given in the following subsection.

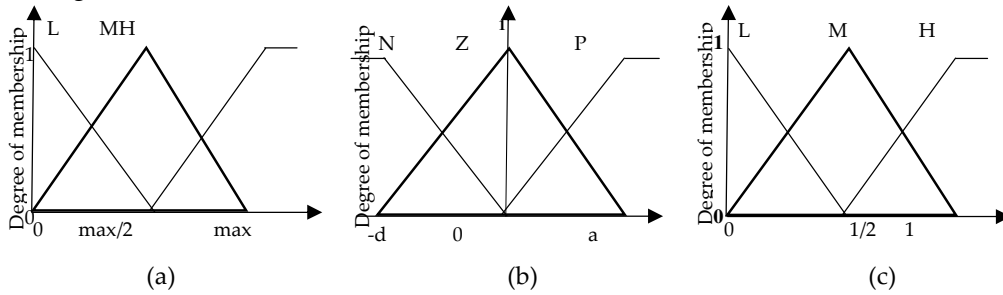


Figure 1. Fuzzy delay estimation system. (a) Average speed (m/s/veh) input sets. (b) Average speed derivative (m/s²/veh) input sets. (c) Average acceleration, deceleration and stopped delay (s/veh) outputs sets.

Table 1. Fuzzy rules relating inputs and outputs sets.

Average acceleration/ deceleration /stopped delay time (sec/veh)		Average speed derivative (m/s ² /veh)		
		N	Z	P
Average speed (m/s/veh)	L	L/H/L	L/L/H	H/L/L
	M	L/M/L	L/L/M	M/L/L
	H	L/L/L	L/L/L	L/L/L

2.2. Traffic signal adaptation

Self-organizing TSC is an online adaptation controller based on the individual estimations that different participating edges make locally through RSU. As described in the previous section, every RSU in an isolated intersection continuously monitors the individual traffic conditions for each approaching edge, and estimates through fuzzy system the current cumulative delay time. Only when the estimated of cumulative delay time exceeds a predefined threshold value, RSU activate the suitable control action (i.e. termination of the current state or not) as well as choosing the suitable policy (e.g. platoon, phase, marching and congestion policies used in COLOMBO project). Policies focus primarily on the duration of the current green stage. Each policy differs from the others mainly by the condition used to adjust the green time. Predefined threshold value may be corresponds to the level of service LOS of delay time to be monitored for each edge and/or for the intersection as a whole. At signalized intersections the motorized vehicles' LOS is a simple grading function of the average vehicle control delay. It may be calculated per intersection, per edge, or per lane group.

The adaptation mechanism is based on comparisons which are occurred when the leader updates the group fused data and sends it to the corresponding RSU. These comparisons are employed based on existing of vehicles and cumulative delay time made by different incoming edges. With predefined threshold value, traffic management policies can be changed in an adaptive way. In addition, the average cumulative delay time of last updating is exchanged to quantify the level of service for the intersection as a whole. Finally, RSU situated in the centre of an intersection will get a global and complete vision of the level of cumulative delay time for whole the approaching edges in the intersection. A key aspect in our solution is to identify the average cumulative delay time close to the RSU of the intersection that will change the adaptation procedure. Adaptation technique defines a procedure that is open for further optimization. The edge is considered to have increase value of cumulative delay time if its previous estimations sustainable reported some

stayed vehicle from previous cycle, and such cycle is not operated well to clear all the vehicles. Every edge has a counter that represent accumulative delay time updated to the current moment according to the following equation:

$$D_e(k) = \begin{cases} D_e(k-1) + Delay_e(k) & \text{if } car_e(k) > 0 \text{ and } k \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

$$\text{with } Delay_e(k) = \sum_{i=1}^3 F_i \left(v_e(k), \frac{dv_e(k)}{dk} \right)$$

Where $D_e(k)$ and $D_e(k-1)$ are the new and the previous value of accumulative GTD for edge e at time-step k and previous time-step $(k-1)$ respectively. $Delay_e(k)$ is the summation of estimated average acceleration F_1 , deceleration F_2 and stopped delay F_3 respectively based on the fuzzy inference F with edge average speed $v_e(k)$ and its derivative $dv_e(k)/dk$ as an inputs. Finally, $car_e(k)$ is the number of vehicles in edge e at time-step k .

Then, average of accumulative delay time for an intersection of n edges is given by:

$$Avg D_e(k) = \begin{cases} Avg D_{in}(k) & \text{for incoming edge} \\ Avg D_{out}(k) & \text{for outgoing edge} \end{cases}$$

$$= \begin{cases} \frac{1}{n} \sum_{e=1}^n D_e(k) & \text{for } n \text{ incoming edge} \\ \frac{1}{m} \sum_{e=1}^m D_e(k) & \text{for } m \text{ outgoing edge} \end{cases}$$

Since our solution has to be robust to low PRs, instead of using the counting number of cars, the updating of accumulative delay time is computed with only sensed car.

The policy selection algorithm makes use of previous indicator(i.e. $D_e(k)$) to decide which policy should be executed. Platoon and phase policies also use this measure to determine the duration of green period by applying a threshold (the so called traffic threshold) over it. Here threshold can be chosen as constant value (e.g. LOS required for the whole of the intersection or for each edge of it).

Based on [11], platoon and phase policies are not suitable for low traffic conditions. Swarm and platoon are the best policies for very high traffic conditions. Congestion policy is selected when all the inputs lanes are congested and there are no suitable decision based on available information or when the output lanes are congested and there are vehicles waiting in the intersection.

Thus, the following simple selection rules can be use:

- If $D_e(k) < 10$ then Policy is “Marching”
- If $D_e(k) \geq 10$ and $D_e(k) < 20$ then Policy is “Marching”
- If $D_e(k) \geq 20$ and $D_e(k) < 35$ then Policy is “Marching”
- If $D_e(k) \geq 35$ and $D_e(k) < 55$ then Policy is “Phase”
- If $D_e(k) \geq 55$ and $D_e(k) < 80$ then Policy is “Platoon”
- If $D_e(k) > 80$ then Policy is “Congestion”

One further issue should be mentioned here, delay time estimation is done instantaneously for each edge as well as for the whole intersection. The policy selection procedure of the TSC for the whole intersection should be rather insensitive to very short peaks delay time estimation, like a singular platoon in one edge, but should react rapidly to more persistent traffic changes where we expect a burst in traffic from a single direction that will last for specific period (e.g. fifteen to

twenty minutes). In order to do that, total vehicles sensed time (VST) is proposed by the following equation:

$$VST_e(k) = \begin{cases} VST_e(k) + 1 & \text{if } car_e(k) > 0 \text{ and } k \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

where $VST_e(k)$ and $VST_e(k-1)$ are the vehicle sensed total time per edge e at time (k) and $(k-1)$ respectively. With this proposal, the percentage delay time can be determined using the following equation:

$$ADP_e(k)\% = D_e(k)/VST_e(k)$$

Where, $ADP_e(k)\%$ is the percentage delay time for edge e at time k .

To this aim, every edge of an intersection evaluates its local delay time estimation. If the evaluation process continues for a certain period of time (typically 15 minutes) with acceptable (typically $ADP_e(k) < 10\%$), no change for intersection TSC policy will be required, otherwise policy selection procedure is activated to select new policy. The above description for policy selection procedure can be given by the following equation:

$$Terminate = \begin{cases} Yes & \text{if } \max_{e=1}^n ADP_e(k)\% \geq 0.1 \\ No & \text{otherwise} \end{cases}$$

Where $Terminate$ is the Boolean activation result for policy selection procedure. $\max_{e=1}^n ADP_e(k)\%$ is the maximum $ADP_e(k)\%$ for n edge of an intersection. The results of the current proposed approach are described in the following section.

4. SIMULATION RESULTS

For evaluating the proposed TSC approach, a simple scenario consisting of an intersection was taken from COLOMBO framework (called Rilsa intersection [10], as shown in Fig. 2). This is done for two reasons, comparability and traffic realistic.

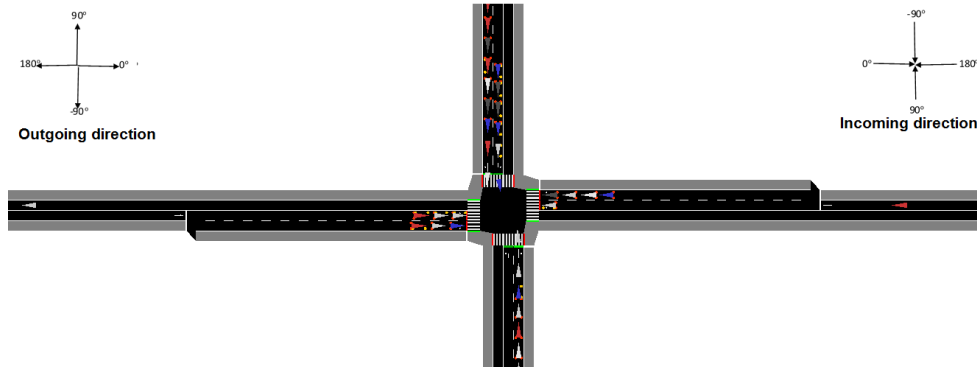


Figure 2. RILSA Intersection with incoming and outgoing direction

At the network level, all communications are performed by the ns-3 standard *Yans* WiFi model using IEEE 802.11p with ETSI ITS G5 standards. V2X communications with a fixed 170m transmission range are assumed. The value of 170 meters is chosen to match the maximum communication range of a mobile node used in COLOMBO framework. A 6 Mbps bandwidth rate with OFDM and default log-distance propagation model is used to compute signal loss.

In the simulation study, RSU periodically receives messages from group leader (if exist) within one second sampling resolution indicating number of cars and average speed per incoming and

outgoing edge respectively. All simulations were performed in the same one hour time span. Vehicle densities are changed during time according to a wave trend that follows the green and red timings controlled by the traffic light. Table 3. reports the main configurations and parameters used in our simulations.

Table 3. Simulation parameters.

Parameter	Value
Wi-Fi mode	802.11p/ETSI ITS 5G
Transmission mode	6 Mbps (OFDM)
Node radius	170 m
Propagation loss	Logarithmic
Propagation speed	Constant (3×10^8 m/s)
Penetration rate	100,50,20,10,5,2,1%
Simulation time	1 hour

Vehicles densities and traffic conditions change during time according to a wave trend that follows the green and red timings controlled by the traffic signals. First, simulations have been run using one single policy at a time to compare with. The simulation involved the following policies: marching, platoon, phase and congestion. Then, COLOMBO framework with swarm algorithm as well as our approach (using fuzzy logic) are simulated. All of the above simulations had been run for measuring how the average waiting time, time loss and duration of the vehicles to accomplish their route varies, depending on the PR.

Average waiting time under different PR, shown in Fig. 3, depicts the number of steps in which the vehicle speed was below 0.1 m/s measured in simulation steps from SUMO output.

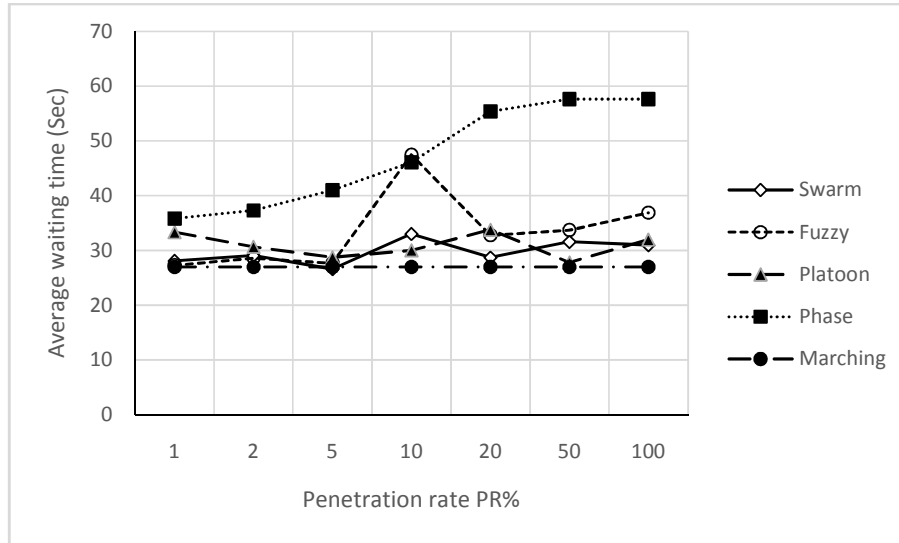


Figure 3. Average waiting time vs. penetration rates

Time loss under different PR, shown in Fig. 4, depicts the time lost due to driving below the ideal speed. Finally, the Fig. 4: Time loss vs. penetration rates duration time under different PR, shown in Fig. 5, depicts the time the vehicle needed to accomplish their route.

These figures (i.e. Fig. 3-5) show the policies behaviour when simulated each one alone as well as with swarm and fuzzy algorithms in COLOMBO framework with different PR. To evaluate our approach with over mentioned ones, a simple comparison can be made in the following section

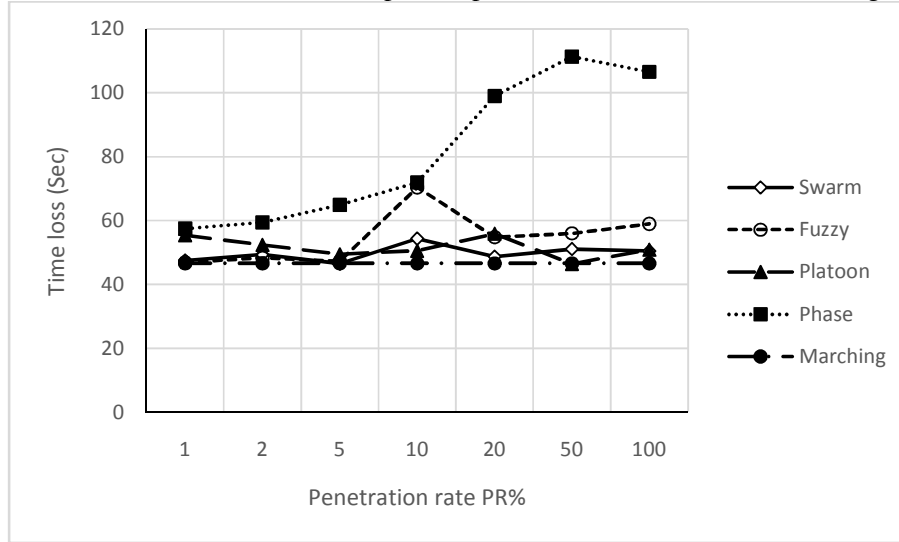


Figure 3. Time loss vs. penetration rates

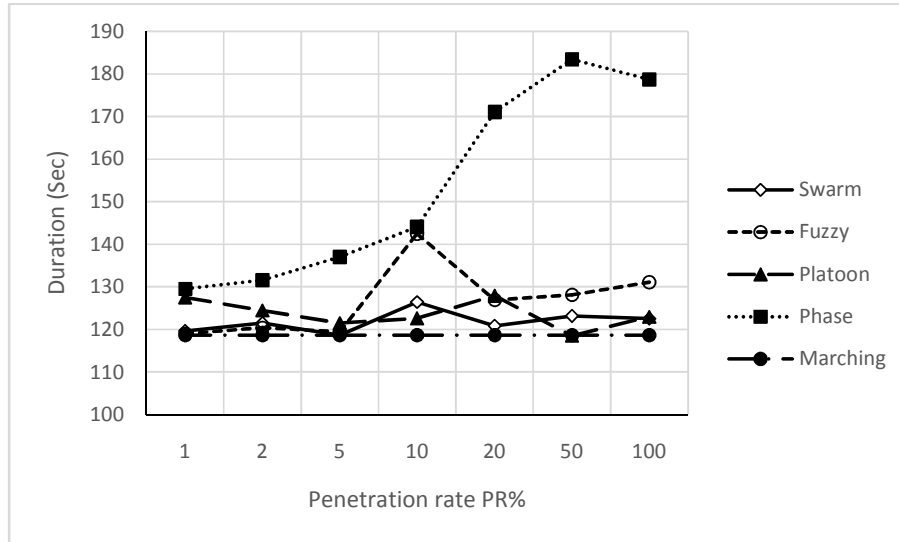


Figure 4. Duration vs. penetration rates

5. COMPARISON

In order to evaluate our approach, a simple comparison with COLOMBO approach is done here. Fig. 3-5 shows that marching policy works well for all PR. This policy adopts a static approach (i.e. constant TSC setting) with dynamic phase selection. Since RILSA intersection simulated using only two phases (i.e. no need for dynamic phase selection) and using COLOMBO framework (i.e. with optimized parameters), this may reflect some sort of optimized results with this policy.

Phase policy fits well for low PR while it does not for high PR. This policy maintains the green light as long as there are no cars on the other directions. The results prove that this behaviour is desirable when there is a dominant traffic flow (i.e. high traffic flow even under low PR) opposed by a irregular one. Platoon policy gets significant results in low-medium PR (i.e. 2-20%) with minimum values at 50%. This policy creates platoons of vehicles that are free to leave the intersection since nothing blocks them after they pass the central area. Creating platoon required some characteristic, such as platoon size, length and period, to be available to study their behaviour. These characteristics are difficult to study under PPR especially for adaptive problem. The above results clearly indicate that PPR should be handled under specific policies.

Best TSC approach should be able to properly detect each policy situation. Swarm algorithm (more specifically, policy selection procedure of it) select between the above policies with dynamic mechanism. This mechanism depend on parameters optimization that provide smooth transitions between policies. In spite of that, this transition has a clear oscillation effect with PR₀10%. In other words, swarm algorithm has an optimization solution with stable transition effect rather than direct policy selection procedure. In the other hand, using simple and direct if then rules (with fuzzy delay estimation) give the same behaviour as for individual policies based on threshold values for policy selection procedure. Both of the above policy selection procedure give comparable results with different PR except at 10%. The results are quite interesting since they show that our proposal is capable to maintain the same performance regardless the PR of equipped vehicles. These comparable results led us to the following section of conclusion.

6. CONCLUSION

From the previous comparable results, some conclusions can be stated here. Our TSC solution includes several simplifications compared to COLOMBO's one, taking into consideration PPR based approach. The policy selection procedure in COLOMBO's solution is not relevant for the calculation of TSC setting with low PR because it rely on counting vehicles.

This can be problematic if not all vehicles are sensed like in PPR based approach. That's why different versions of policy selection procedure had been proposed as an optimization problem in COLOMBO's solutions. In the other hand, our solution has the very positive logical behavior of policy selection procedure. The TSC evaluation strongly depend on the policy selection procedure. Using threshold values, as in our solution for policy selection procedure, make it open for further optimization. With these threshold values our solution can get almost the same performance even when one vehicle is sensed under the RSU communication range without relying on counting vehicle. This motivates the solution to be used for PPR based approach. At the same time, focusing on developing policy selection procedure with threshold values based on delay time estimation is not enough. In fact, as shown in Fig. 5, the duration for each vehicle to accomplish their route give an indicator for another parameter should be taken into consideration, evaluation period. Most TSC evaluated for typically 15 minutes as said before. But none of the compared approach for policy selection procedure had been taken this period into consideration. One obvious issue is the lack of data for intervals where no equipped vehicle was sensed. The probability to have no data for an interval depends on the aggregation interval's duration and the PR. For this reason, low PRs show data lacks at times where no equipped vehicle has been within the communication range. As a result, our approach should be further investigate by taking evaluation period into consideration.

REFERENCES

- [1] M. Ferreira, R. Fernandes, H. Conceicao, W. Viriyasitav at, and O.Tonguz. (2010) "Self-organized traffic control". In Proceedings of the 7th ACM international workshop on Vehicular Inter-networking, pp. 85-90. ACM,.

- [2] Hugo Conceicao, Michel Ferreira and Peter Steenkiste(2013) "Virtual Traffic Lights in Partial Deployment Scenarios," IEEE Intelligent Vehicles Symposium(IV) June 23-26, Gold Coast, Australia.
- [3] Gershenson, C.(2005)"Self-organizing Traffic Lights," Complex Systems, Vol.16, pp. 2953. 2005.
- [4] Priemer, C., Friedrich, B. (2009)"A decentralized adaptive traffic signal control using V2I communication data," 12th International IEEE Conference on Intelligent Transportation Systems, ITSC 09. pp. 16. 2009.doi:10.1109/ITSC.2009.5309870
- [5] Datesh, J.; Scherer, W.T.; Smith, B.L. (2011) "Using k-means clustering to improve traffic signal efficacy in an IntelliDriveSM environment," 2011IEEE Forum on Integrated and Sustainable Transportation System(FISTS). pp. 122-127. doi:10.1109/FISTS.2011.5973659
- [6] He, Q.; Head, K.L.; Ding, J. (2012)"PAMSCOD: Platoon-based arterial multi-modal signal control with online data," Transportation Research Part C: Emerging Technologies. Vol. 20, pp. 164-184. 2012.doi:10.1016/j.trc.2011.05.007
- [7] Lee, J.; Park, B.; Yun, I. (2013)"Cumulative Travel-Time Responsive Real-Time Intersection Control Algorithm in the Connected Vehicle Environment," Journal of Transportation Engineering. Vol. 139, pp. 10201029. 2013.doi:10.1061/(ASCE)TE.1943-5436.0000587
- [8] Goodall, N.; Smith, B.; Park, B., (2013)"Traffic Signal Control with Connected Vehicles," Transportation Research Rec. Journal of Transportation Research Board, Vol. 2381, pp. 65-72. doi:10.3141/2381-08.
- [9] EU FP7 COLOMBO Project, (2012-2015)[Available Online]: <http://www.COLOMBO-fp7.eu/> [Accessed 12 June 2016].
- [10] RiLSA1, COLOMBO, (2014). [Available Online]: <http://sourceforge.net/projects/sumo/files/traffic-data/scenarios/RiLSA/> [Accessed 12 June2016].
- [11] COLOMBO, Deliverable 2.2 (2014),"Policy Definition and dynamic Policy Selection Algorithms". [Available Online]: <http://www.COLOMBOfp7.eu/> [Accessed 12 June 2016].

AUTHORS

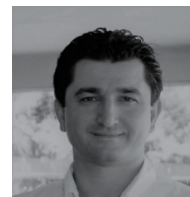
Muntaser A. Salman has been with College of computer science and information technology at university of Anbar, Anbar, Iraq, since 2003. He received his B.Sc. and M.Sc. degrees in electrical engineering from Basrah University, Basrah, Iraq, in 1997 and 2000 respectively.

Currently, he is working toward the Ph.D. degree at Computer Engineering Department, Institute of Engineering and Natural Sciences, Yildirim Beyazit University, Ankara, Turkey. His research interests include computer networks, vehicular networks, computational intelligence algorithms and intelligent transportation systems



Suat Ozdemir has been with the Computer Engineering Department at Gazi University, Ankara, Turkey, since 2007. He received his MSc degree from Syracuse University and PhD degree from Arizona State University in 2001 and 2006, respectively.

Dr.Ozdemir's research are as mainly include wireless and sensor networks, network security, and data mining. He is a member of IEEE and currently serving as editorial board or TPC member for various leading IEEE and ACM journals and conferences.



Fatih V. Celebi was born in Kahramanmaraş, Turkey, 1963. He received his B.Sc. and M.Sc. degrees in electrical and electronics engineering from Middle East Technical University (METU) and Gaziantep University, Turkey, in 1988 and 1995, respectively.

He earned his Ph.D. degree in Electronics/Computer engineering from Erciyes University in 2002. His research interests include Artificial Intelligence Techniques and Optical Design. He is currently a full professor and Vice president Yildirim Beyazıt University, Ankara, Turkey.



INTENTIONAL BLANK

PERFORMANCE EVALUATION OF MOBILITY AND ROUTING PROTOCOLS FOR VEHICULAR AD HOC NETWORKS USING NS-2 AND VANETMOBISIM

Fatma Baccar¹, Kais Mnif¹ and Lotfi Kammoun²

¹National School of Electronics and Telecommunications,
NTS'Com , Sfax, Tunisia

²National School Engineers of Sfax, Sfax, Tunisia

ABSTRACT

In this paper, we will focus on the performance evaluation of a vehicular mobility scenario graph. Indeed, we will analyze the performance metrics (throughput, packets loss and end to end delay) using the IEEE 802.11p standard of the proposed mobility graph. In addition, we examine the impact of the packet length, vehicle speed and routing protocols (Ad-Hoc On-demand Distance Vector "AODV", Destination Sequenced Distance Vector "DSDV" and DumbAgent). Our simulations are based on the networks simulator "NS-2" and the mobility simulator "VanetMobisim" to evaluate the performance of the vehicular ad hoc network.

KEYWORDS

Vanet; mobility graph; 802.11p; throughput; end to end delay; packets loss; routing protocols; vehicle speed; packet size; NS-2; VanetMobisim

1. INTRODUCTION

Vehicular Ad hoc Networks (VANETs) are a special type of Ad Hoc networks; it is a subclass of mobile Ad hoc networks (MANETs). The purpose of this network is to provide safety, to minimize road accident and to give new interests for inter vehicle communications by: helping emergency vehicles to pass other vehicles quickly, broadcasting warning messages to neighboring vehicles in case of car accidents, providing drivers with latest real time traffic information, assisting drivers to find accessible parking space [1], etc. VANET is different from other kinds of networks; some of its characteristics are: high mobility, dynamic topology, short communication periods and limited bandwidth. VANET communications are based on broadcast messages which are exchanged between vehicles. The IEEE 802.11p is employed as a transmission protocol. It's an approved extension to the IEEE 802.11 standard, adding wireless access in vehicular environments (WAVE), for easier and more effective communication between vehicles with dynamic mobility. This technology uses the 5.9 GHz band in different propagation environments [2].

The simulation was used to evaluate the performance of VANET due to the high cost of deploying and implementing VANET systems in a real environment. A lot of simulators for VANETs have been emerging [3] [4]. One of the first attempts to authors was to present a comprehensive study and to make comparison of the various publicly available VANET simulation software and their components [5] [6] [7].

After study, we have decided to work with VanetMobisim simulator [8] which can be used to understand the properties of the mobility graphs of vehicular traffic and to interface it with NS-2 [9] in order to evaluate the performance metrics using the parameters of 802.11p standard. The traffic simulator VanetMobisim is an open source and it supports Intelligent Driver graph with Intersection Management (IDM_IM) which generates realistic vehicular mobility graph [10].

Several publications [11] [12] [13] have studied the performance for vehicular ad hoc networks; however they do not support realistic vehicular mobility simulation. Mostly, the authors simulate the mobility and the routing protocol separately.

The rest of the paper is structured as follows. In section 2, we will briefly describe DumbAgent, AODV and DSDV protocols. In section 3, we will describe the IDM_IM mobility model graph. The simulation system structure, description of the scenario graph and simulation results will be discussed in section 4. Finally, the conclusions and future work are presented in Section 5.

2. ROUTING PROTOCOL

For our performance comparison study, we choose the most known and the most used routing protocols for VANET such as DumbAgent, AODV and DSDV were chosen. We will shortly describe these protocols in the following section.

2.1. DumbAgent protocol

DumbAgent routing protocol host agents and give a place to store a database of routing information. The technique is to embody the intelligence in the system. When vehicle moves from node to node, it updates its routing information as they go. The goal of the routing agent is to explore the network and to update every visited node. Each routing agent memorizes a history of where it has been. At each node, the agent uses its information history to update its routing table with adding the best paths.

2.2. DSDV protocol

Destination sequenced distance vector protocol (DSDV) [14] is a proactive routing protocol which is an amelioration of the Distributed Bellman Ford algorithm. DSDV tries to solve the routing loop problem. It provides one path only between source and destination, which is computed using the distance vector algorithm. To reduce the network overhead, two types of update packets are used: full dump and incremental update.

2.3. AODV protocol

Ad-Hoc On-demand Distance Vector protocol (AODV) [15] [16] is a reactive routing protocol which is based on DSDV protocol, therefore, paths are determined by sources only when needed to reduce traffic overhead. Paths are maintained only as long as data are traveling along the routes from the sender to the receiver. AODV protocol provides unicast and multicast communication. In this protocol, the sequence numbers are used for loop prevention and as route freshness criteria.

3. MOBILITY MODEL GRAPH

In order to model a realistic vehicular movement in our simulation, it's preferable to use a realistic mobility model graph. So, we use the Intelligent Driver Model with Intersection Management (IDM_IM) [10]. Generally, it's the most mobility model graph used and it's a part

of the VanetMobisim tools. The Intelligent Driver Model (IDM) is a macroscopic car following model that adapts automatically a vehicle speed according to other vehicles driving ahead. This type is one of the cars following models category [3]. IDM_IM model uses a small set of parameters, which can be calculating with the help of real traffic measurements. This model is an extension of the IDM model, in order to introduce the management of intersections regulated by traffic lights and of broads with multiple lanes [17]. It can manage crossroads regulated by both stop signs and traffic lights.

4. PERFORMANCE EVALUATION

4.1. Simulation System Structure

Our simulation process is shown in figure 1. First; we use the VanetMobisim to describe the scenario by defining the environment details and the vehicle mobility using XML language. After running VanetMobisim simulator, it generates a trace file that contains the vehicular traffic and all environment details (node identifier, position, simulation time, vehicular speed...). Next, the Network Simulator NS-2 takes as input the generated file of VanetMobisim. NS-2 uses the Tcl script as a programming language to describe the details related to communications and network configuration. Finally, we get two files (*.nam and *.tr) as the outputs after running NS-2. The Network Animator file records all the positioning and graphical informations performed during the simulation time (see figure 2) of the scenario. The trace file contains all of the informations about the simulation results (packets sent, received and dropped, attached sequence number, protocol type, packet sizes...) To extract the statistics of the performance metrics from the generated file of NS2, we use AWK tool.

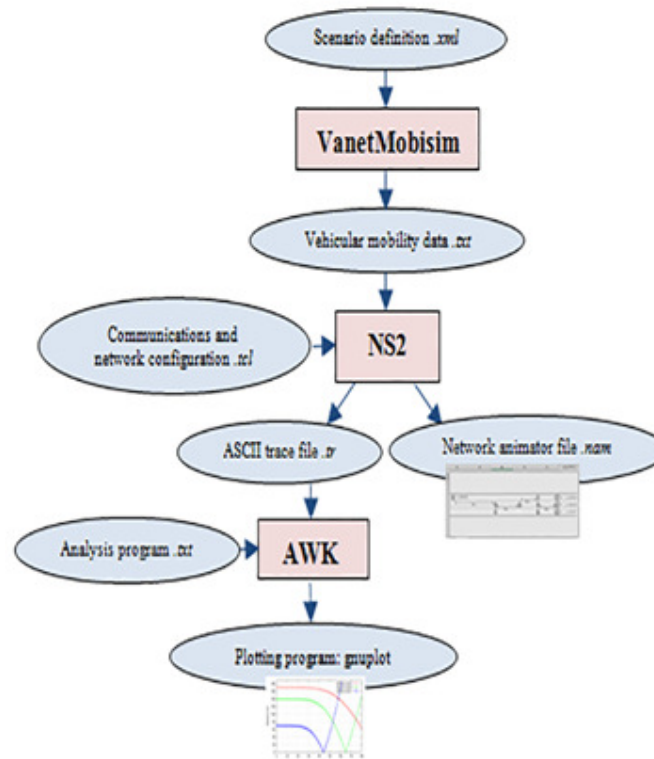


Figure 1. Simulation system structure

4.2. Scenario

Our test scenario aims to present a real situation. The scenario represents a part of a highway. This part of the road comprises ten vehicles dispersed on three parallel unidirectional lanes (see figure 2). The cars have a minimum speed equal to 60km/h and a maximum speed around 70, 100 and 120 km/h respectively in lanes 1, 2 and 3. In exception, the vehicle 0 is a police car and it has a maximum speed equal to 140 km/h, the police car is in the emergency situation and diffuses a periodic message every 0.2 seconds with a payload equal to 500 bytes. To better evaluate the performance metrics, we vary the size of the packets sent by the police vehicle as well as the routing protocol used (DumbAgent, AODV and DSDV). Tab.I resumes all simulation parameters.

Table1. Simulation parameters

Simulation environment	Ubuntu 14.04
Traffic simulator	VanetMobisim
Network simulator	NS2
Simulation time	80 seconds
Simulation area	2000*300 meters
Number of nodes	10
Mobility model	IDM_IM
Packet size	500, 1000, 1500 bytes
Max speed	Lane 1: 70km/h Lane 2: 100km/h Lane 3: 120km/h
MAC protocol	802.11p
Radio propagation model	Two Ray Ground
Routing protocol	DumbAgent, AODV, DSDV

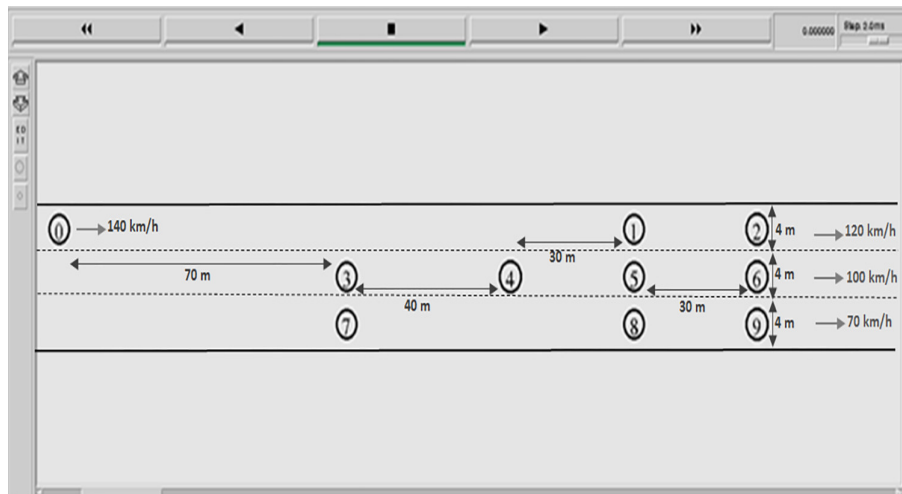


Figure 2. Simulation scenario graph

4.3. Results

In this subsection, we will present the simulation results obtained of the scenario described in figure 2.

We consider the throughput, the end to end delay and the packet loss of the nine vehicles when the vehicle 0 transmits a periodic packet with a payload equal to 500 bytes. The protocol used in this case is the DumbAgent for more evaluating the performance metrics with the 802.11p standard.

- **Throughput**

T is the throughput : it is the rate of successful packet delivery through a network connection per unit of time:

$$T = \frac{S(t)}{t} \quad (1)$$

Where, t is the unit of time taken and $S(t)$ is the total successful packet received at the defined time t .

- **End to end delay**

D_i is the end to end delay. This term includes all the time required for a packet to be generated, transmitted through the network, and received by the destination:

$$D_i = tr_i - ts_i \quad (2)$$

Where, i is the packet identifier, tr_i is the time at which a packet is received at destination, ts_i is the time at which a packet is sent from source.

$D_{average}$ is the average end to end delay:

$$D_{average} = \frac{1}{n} \sum_{i=1}^n (tr_i - ts_i) \quad (3)$$

Where, n is the number of packets which delivered successfully.

- **Packet loss**

The reliability of the network connection is evaluated by the packet loss rate P_{loss} .

$$P_{loss} = \frac{L}{p} \quad (4)$$

Where, L is the number of non received packets and p is the total number of sent packets.

Figure 3 illustrates the distances separating the police car and other vehicles 2, 5 and 7 during the simulation time.

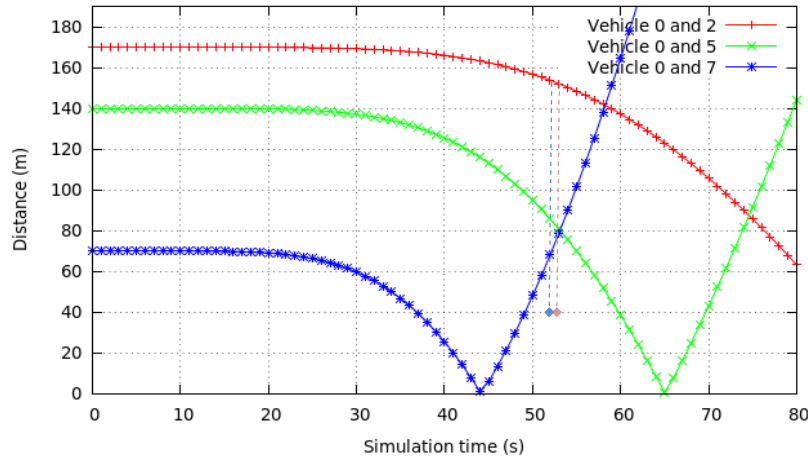


Figure 3. Distance between vehicle 0 and vehicles 2, 5 and 7

The throughput of vehicle 2, 5 and 7 with a packet size 500 bytes is shown in figure 4. We can notice that the throughput of vehicle 2 is equal to 0 kbps for 59 seconds but after this time it becomes between 3.6 and 4.4 kbps. According to figure 3, the distance between the police car and vehicle 2 is greater than 140 meters for 59 seconds. The time of state transformation of the throughput is 58 seconds for the vehicle 7. The throughput of vehicle 5 does not reach 0 kbps; this is due to the distance that separates it from the vehicle 0 which is still less than 140 meters according to figure 3.

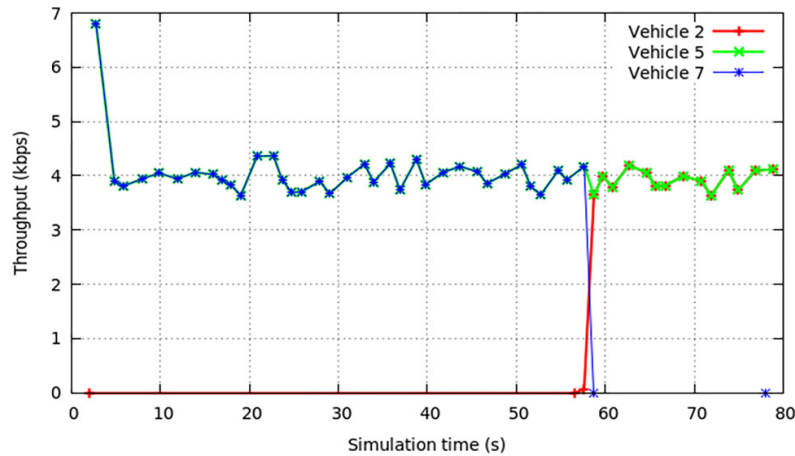


Figure 4. Throughput of vehicles 2, 5 and 7 (packet size: 500 bytes)

Figure 5 shows the percentage of packet loss between vehicle 0 and vehicles 2, 5 and 7 during simulation time. The packet loss between police car and vehicle 2 and vehicle 7 is 0 % when the distance between the vehicle 0 and the other vehicles is less than 140 meters. All the simulation time, there is no packet loss between vehicle 0 and vehicle 5.

We can conclude that all vehicles with a distance less than 140 meters from vehicle 0 have the same throughput and have no packets loss with the police car.

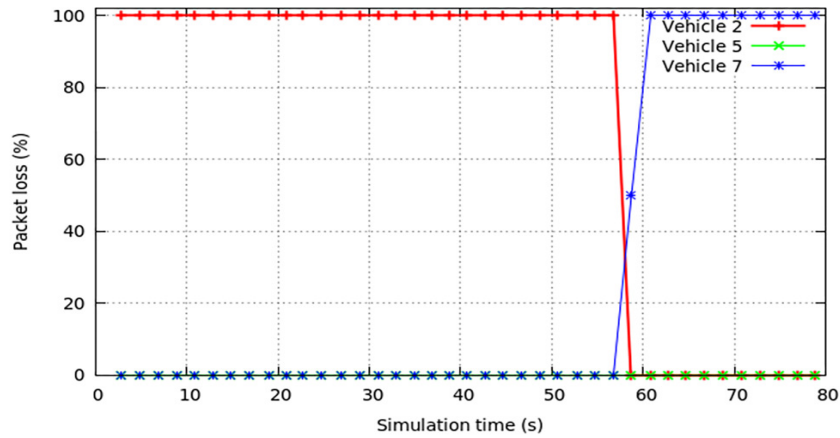


Figure 5. Packet loss between vehicle 0 and vehicles 2, 5 and 7
(packet size : 500 bytes)

Figure 6 presents the end to end delay between police car and vehicle 2, 5 and 7. We may notice that when the distance between vehicle 0 and other vehicles is less than 140 meters, we have a tracing of end to end delay. According to figure 3, when the distance between the transmitter and the receiver decreases, the end to end delay decreases as well.

So, as a result the throughput, the packet loss and the end to end delay are affected by varying the distance between police car and other vehicles and not by varying the speed of vehicles.

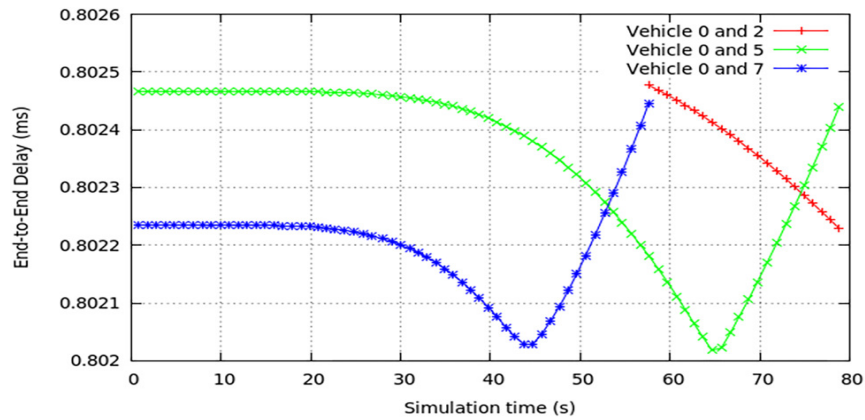


Figure 6. End to end delay between vehicle 0 and vehicles 2, 5 and 7
(packet size : 500 bytes)

To obtain a statistical significance, we calculate the average performance metrics in figure 7, figure 8 and figure 9.

Figure 7 illustrates the average throughput off all vehicles with packet size 500 bytes. We can show that the vehicles 2, 6 and 9 have the lowest value of throughput. The average throughput of others vehicles can reach 4 kbps.

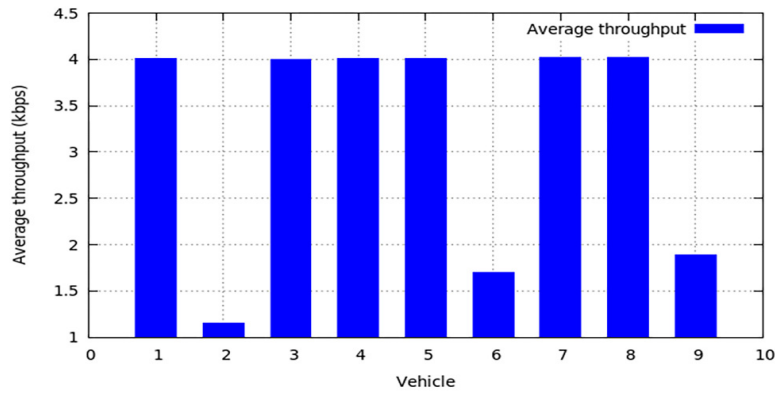


Figure 7. Average throughput of all vehicles (*packet size: 500 bytes*)

The percentage of the average packet loss is present in figure 8. Since the vehicles 2, 6 and 9 have had the minimum value of average throughput in figure 7, they have the maximum value of average packet loss between them and vehicle 0. As a result, the vehicle 1 and 5 haven't lost any packet with the police car.

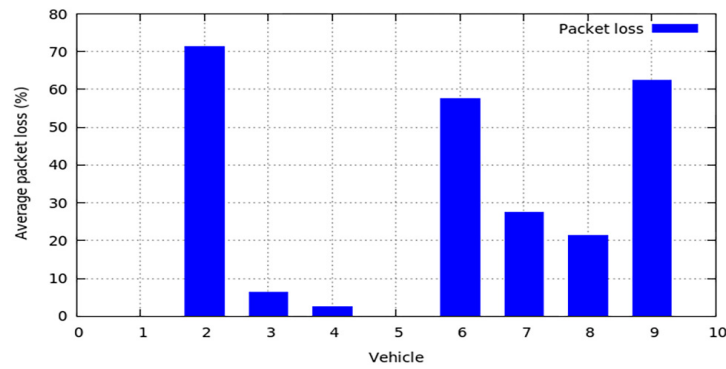


Figure 8. Average packet loss off all vehicles (*packet size : 500 bytes*)

The average end to end delay of all vehicles is calculated in figure 9 with packet size 500 bytes. The average value of the end to end delay between transmitter and receiver is almost the same for all vehicles (0.8 ms).

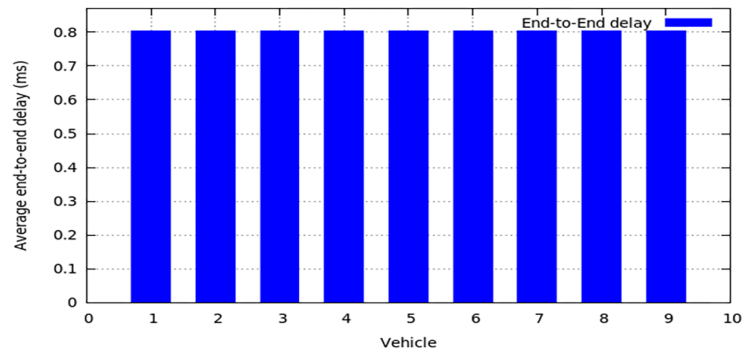


Figure 9. Average of the end to end delay between vehicle 0 and other vehicles (*packet size : 500 bytes*)

In figure 10 and figure 11, we modified the packet size sent by the police car to evaluate better the effect of the packet size in the performance metrics. The vehicle 0 sent a periodic packet every 0.2 seconds with a payload size of 500, 1000 and 1500 bytes respectively in three network simulations. Figure 10 and figure 11 show the average throughput and end to end delay of all vehicles with three different packet sizes. As the packet size increases, the average throughput and the average end to end delay increases as well, but the increment of throughput of vehicles 2, 6 and 9 is not as high as other vehicles.

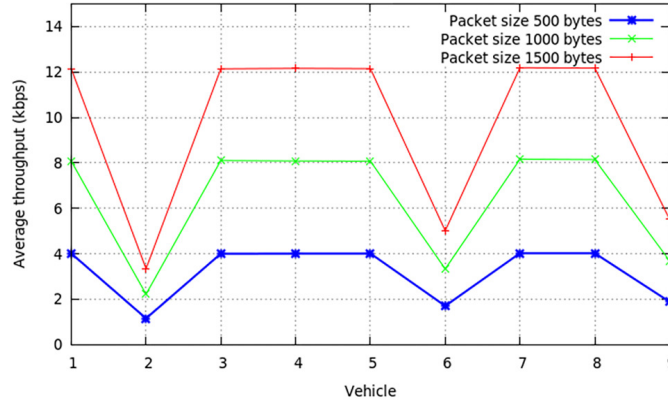


Figure 10. Average throughput of all vehicles (*packet size : 500, 1000, 1500 bytes*)

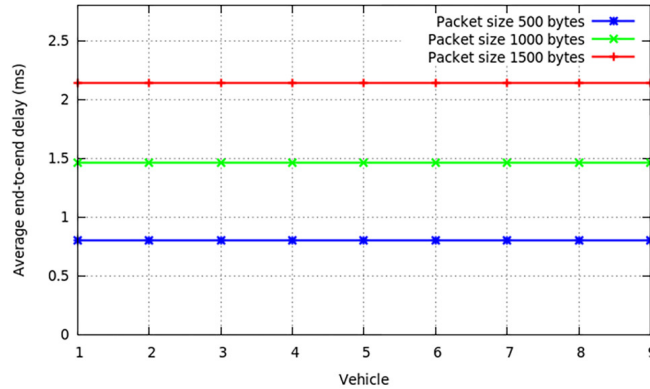


Figure 11. Average end to end delay between vehicle 0 and other vehicles (*packet size : 500, 100, 1500 bytes*)

In the end of this paper, we will evaluate the effect of different routing protocols (DumbAgent, AODV and DSDV) on the performance metrics. For example, we choose in simulation the vehicle 7 with a packet size 500 bytes.

Figure 12 illustrates the throughput of vehicle 7 and figure 13 shows the packet loss between vehicle 0 and vehicle 7 with different protocols. We note that the different protocols give almost the same results in the two figures.

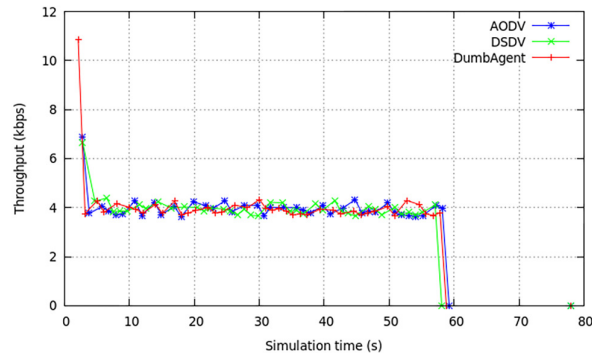


Figure 12. Throughput of vehicle 7 with different protocols (*packet size: 500 bytes*)

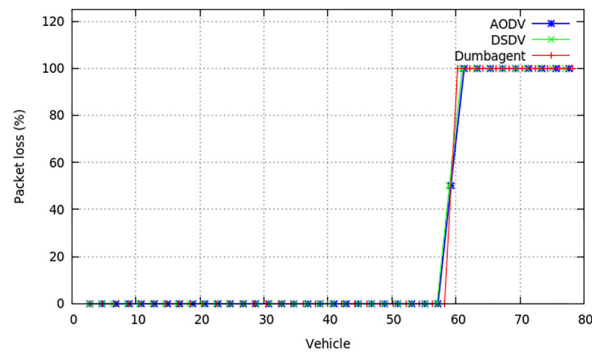


Figure 13. Packet loss between vehicle 0 and vehicle 7 with different protocols (*packet size : 500 bytes*)

The end to end delay between vehicle 0 and vehicle 7 with different protocols is calculated in figure 14. AODV and DumbAgent protocols give the same and the best result compared to DSDV protocol.

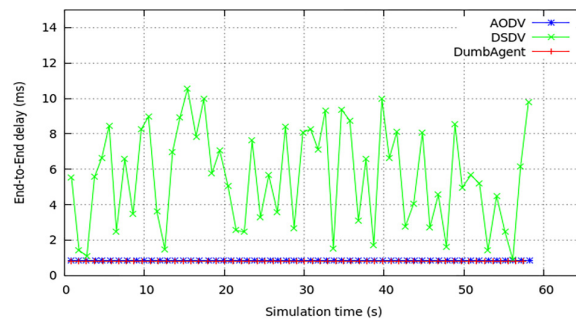


Figure 14. End to end delay between vehicle 0 and vehicle 7 with different protocols (*packet size : 500 bytes*)

We are moving now to present the average performance of metrics to give more realistic results.

Figure 15 presents the average throughput of all vehicles with different protocols. We can say that the throughput results of the different protocols converge with a slight preference for the DumbAgent protocol.

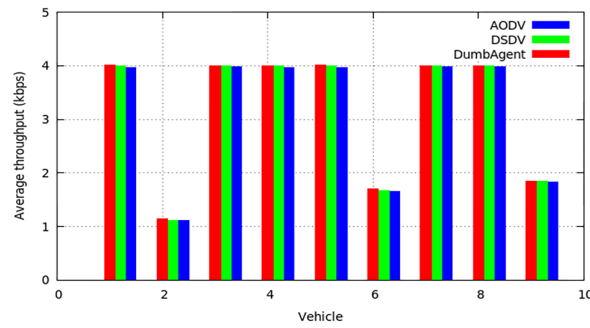


Figure 15. Average throughput of all vehicles with different protocols
(packet size: 500 bytes)

Figure 16 presents the average packet loss of all vehicles with different protocols. All protocols present the same results with some preference to DSDV and DumbAgent protocols in vehicle 3, 4 and 6 compared to AODV protocol.

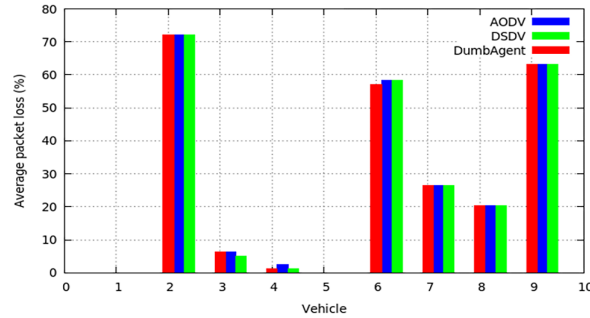


Figure 16. Average packet loss of all vehicles with different protocols
(packet size : 500 bytes)

Figure 17 illustrates the average end to end delay between vehicle 0 and other vehicles with different protocols. It is clear that DSDV protocol has the highest value compared to other protocols. AODV and DSDV protocols are the best in term of end to end delay.

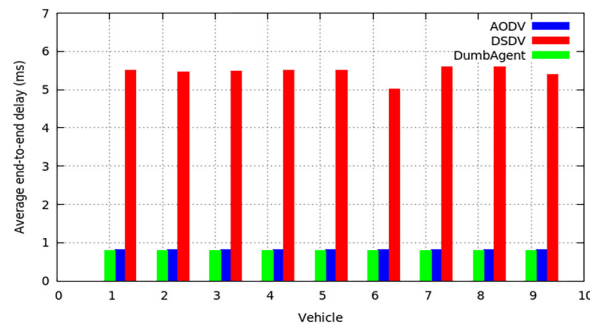


Figure 17. Average end to end delay between vehicle 0 and other vehicles with different protocols (packet size : 500 bytes)

In conclusion, we can say that AODV, DSDV and DumbAgent have the same results in term of throughput and packet loss. AODV and DumbAgent are better than DSDV in term of end to end

delay. DSDV requests a regular update of its routing tables and makes it gourmand in term of end to end delay.

5. CONCLUSION

In this paper, we implemented the standard 802.11p in NS-2 simulator to evaluate the performance of metrics (Throughput, packet loss and end to end delay) of mobility model graph that is generated by VanetMobisim simulator. The performance of metrics is analyzed according to the variation of packet size, exchanged vehicle speed and routing protocols.

From simulation results we can conclude:

- The throughput, the packet loss and the end to end delay are affected by varying the distance between sender and receiver and no by varying the speed of vehicles.
- When the distance between sender vehicle and receiver vehicles is less than 140 meters, the throughput for all vehicles is the same under the condition that the sending power of the signal, the sensitivity of the receivers and the number of cars in the given physical environment are fixed.
- As a result of varying of the packet size: as the packet size increases, the average throughput and the average end to end delay increases as well. When the value of the packet size s multiplied by n then the throughput value and the end to end delay value are multiplied by n also.
- As a result of varying of the routing protocols: AODV, DSDV and DumbAgent have the same results in term of throughput and packet loss but AODV and DumbAgent are better than DSDV in term of end to end delay since the DSDV is very slow in routing.

As a future, we can extend our work for different radio propagation models and environments [18] [19]. We can also change the mobility model graphs to show his effect in the simulation results.

REFERENCES

- [1] S. Al-Sultan, M.M Al-Doori, A.H. Al-Bayatti and H. Zedan, "A comprehensive survey on vehicular ad hoc network", Journal of Network and Computer Applications, London, UK, pp. 380-392, January 2014.
- [2] R. Uzcategui and G. Acosta-Marum, "WAVE: A Tutorial", IEEE Communications Magazine, May 2009.
- [3] J. Harri, F. Filali and C. Bonnet, "Mobility Models for Vehicular Ad Hoc Networks: A Survey and Taxonomy", IEEE Communications Surveys & Tutorials, Vol. 11, No. 4, pp. 19-41, December 2009.
- [4] Y.R.B Al-Mayouf, M. Ismail1, N. F. Abdullah, S.M. Al-Qaraawi and O.A. Mahdi "Survey on Vanet technologies and simulation models", ARPN Journal of Engineering and Applied Sciences, Vol. 11, No. 15, pp. 9414-9427, August 2016.
- [5] F.J. Martinez, C.K. Toh, J.C. Cano, C.T. Calafate and P. Manzoni, "A survey and comparative study of simulators for vehicular ad hoc networks (VANETs)", in Wireless Communications and Mobile Computing, Vol. 11, pp. 813-828, July 2011.

- [6] N.M. Mittal and S. Choudhary, "Comparative Study of Simulators for Vehicular Ad-hoc Networks (VANETs)", *International Journal of Emerging Technology and Advanced Engineering*, Vol. 4, Issue 4, pp. 528-537, April 2014.
- [7] S. Khandelwal, "Comparative Analysis of Network Simulator for Vehicular AdHoc Networks (VANET) Communication", *Journal of Advanced Computing and Communication Technologies*, Vol. 2, No. 2, April 2014.
- [8] "VanetMobiSim", <http://vanet.eurecom.fr>.
- [9] "Network Simulator ns-2", <http://www.isi.edu/nsnam/ns/>IEEE Wireless Communications, Vol. 13, No. 5, pp. 36–43, 2006.
- [10] M. Fiore, J. Haerri, F. Filali and C. Bonnet, "Vehicular Mobility Simulation for VANETs", *Proceedings of the 40th Annual Simulation Symposium*, pp. 301-309, March 2007.
- [11] R.S. Shukla and N. Tyagi, "Performance evaluation of mobility model and routing protocols for inter vehicular communication system", *International Conferene on Emerging Trends in Networks and Computer Communications (ETNCC)*, April 2011.
- [12] D. Shree and D. Singh, "Performance Evaluation of Realistic Mobility Models using Road Side Units", *International Journal of Computer Applications*, Vol. 80, No 15, pp. 0975-8887, October 2013.
- [13] Nidhi and D.K. Lobiyal, "Performance Evaluation of VANET Using Realistic Vehicular Mobility", Chapter in *Advances in Computer Science and Information Technology, Networks and Communications*, Vol. 84 of the series *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering* pp. 477-489, February 2012.
- [14] C.E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers", *ACM SIGCOMM computer communication review ACM*, New York, NY, USA, Vol. 24, pp. 234–244, September 1994.
- [15] C.E. Perkins and E.M. Royer, "Ad-hoc On-Demand Distance Vector Routing ", 2nd IEEE workshop on mobile computing systems and applications, pp. 90-100, February 1999.
- [16] C.E. Perkins, E.M Belding-Royer and S. Das, "Ad hoc on-demand distance vector (AODV) routing", pp. 1721-2070, July 2003.
- [17] M. Treiber, A. Hennecke and D. Helbing, "Congested Traffic States in Empirical Observations and Microscopic Simulations", *Physical Review E*, Vol. 62, pp. 1805– 1824. August 2000.
- [18] D. Dhoutaut, A. R'egis and F. Spies, "Impact of Radio Propagation Models in Vehicular Ad Hoc Networks Simulations", *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, pp. 40-49, September 2006.
- [19] R.C. Poonial and V.Singh, "PERFORMANCE EVALUATION OF RADIO PROPAGATION MODEL FOR VEHICULAR AD HOC NETWORKS USING VANETMOBISIM AND NS-2", *International Journal of Distributed and Parallel Systems (IJDPS)*, Vol. 3, No. 4, July 2012.

INTENTIONAL BLANK

DENIAL-OF-SERVICE ATTACKS AGAINST THE 4-WAY WI-FI HANDSHAKE

Mathy Vanhoef and Frank Piessens

imec-DistriNet, KU Leuven

ABSTRACT

The 4-way Wi-Fi handshake is used to negotiate fresh pairwise keys, and authenticates both the client and Access Point (AP). We analyze this handshake, and discover several new denial-of-service (DoS) attacks against it. Interestingly, our attacks work even if Management Frame Protection (MFP) is enabled.

The first attack abuses the observation that messages in the 4-way handshake undergo link-layer encryption once the pairwise key is installed. More precisely, when message 4 of the handshake is dropped, the handshake times out. The second attack is similar to the second one, but induces the AP into sending the first message 4 with link-layer encryption. Again, this causes the handshake to time out. In the third attack, an adversary waits until the victim completes the 4-way handshake. Then she initiates a rekey by injecting a malformed 4-way handshake messages, causing several implementations to disconnect the client from the network. Finally, we propose countermeasures against our discovered attacks.

KEYWORDS

Network Protocols, Wi-Fi, 802.11, Denial-of-Service attacks, 4-way handshake

1. INTRODUCTION

Nowadays, wireless networks are usually based on the 802.11 standard, which is more widely known under the name Wi-Fi. This standard has gained major attraction over the years, and is currently used in a plethora of scenarios, ranging from personal use to reliability-critical industrial use. Because adversaries can monitor (and interfere with) wireless transmissions remotely, it is essential to protect the privacy and security of transmitted data. Initially, the 802.11 standard provided Wired Equivalent Privacy (WEP) to protect data. Unfortunately, it contained major design flaws, and is considered completely broken [1, 2, 3]. Instead, nearly all modern networks rely on Wi-Fi Protected Access (WPA) to encrypt data [4].

Both version 1 and 2 of WPA use a 4-way handshake for authentication, and for the negotiation of fresh pairwise keys. Even Wi-Fi networks that use 802.1x authentication, i.e., those that require a username and password, will use the 4-way handshake during the last step of the connection phase. As a result, it is critical that the 4-way handshake is reliable, and does not contain any security flaws. Given its high importance, several works have formally analyzed the security of this handshake [5, 6, 7]. However, even though these works discovered and addressed

one denial-of-service (DoS) attack against the 4-way handshake, in practice implementations of the handshake still contain several deficiencies. In this work, we perform a detailed study of implementations of the 4-way handshake, and discover several new denial-of-service attacks against it.

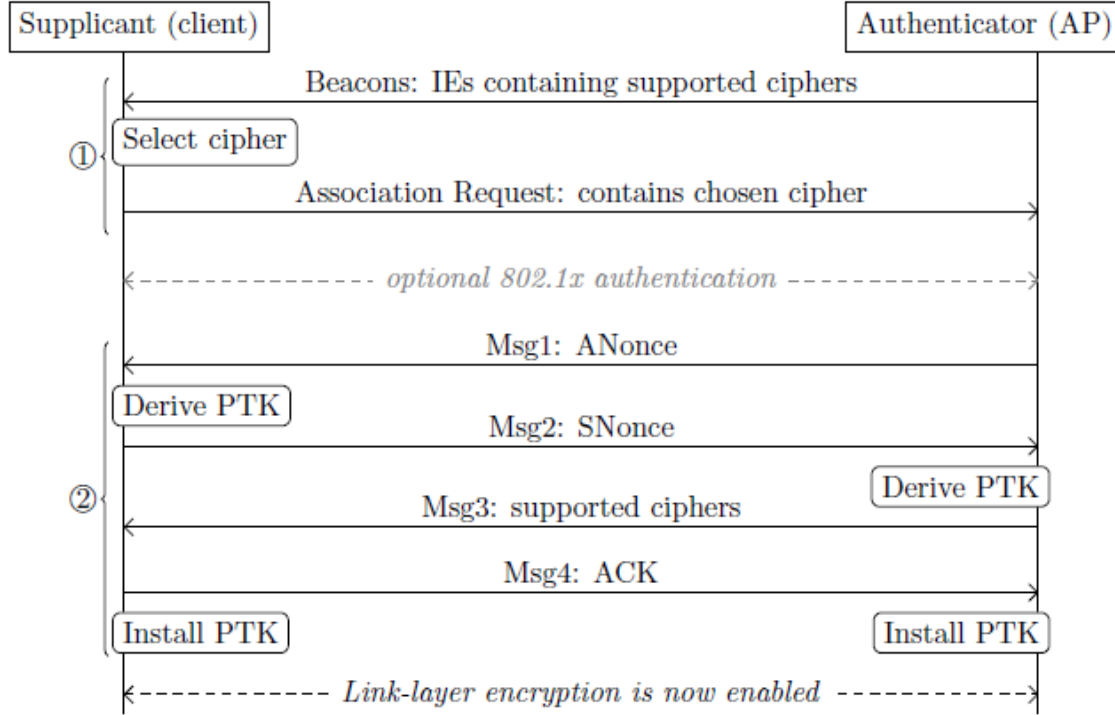


Figure 1: Simplified overview of the messages exchanged when connecting to a network, including the actions of the client (supplicant) and AP (authenticator). The 4-way handshake is illustrated in stage 2.

The remainder of this paper is structured as follows. First, Section 2 introduces the 4-way handshake and Management Frame Protection (MFP). Our novel denial-of-service attacks against the 4-way handshake are presented in Section 3. In Section 4 we propose countermeasures to the identified attacks. Finally, we present related work in Section 5 and conclude in Section 6.

2. BACKGROUND

In this section we first explain how stations discover nearby networks. Then we introduce the 4-way handshake, and its high-level interaction with link-layer confidentiality protocols. Finally, we explain how the Management Frame Protection (MFP) amendment of 802.11 works.

2.1. Network Discovery

An Access Point (AP) periodically broadcasts beacons to advertise its presence. This is illustrated in stage 1 of Figure 1. These beacons include the supported link-layer encryption algorithms (i.e., the supported ciphers) that are supported by the AP. This is either the Temporal Key Integrity Protocol (TKIP) or the CTR CBC-MAC Protocol (CCMP). When a client wants to connect to an

AP, and has selected a supported encryption algorithms to use, it sends an association request to the AP. This association request contains the encryption algorithm (cipher) selected by the client.

2.2. The 4-way Handshake

In order to start the 4-way handshake, the client and Access Point (AP) must first possess a shared secret called the Pairwise Master Key (PMK). The PMK is commonly derived from a pre-shared key, or from an 802.1X handshake. The 4-way handshake verifies that both entities possess the same PMK, generates a fresh Pairwise Transient Key (PTK), and confirms the selection of the cipher suite. It also synchronizes the installation of the PTKs. Note that once a PTK has been installed, all traffic is encrypted at the link-layer.

Stage 2 of Figure 1 shows the messages exchanged during the 4-way handshake. Simplified, the first two messages contain random nonces to generate a fresh PTK, and the last two messages protect against downgrade attacks. The handshake messages are defined using EAPOL frames, and we use the notation message *n* to refer to a specific message. After the client has transmitted message 4, it installs the PTK, while the AP installs the PTK after receiving message 4. Finally, to handle missed frames, the AP will retransmit the previous message if it did not receive a response. If the client already received this message, it will transmit a new response.

Finally, in an existing connection it is possible to rekey the PTK by executing a new 4-way handshake. During this rekey handshake, the EAPOL frames undergo link-layer encryption using the currently installed PTK.

2.3. Management Frame Protection (MFP)

A client can disconnect from a network by sending a deauthentication or disassociation frame to the AP. By default, these messages are not authenticated. As a result, an adversary can forge them to forcibly disconnect a client from a network. Continuously injecting these forged deauthentication packets causes a denial-of-service attack [8]. Fortunately, this attack can easily be prevented by using Management Frame Protection (MFP). This feature was introduced in the 802.11w amendment of the 802.11 standard. When this amendment is enabled, an adversary can no longer forge deauthentication or disassociation frames in order to disconnect a client.

3. DENIAL-OF-SERVICE (DoS) ATTACKS

In this section we present three novel denial-of-service (DoS) attacks against implementations of the 4-way handshake. The first exploits a race condition between installing the pairwise key and sending message 4. In the second attack we make the handshake fail by blocking message 4. Finally, we also discovered that injecting a malformed message 1 can cause the client to disconnect from the AP.

3.1. Encrypted Message 4 Race Condition

In the 802.11 standard, installing the PTK and sending an EAPOL message are both done by calling primitives in the MAC Sublayer Management Entity (MLME). However, in an actual implementation, these MLME primitives do not have to correspond similar interfaces [9, x6.3.1]. In practice, we indeed see that several operating systems use different kernel interfaces for

installing the PTK and sending EAPOL messages. For instance, on Linux the nl80211 kernel interface is can be used to install the PTK, while the handshake messages are transmitted by the sendto system call. This means there is no guarantee in which order these two actions will be performed, and hence the PTK may be installed before message 4 is transmitted [10]. Additionally, message 4 may still be queued for transmission due to a busy medium, while the PTK is already being installed. As a result message 4 may undergo link-layer encryption, and will therefore be rejected by the AP. This will eventually cause the handshake to time out.

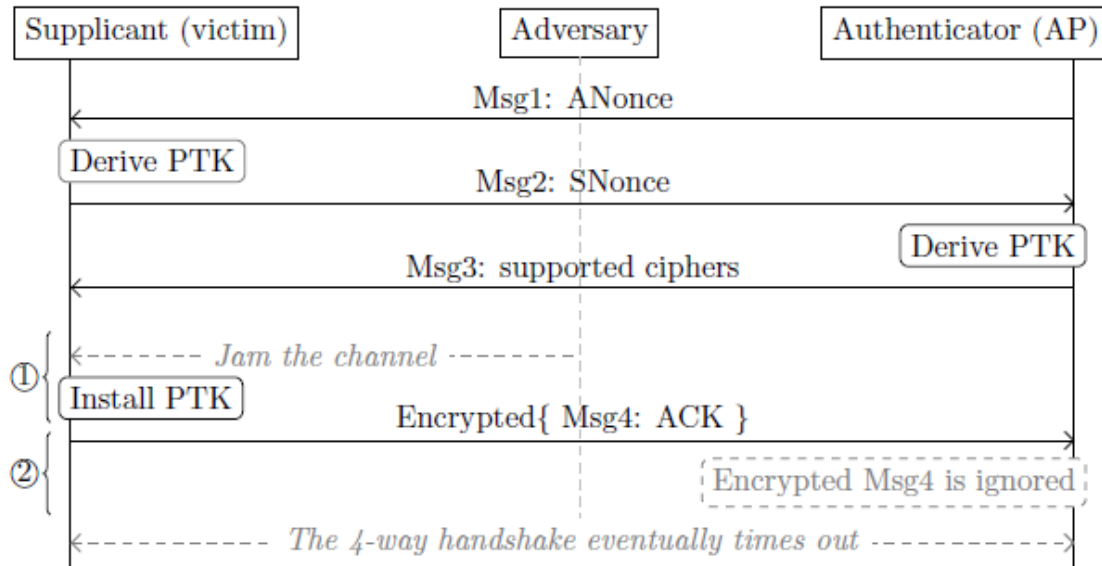


Figure 2: Encrypted message 4 race condition. Here the victim is induced into installing the pairwise key (PTK) before sending message 4.

Figure 2 illustrates this attack more clearly. At stage 1 of the attack, the adversary briefly jams the wireless channel. As a result, the victim queues message 3 for transmission until the wireless channel is no longer busy, i.e., until the adversary stops jamming. While message 4 is queued, the victim already installs the pairwise key. When the adversary now stops jamming, the victim will send message 4 using link-layer encryption, since the PTK has already been installed. However, the AP has not yet installed the pairwise key, and therefore will reject frames that underwent link-layer encryption. This is illustrated in stage 2 of Figure 2. Since the AP never receives message 3, the 4-way handshake will eventually time out. We tested this attack against OpenBSD 6.0, which was acting as a client using a Sitecom WL-172 v1 wireless NIC, and confirmed the vulnerability.

3.2. Blocked Message 4

If message 4 of the handshake does not reach the AP, the handshake will never successfully complete. This is because the client installs the PTK after transmitting message 4, meaning it now only accepts frames that are encrypted at the link-layer. However, the AP will retransmit message 3 without link-layer encryption when it did not receive message 4. The client rejects this unencrypted message 3, and hence will not retransmit message 4. Eventually, the AP reaches its retransmission limit, and will abort the handshake. An attacker can abuse this as an e

cient denial-of-service attack, by selectively jamming message 4. Note that selectively jamming frames is possible using cheap Wi-Fi USB dongles [11].

Figure 3 illustrates this attack. During state 1 of the attack, the adversary blocks message 4 from arriving at the AP using a selective jammer. Immediately after the victim transmitted message 4, she will install the pairwise key (PTK). At this point, the victim only accepts frames that are encrypted at the link-layer. When the AP now retransmits message 3 without link-layer encryption, the victim will reject it. This is illustrated in stage 2 of Figure 3. Finally, since the AP never receives message 4 of the handshake, the handshake will eventually time out and be aborted.

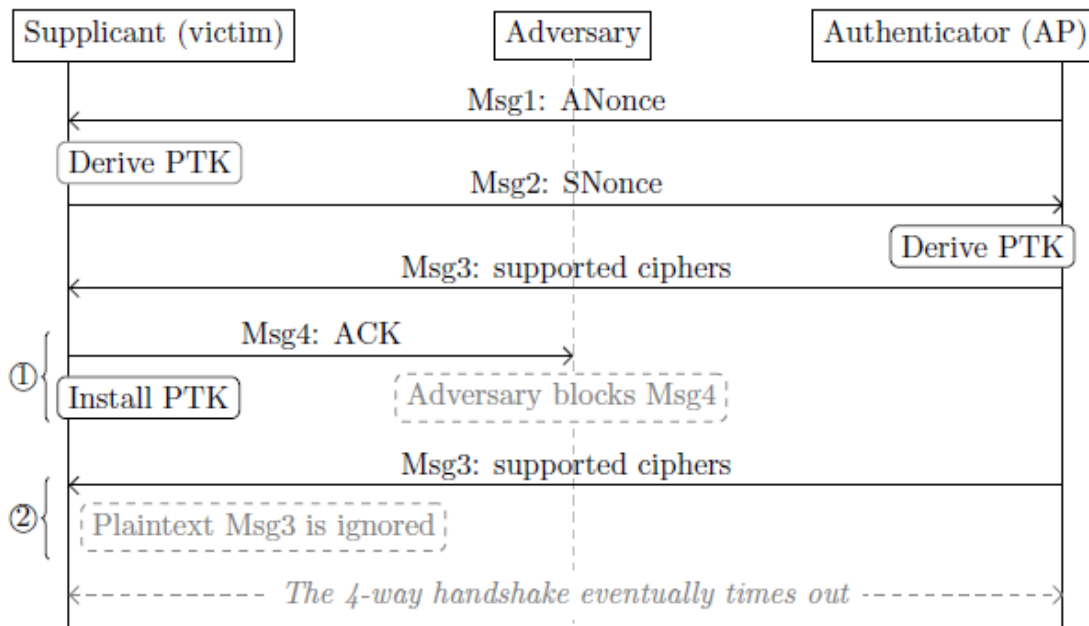


Figure 3: Blocked message 4 attack. The first transmission of message 4 is blocked, after which the victim installs the PTK, meaning retransmissions of message 3 will be ignored.

We remark that some implementations of the 4-way handshake always accept plaintext handshake messages, even when a PTK has been installed. That is, by testing several implementations, we discovered that some accept plaintext EAPOL frames (i.e., handshake frames) at any moment (see column 2 in Table 1). Allegedly this is done because some implementations transmit certain EAPOL frames without link-layer encryption (e.g. group key updates), even though both the client and AP already installed the PTK [12]. Even if plaintext handshake messages are always accepted, the attack in Figure 3 still causes a denial-of-service. This is because nearly all implementations will transmit message 4 using link-layer encryption once a PTK has been installed, and the AP will reject these frames since it did not yet install the PTK (similar to the attack in Figure 2). Interestingly, this behaviour contradicts the 802.11 standard. More precisely, the standard states that in the initial 4-way handshake, message 4 should always be sent without link-layer encryption [9, x11.6.6.5]. However, few implementations follow this requirement. Only MediaTek (re)transmits message 4 without link-layer encryption (see column 3 in Table 1).

3.3. Failed Rekey Using a Malformed Message 1

In the previous section we observed that several implementations accepted plaintext EAPOL frames, even though they already installed the PTK (recall column 1 in Table 1). We can abuse this behaviour to inject a forged message 1 towards the client. Note that this is valid behavior, since the AP can decide at any moment to refresh the pairwise keys (PTK) by starting a new 4-way handshake. More importantly, if this message contains invalid or malformed data, the client will abort the handshake, and subsequently disconnect from the network.

One way to create a malformed message 1, is by including an invalid PMKID alongside the ANonce (see stage 1 of Figure 4). Recall from section 2 that the PMK is the shared secret between the client and AP, and can either be derived from a preshared key, or from an 802.1X authentication. In general though, it is possible for the client and AP to share multiple valid PMKs. Therefore, the first message of the 4-way handshake may include a PMKID, which identifies the specific PMK that will be used [9, x11.6.6.2]. Note that the PMKID is essentially just a hash of the secret PMK. Interestingly, we found that many clients will abort the handshake and disconnect from the network when message 1 contains an unknown PMKID. Hence an adversary can cause a denial-of-service during an initial 4-way handshake, by injecting a message 1 with an unknown PMKID. Additionally, if the victim always accepts plaintext EAPOL frames, this message can even be injected after the initial 4-way handshake completed. Put differently, then our denial-of-service attack works even when the client has already installed the PTK. This attack latter variant of the attack is illustrated in stage 1 Figure 4, where the adversary injects a plaintext message 1 while the victim already installed a PTK.

In contrast to injecting deauthentication frames to disconnect a client, injecting a malformed message 1 is possible even if Management Frame Protection (MFP) is enabled. Indeed, if MFP is enabled, an adversary cannot forge deauthentication or disassociation frames. However, message 1 of the handshake can still be forged, and hence can still be abused to perform an efficient denial-of-service attack.

We tested this attack against Linux's `wpa_supplicant`. This confirmed that the client aborts the handshake and disconnects from the network when receiving a message 1 containing an invalid PMKID.

Table 1: Behaviour of several 4-way handshake implementations. The second column shows whether EAPOL frames that did not undergo link-layer encryption are accepted even if a PTK is installed. The third column shows whether message 4 is retransmitted without link-layer encryption during an initial 4-way handshake.

Implementation	Plaintext Reception	Plaintext (Re)transmission
FreeBSD	Yes	No
NetBSD	Yes	No
OpenBSD	No	No
Linux	Yes	No
Android	Yes	No
Windows	No	No
Apple	No	No
MediaTek	Yes	Yes
Broadcom	No	No

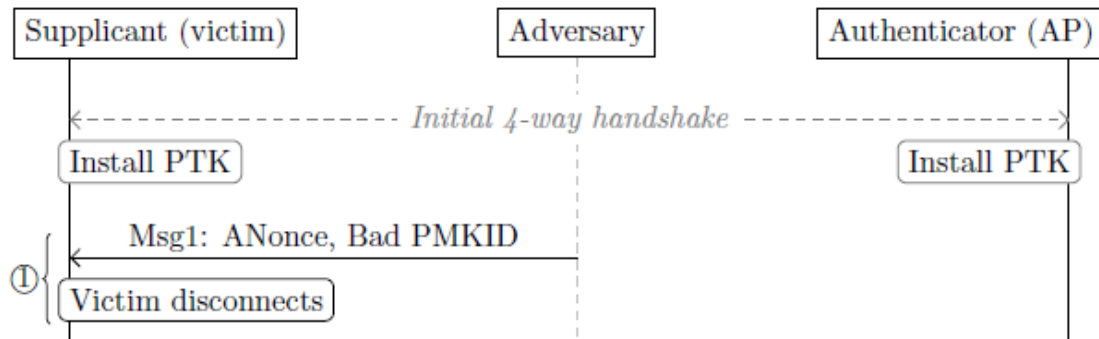


Figure 4: Instigating a failed rekey using a malformed message 1. This messages contains an invalid PMK ID, and in response the victim will disconnect from the AP.

4. PROPOSED COUNTERMEASURES

In this section, we propose countermeasures against the denial-of-service attacks we discovered, and explain their advantages and disadvantages.

4.1. Plaintext EAPOL Frames

The first two issues discussed in Section 3 can be dealt with simultaneously. In particular, we can simply send all EAPOL frames without link-layer encryption. Note that this does not negatively impact security, because sensitive information in EAPOL frames is already encrypted, and the full frame is also authenticated. Hence link-layer encryption is not required to protect the EAPOL frames used in the 4-way handshake. Not encrypting EAPOL frames at the link-layer is also consistent with RFC 5247, which states that "presence or absence of lower layer security is not taken into account in the processing of EAP messages" [13, x3.4]. Additionally, the formal security proof of the 4-way handshake also not require link-layer encryption. In other words, it is safe to send all EAPOL frames without link-layer encryption [5].

Unfortunately, only sending plaintext EAPOL frames introduces some compatibility issues. In particular, some implementations require that these frames are encrypted during a rekey. Sending them without encryption would therefore break compatibility. Nevertheless, in a first step, implementations can be modified so they always accept plaintext EAPOL frames. Additionally, they should always send plaintext EAPOL frames during the initial 4-way handshake even if a PTK is already installed. This does not introduce compatibility issues, but does solve the encrypted message 4 race condition, as well as the dropped message 4 issue of Section 3. Once most implementations accept plaintext EAPOL frames at any moment, we can also send plaintext EAPOL frames during a rekey.

4.2. Handling a Malformed Message 1

To prevent the malformed message 1 attack of Section 3.3, an implementation should ignore such malformed messages. This is the approach that OpenBSD is currently using. There, if the client receives a malformed handshake message, it is simply dropped. Hence the client remains connected to the network, awaiting the real message 1 from the AP.

Another modification that should be made is that, during a rekey handshake, the authenticity of message 1 should be validated by the currently installed PTK. Note that during the initial 4-way handshake, message 1 is sent unauthenticated, since the AP does not yet know the PTK (recall Figure 1). However, during a rekey we can authenticate message 1 using the PTK that was negotiated in the previous 4-way handshake. This assures an adversary cannot forge any handshake messages once the initial 4-way handshake has completed.

5. RELATED WORK

Several works have analyzed the security of the 4-way handshake [5, 6, 7, 14]. In particular, He et al. discovered a denial-of-service vulnerability [5, 7], which led to the standardization of a slightly improved design of the 4-way handshake [15]. In their DoS attack, the adversary injects a forged message 1 using a different ANonce than the one the real AP is using. This causes the client to generate an invalid PTK, making the handshake fail. The solution is to make the client always use the same SNonce in a specific handshake, and to verify the ANonce when receiving message 3 of the handshake [5]. Note that message 3 is authenticated, and hence cannot be forged by an attacker. The advantage of our DoS attacks is that they are not yet addressed in the official 802.11 standard, and that several implementations are still affected by them.

Several other DoS attacks also exist against Wi-Fi networks that abuse different parts of the protocol. Arguably the most well-known of these is a deauthentication attack, where an adversary forges deauthentication frames to disconnect the client from the network [16]. This is possible because, by default, these messages are not authenticated. However, nowadays this attack can easily be prevented by enabling protected management frames [9, 802.11-4.5.4.9]. In contrast, our attacks remain possible even when protected management frames is enabled.

Several DoS attacks also exploit weaknesses in the link-layer encryption protocol called TKIP. In particular, Glass and Muthukkumarasamy [17] abuse the TKIP Michael countermeasures to make a Wi-Fi network unusable for one minute. Vanhoef and Piessens improved this attack, by removing the requirement of a man-in-the-middle position [4]. The advantage of our DoS attacks is that they can be executed on any Wi-Fi network, even if the network does not support the TKIP encryption algorithm.

Finally, Konings et al. found several DoS vulnerabilities in the physical and MAC layer of 802.11 [19]. Some of these make the network unusable for one minute, while others only do so for a brief amount of time. A survey of DoS attacks at the physical and MAC layer is given by Bicakci and Tavli [20]. Generally, these attacks require injecting a large amount of frames, while our attacks require a lower amount of packets to be injected.

6. CONCLUSION

Implementations of the 4-way handshake (still) contain several denial-of-service vulnerability. This in spite of previous analysis and security proofs of the 4-way handshake. Our attacks can be mitigated by always sending and accepting plaintext EAPOL frames. Because this may introduce compatibility issues, we first recommend doing this only during the initial 4-way handshake. This does not introduce compatibility issues, while already making the initial 4-way handshake more secure and robust. In a second step, implementations can also send plaintext EAPOL frames

during a rekey. Finally, when implementations receive a malformed message 1, e.g., if the message contains an unknown PMKID, the message should be ignored and dropped.

REFERENCES

- [1] S. R. Fluhrer and D. A. McGrew, "Statistical analysis of the alleged RC4 keystream generator," in FSE, 2000.
- [2] A. Stubblefield, J. Ioannidis, A. D. Rubin, et al., "Using the uhrer, mantin, and shamir attack to break wep.," in NDSS, 2002.
- [3] A. Bittau, M. Handley, and J. Lackey, "The final nail in WEP's coffin," in IEEE SP, 2006.
- [4] M. Vanhoef and F. Piessens, "Practical verification of WPA-TKIP vulnerabilities," in ASIA CCS, pp. 427-436, ACM, 2013.
- [5] C. He and J. C. Mitchell, "Analysis of the 802.11i 4-Way handshake," in WiSe, ACM, 2004.
- [6] C. He, M. Sundararajan, A. Datta, A. Derek, and J. C. Mitchell, "A modular correctness proof of IEEE 802.11i and TLS," in CCS, 2005.
- [7] J. Mitchell and C. He, "Security analysis and improvements for IEEE 802.11i," in NDSS, 2005.
- [8] S. Park, K. Kim, D. Kim, S. Choi, and S. Hong, "Collaborative QoS architecture between DiffServ and 802.11e wireless LAN," in Vehicular Technology Conference, 2003.
- [9] IEEE Std 802.11-2012, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Spec, 2012.
- [10] J. Malinen, "wpa keyhandshake question / bug." Retrieved 19 March 2017 from <http://lists.shmoo.com/pipermail/hostap/2005-May/010370.html>, 2005.
- [11] M. Vanhoef and F. Piessens, "Advanced Wi-Fi attacks using commodity hardware," in ACSAC, 2014.
- [12] J. Malinen, "Re: Dealing with retransmitted EAPOL msg 3/4 and 4/4." Retrieved 19 March 2017 from www.spinics.net/lists/hostap/msg03309.html, 2017.
- [13] B. Aboba, D. Simon, and P. Eronen, "Extensible authentication protocol (EAP) key management framework." RFC 5247, 2008.
- [14] L. Wang and B. Srinivasan, "Analysis and improvements over DoS attacks against IEEE 802.11i standard," in NSWCTC, 2010.
- [15] IEEE Std 802.11-2016, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Spec, 2016.
- [16] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions," in Proc. of the 12th USENIX Security Symp., 2003.
- [17] S. M. Glass and V. Muthukkumarasamy, "A study of the TKIP cryptographic dos attack," in 15th International Conference on Networks, IEEE, 2007.

- [18] M. Morii and Y. Todo, "Cryptanalysis for RC4 and breaking WEP/WPA-TKIP," IEICE Transactions, pp. 2087{2094, 2011.
- [19] B. Konings, F. Schaub, F. Kargl, and S. Dietzel, "Channel switch and quiet attack: New DoS attacks exploiting the 802.11 standard," in LCN, 2009.
- [20] K. Bicakci and B. Tavli, "Denial-of-service attacks and countermeasures in IEEE 802.11 wireless networks," Comput. Stand. Interfaces, vol. 31, no. 5, 2009.

CFAR DETECTION IN MIMO RADARS USING FUZZY FUSION RULES IN HOMOGENEOUS BACKGROUND

Faycal Khaldi¹ and Faouzi Soltani²

^{1,2}Département d'électronique, Université des Frères Mentouri Constantine
Constantine 25000, Algeria

ABSTRACT

In this paper, we propose to use fuzzy fusion rules to improve the performances of the Cell Averaging Constant False Alarm Rate (CA-CFAR) detector for MIMO (Multiple Input Multiple Output) radars in homogenous background modeled by a Pareto distribution. We compute the membership function for each individual detector. The global membership function at the fusion centre is a combination of the membership functions collected from individual detectors using four fusion rules, namely; the “MIN”, “MAX”, “algebraic product” and the “algebraic sum”. By means of Monte Carlo simulations, we evaluated the performance of the global system. The obtained results showed that for a number of nodes equal to four, the performance is the best for a high number of receivers and a low number of transmitters. For the best case and in homogenous background, the “algebraic product” fusion rule gives the best result when SNR >4 dB whereas the “algebraic sum” is the best when SNR <4 dB for the CA-CFAR.

KEYWORDS

Radar detection, MIMO, Fuzzy rules, Homogeneous clutter, CFAR

1. INTRODUCTION

A MIMO radar structure is a multi-antenna radar system which consists of using multiple antennas at the transmitter and the receiver. It is therefore a generalization of the concept of multi-static radars [1].

This technique was first used in communications and has recently been extended to radars where the received signals are jointly processed at the multiple receiving antennas. It has the advantage of improving radar performance, in terms of the regulation of the false alarm rate and the maximization of the probability of detection [2]. MIMO radars are, generally divided into two types; the coherent MIMO radar “co-located” and the statistical MIMO radar “widely separated”. The statistical MIMO radar takes advantage of the spatial diversity in the transmit and receive angles to enhance the detection performance.

The difference between the two configurations is the signal model: For Widely Separated antennas, the spatial properties of extended targets are exploited while the target is modelled as a point with no spatial property for coherent MIMO radars [3].

In radar automatic detection system, the main goal is to design an algorithm that set the threshold adaptively to deal with the changing power of the clutter and to keep the false alarm rate constant and at a desired value.

The performances of the CA-CFAR approaches those of the optimum detector if the reference cells are Gaussian, independent and identically distributed (iid).

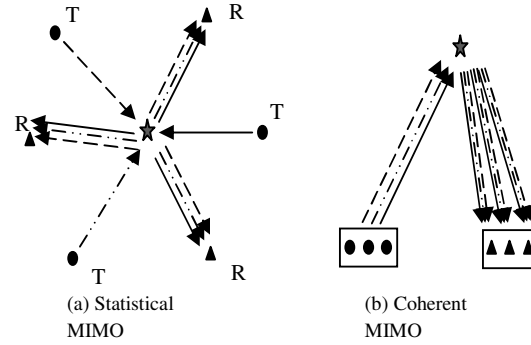


Figure. 1 MIMO radar concept.

In practical situations, the clutter may not be homogeneous. This non homogeneity is caused by either the presence of interfering targets or an extended clutter edge. In this case, the performance of the CA-CFAR degrades seriously. In order to overcome this problem, several modified versions of the CA-CFAR detector were proposed and are generally based on the order statistic technique: the OS-CFAR [4], the GOSCA-CFAR [5], the OSGO-CFAR and the OSSO-CFAR [6].

Several works dealing with target detection in MIMO radars in the Neyman-Pearson sense [7, 8] or using the Generalized Likelihood Ratio [9] have been reported in the literature.

In [10], Janatian generalized the CA-CFAR, the SO-CFAR, the OS-CFAR and the ACMLD (Automatic Censored Mean-Level Detector) for a Gaussian background. Widely Separated MIMO radars were used in homogeneous and non-homogeneous clutter (presence of interfering targets).

Using INGARA database, Weinberg [11] showed that the Pareto distribution offers a good fitting performance as a model for high-resolution high-grazing angle sea clutter.

This paper deals with the analysis of the performance of Widely Separated MIMO radars where the individual detectors are the CA-CFAR detector. Instead of using binary fusion rules, we propose to extend this technique to the use fuzzy fusion rules at the fusion centre. The clutter is assumed to follow a Pareto distribution.

The rest of the paper is organized as follow: section 2 describes the signal model in MIMO radars. In section 3, we analyze the fuzzy CA-CFAR detector in MIMO radars in a Pareto clutter. The results concerning the performance of the MIMO structure in homogeneous clutter are presented and commented in section 4 and followed by some concluding remarks in section 5.

2. SIGNAL MODEL IN MIMO RADARS

The structure under consideration is a MIMO radar system that has M transmit antennas and N receive antennas. The antennas are assumed to be widely separated as shown in Fig. 1.a. It is also assumed that the m^{th} transmitter delivers a signal $\sqrt{E/M} s_m(t)$, where E is the total transmitted power and $\|s_m(t)\|^2 = 1$. That is, systems with a reduced number of nodes (couples Tx-Rx) have an increased available power per node. In other words, each of the M transmitters provides a power equal to $\frac{E}{M}$. The n^{th} received signal is modelled as follows:

$$r_n(t) = \sum_{m=1}^M \alpha_{m,n}(\sigma) s_m\left(t - \frac{R_{m,n}}{c}\right) + e_n(t). \quad (1)$$

Where $s_m(t)$ is the m^{th} transmitted signal, $e(t)$ is an additive thermal noise, $\alpha_{m,n}$ is a complex coefficient including the amplitude and the phase of the received signal and is given by the following expression.

$$\sqrt{\frac{E}{M}} \sqrt{\frac{G_t G_r \lambda_m^2 \sigma}{(4\pi)^3 R_m^2 R_n^2}} \exp\left(-j \frac{2\pi R_{m,n}}{\lambda_m}\right). \quad (2)$$

If the transmitted waveforms are assumed to be orthogonal in such a way that they can be separated in each receiver, the received signal after the matched filtering can be expressed as:

$$q_{m,n} = \alpha_{m,n} + n_{m,n}. \quad (3)$$

The MIMO radar detection problem can be formulated in terms of the binary hypothesis test as follow:

$$Q_0 = \begin{cases} n, & H_0 \\ \alpha + n, & H_1 \end{cases}.$$

Under hypothesis H_0 , the target is declared absent in the received signal and the signal is constituted of clutter only. Under hypothesis H_1 , a target is declared present and the received signal is the sum of both target and clutter signals.

The classical Neyman-Pearson detector uses the Likelihood ratio test and is given by:

$$T(q_0) = \text{Log} \frac{P(q_0/H_1)}{P(q_0/H_0)} \geq \gamma. \quad (4)$$

Where $P(q_0|H_1)$ and $P(q_0|H_0)$ are the probability density functions of the observation vector under the hypothesis H_1 or H_0 respectively. The threshold γ is determined by a prescribed probability of false alarm.

The Likelihood ratio test in (4) is equivalent to the following test [2]:

$$\|Q_0\|^2 \geq \gamma. \quad (5)$$

Where Q_0 is the matched filter output of the cell under test (CUT). For a CA-CFAR detector, $\|Q_0\|^2$ is the sum of the CUT powers, $\gamma = T * Z$ is the detection threshold, Z is the noise power level estimation and T is a factor that adjusts the P_{fa} at a desired value.

The structure of the received data is shown in Fig. 2. The range gating method is employed in only one angular-resolution cell (Fig. 2.a). Each receiver can sense the echoes of all transmitters and therefore, this structure can be formulated as a matrix with $M \times N$ columns and each column contains a CUT (grey cells) plus $2 \times L$ reference cells as shown in Fig. 2.b.

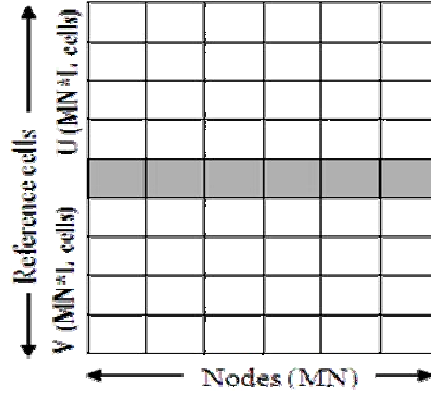
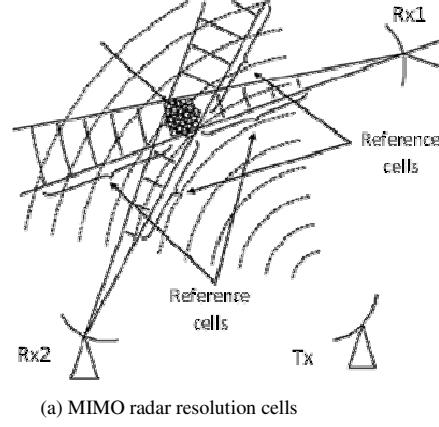


Figure 2 MIMO Radar Concept

3. FUZZY CA-CFAR DETECTOR FOR MIMO RADARS

3.1. Fuzzy CA-CFAR Detector in Pareto Clutter

A block diagram of the fuzzy CA-CFAR detector under consideration is shown in Fig. 3. The received signal is sampled in range by the range resolution cells. The statistics which is the membership function is compared to a threshold to decide about the presence or the absence of a target.

The clutter is assumed to be modeled by a Pareto distribution which is defined as follows:

$$f_X(x) = \frac{\alpha \beta^\alpha}{x^{\alpha+1}} \quad (6)$$

Where α is the shape parameter and β the scale parameter.

In the CA-CFAR detector, the membership function to the false alarm space is given by [12]

$$\mu(z) = P(R > z / H_0) \quad (7)$$

Where

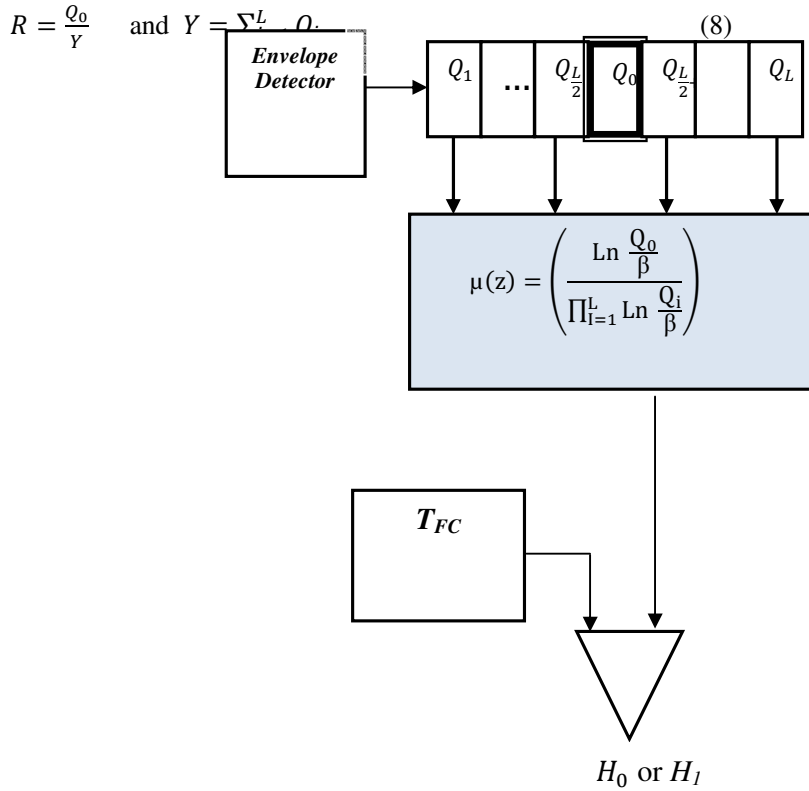


Figure. 3 Block Diagram of the fuzzy CA-CFAR detector

Since the clutter obeys to a Pareto distribution, it was shown that the following transformation leads to an exponential distribution

$$Q_i \simeq \beta e^{X_i} \quad (9)$$

Where Q_i follows a Pareto distribution with parameters α and β , $Q_i \simeq Pa(\alpha, \beta)$ and X_i follows an exponential distribution with parameter α , $X_i \simeq exp(\alpha)$

The decision rule concerning a fuzzy CA-CFAR detector is given by []

$$\mu: X \rightarrow \begin{cases} 1 & \frac{X_0}{\sum_{i=1}^L X_i} > T \\ 0 & \frac{X_0}{\sum_{i=1}^L X_i} < T \end{cases} \quad (10)$$

Using the transformation in (9), the decision rule becomes

$$\mu: Q \rightarrow \begin{cases} 1 & \frac{Q_0}{\prod_{i=1}^L Q_i} > T \cdot \beta^{1-L} \\ 0 & \frac{Q_0}{\prod_{i=1}^L Q_i} < T \cdot \beta^{1-L} \end{cases} \quad (11)$$

The membership function to the false alarm space is then

$$\mu(z) = Prob \left(\frac{Ln \left(\frac{Q_0}{\beta} \right)}{\prod_{i=1}^L Ln \left(\frac{Q_i}{\beta} \right)} > T / H_0 \right) \quad (12)$$

Using the results in [12], the membership function reduces to

$$\mu(z) = \frac{1}{(z + 1)^L} \quad (13)$$

3.2. Fuzzy Fusion Rules in MIMO Radars

The number of fuzzy decisions (D_1, D_2, \dots, D_{MN}) is equal to the number of nodes $M.N$ where M is the number of transmitters and N is the number of receivers. Each node transmits its membership function to the fusion centre where a global membership function μ_{FC} is derived. The fuzzy fusion rules considered in this work are “MIN”, “MAX”, “Algebraic sum” and “Algebraic product”.

- 1) The “MIN” fusion rule

The membership function at the fusion centre, μ_{FC} is defined as

$$\mu_{FC} = MIN(\mu_{D_1}, \mu_{D_2}, \dots, \mu_{D_{MN}}) \quad (14)$$

The corresponding threshold at the fusion centre is [12]

$$T_{FC} = 1 - (1 - Pfa)^{\frac{1}{MN}} \quad (15)$$

- 2) The “MAX” fusion rule

For this rule, μ_{FC} is defined as

$$\mu_{FC} = MAX(\mu_{D_1}, \mu_{D_2}, \dots, \mu_{D_{MN}}) \quad (16)$$

The corresponding threshold at the fusion centre is [12]

$$T_{FC} = Pfa^{\frac{1}{MN}} \quad (17)$$

- 3) The “Algebraic sum” fusion rule

Following the same reasoning as previously, μ_{FC} is found to be

$$\mu_{FC} = 1 - \prod_{i=1}^{MN} (1 - \mu_{D_i}) \quad (18)$$

The corresponding threshold at the fusion centre is obtained from the Pfa expression [13]

$$Pfa = 1 - \frac{\Gamma(MN, -\ln(1 - T_{FC}))}{(MN-1)!} \quad (19)$$

4) The “Algebraic product” fusion rule

In this case, μ_{FC} is defined as

$$\mu_{FC} = \prod_{i=1}^{MN} (1 - \mu_{D_i}) \quad (20)$$

The corresponding threshold at the fusion centre is obtained from the Pfa expression [13]

$$Pfa = \frac{\Gamma(MN, -\ln(1 - T_{FC}))}{(MN-1)!} \quad (21)$$

4. RESULTS AND DISCUSSIONS

To demonstrate the effectiveness of using fuzzy fusion rules in a MIMO structure, we used Monte-Carlo simulations to assess the detection probability (P_D) as a function of the signal-to-clutter ratio (SCR). We assume that the number of reference cells is $L=16$, the design P_{fa} is equal to 10^{-4} and the clutter is homogeneous. We also assume that the number of nodes MN is equal to 4 with three different cases ($M=4$ and $N=1$, $M=2$ and $N=2$, $M=1$ and $N=4$). For the four fusion rules considered, the thresholds at the fusion centre are calculated using expressions (15), (17), (19) and (21).

Fig. 4 shows the detection performance with respect to M and N . It is clear that the highest P_D is obtained for $M=1$ and $N=2$. In general, the performance increases as the number of receivers increases.

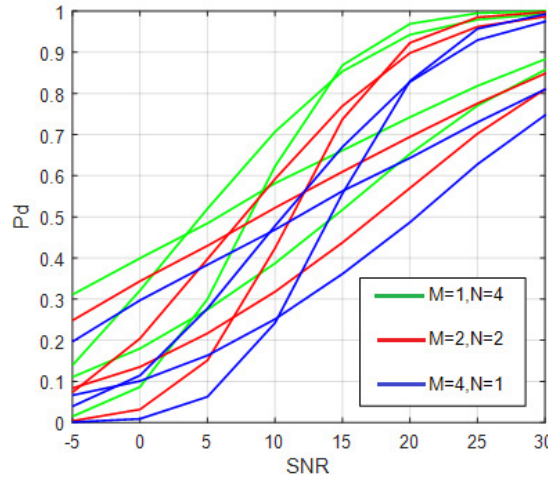


Figure. 4 CA-CFAR in MIMO radars with “MIN”, “MAX”, “algebraic product” and “algebraic sum” fuzzy fusion rules in homogenous background in cases ($M=1$, $N=4$), ($M=2$, $N=2$) and ($M=4$, $N=1$)

Next, we compare the performance of the for fusion rules for the case of $M=1$ and $N=4$. We observe that the “Algebraic product” fusion rule gives the best results for an SCR > 4 dB and the “MIN” fusion rule has comparable performance as the latter SCR > 15 dB.

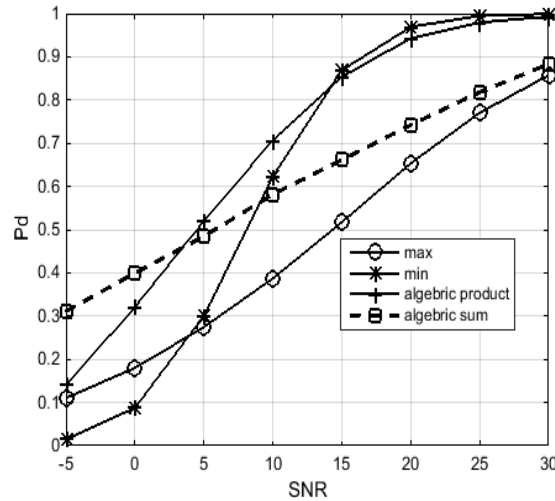


Figure. 5 CA-CFAR in MIMO radars with “MIN”, “MAX”, “algebraic sum” and “algebraic product” fusion rules in homogenous background

5. CONCLUSIONS

In this paper, we evaluated through Monte-Carlo simulations, the performance of a MIMO radar where each detector is constituted of a fuzzy CA-CFAR detector. At the fusion centre, the membership function to the false alarm space from all detectors are received and combined according to four fuzzy fusion rules. Different values of the number of transmitters and receivers were considered. The simulation results demonstrated clearly that the highest probability of detection is attained when the number of receivers increases. In addition, the best performance was provided by the “Algebraic product” fuzzy fusion rule and the “MIN” fusion rule for high SCR.

REFERENCES

- [1] J. Li and P. Stoica, *MIMO Radar Signal Processing*, Wiley, New Jersey, 2009.
- [2] E. Fishler, et al., “Spatial diversity in radars- models and detection performance,” *IEEE Transaction on Signal Processing*, vol. 54, no. 3, pp. 823-838, 2006.
- [3] C. Y. Chong, “Signal Processing for MIMO Radars: Detection under Gaussian and non-Gaussian environments and application to STAP,” Ph.D. thesis, Supelec, France, 2011.
- [4] H. Rohling, “Radar CFAR thresholding in clutter and multiple target situations,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 19, no. 4, pp. 608-621, 1983.
- [5] H. You, “Performance of some generalized modified order statistics CFAR detectors with automatic censoring technique in multiple target situations,” *IEE Proceedings, Radar, Sonar and Navigation*, vol. 141, no. 4, pp. 205-212, 1994.
- [6] A.R. Elias-Fuste, M.G. DE Mercado, and E.R. Davo, “Analysis of some modified order statistics CFAR: OSGO and OSSO CFAR,” *IEEE Transaction on Aerospace and Electronic Systems*, vol. 26, no. 1, pp. 197-202, 1990.

- [7] C. Y. Chong, F. Pascal, J.P. Ovarlez, and M. Lesturgie, "MIMO Radar Detection in Non-Gaussian and Heterogeneous Clutter," *IEEE Journal of Selected Topics in Signal Processing*, vol. 4, no. 1, pp. 115-126, 2010.
- [8] G. Cui, L. Kong, and X. Yang, "Multiple-input multiple-output radar detectors design in non-Gaussian clutter," *IET Radar, Sonar and Navigation*, vol. 4, no. 5, pp.724-732, 2010.
- [9] J. Liu, Z. J. Zhang, Y. Cao, and S. Yang, "A closed-form expression for false alarm rate of adaptive MIMO-GLRT detector with distributed MIMO radar," *Signal Processing*, vol. 93, pp.2771-2776, 2013.
- [10] N. Janatian, M. Modarres-Hashemi, and A. Sheikhi, "CFAR Detectors for MIMO Radars," *Circuits Systems and Signal Processing*, vol. 32, no. 3, pp. 1389-1418, 2013.
- [11] G.V. Weinberg, 'Assessing Pareto fit to high resolution high grazing angle sea clutter', *Electron. Lett.*, 2011, **47**, (8), pp. 516-517.
- [12] Z. Hammoudi, F. Soltani, Distributed CA-CFAR and OS-CFAR detection using fuzzy space and fuzzy fusion rules, *IEE Proceedings Part F Vol. 151 (3) (2004)* 135–142.
- [13] H. A. Meziani, F. Soltani, Decentralized Fuzzy CFAR Detector in Homogeneous Pearson Clutter Background, *Signal Processing Elsevier*, Vol. 91 (2011), 2530–2540.

AUTHORS

Faouzi Soltani was born in Constantine Algeria in October 1962. He received the Engineer degree from Algiers National Polytechnic in 1985, the MPhil (Eng) degree from Birmingham University (UK) in 1989 and the Doctorat d'état degree from Constantine University in 1999 all in Electronic Engineering. He joined the department of Electronic Engineering of Constantine University in 1989 as an assistant professor then as a full professor in 2004. He is the head of "Signals and Communication Systems" research laboratory. His main research interests include radar CFAR detection, estimation theory, neural networks and clutter modeling.



Faycal Khaldi received his Master degree from Medea University, Algeria in 2013. He joined Constantine university as a PhD student where he is working on MIMO radar signal processing in homogeneous and non homogeneous clutter.

AUTHOR INDEX

Abdessalam Chouaya 01

Amine Boulemtafes 13

Chafika Benzaid 13

Chayma Zatout 13

Dalila Hamidouche 13

Faouzi Soltani 95

Fatih V. Celebi 57

Fatma Baccar 71

Faycal Khaldi 95

Frank Piessens 85

Kais Mnif 71

Lamia Chaari Fourati 01

Lotfi Kammoun 71

Maroua Abdelhafidh 01

Mathy Vanhoef 85

Mohamed Abid 25

Mohamed Fourati 01

Mohammad Derawi 45

Mohammed Mazouzi 25

Muntaser A. Salman 57

Nadjib Badache 13

Roa Alharbi 37

Salim Lachdhaf 25

Suat Ozdemir 57