A STUDY OF IDENTIFYING ATTACKS ON INDUSTRY INTERNET OF THINGS USING MACHINE LEARNING

Chia-Mei Chen[1], Zheng-Xun Cai[1], Gu-Hsin Lai[2]

[1]Department of Information Management,
National Sun Yat-sen University, Taiwan
[2]Department of Technology Crime Investigation,
Taiwan Police College, Taiwan

ABSTRACT

The "Industry 4.0" revolution and Industry Internet of Things (IIoT) has dramatically transformed how manufacturing and industrial companies operate. Industrial control systems (ICS) process critical function, and the past ICS attacks have caused major damage and disasters in the communities. IIoT devices in an ICS environment communicate in heterogeneous protocols and the attack vectors might exhibit different misbehavior patterns. This study proposes a classification model to detect anomalies in ICS environments. The evaluation has been conducted by using ICS datasets from multiple sources and the results show that the proposed LSTM detection model performs effectively.

KEYWORDS

Industry Internet of Things, Machine Learning, Anomaly Detection.

1. INTRODUCTION

The emerging technologies of Industry Internet of Things (IIoTs) and 5G have started a new chapter for industries and businesses. The "Industry 4.0" revolution has dramatically transformed how manufacturing and other industrial companies operate. Industry 4.0 converges operations technology (OT) and information technology (IT) networks. While this union of these formerly disparate networks certainly facilitates data exchange and enables organizations to improve business efficiency, it also comes with a host of new security concerns [1].

Industrial Control System (ICS) is a major core system for manufacturing processes and critical infrastructure operations, which is a collection of all control systems, such as Supervisory Control and Data Acquisition (SCADA), Industrial Automation and Control System (IACS), Distributed Control System (DCS), Process Control System (PCS) [2]. It plays a significant role in industrial physical infrastructure to ensure each fundamental element to be under surveillance and co-work with others.

Industry control systems (ICS) and other OT devices used to be deployed in an internal network without security protection but are connected to IT networks nowadays. ICS design had not considered the security functionality, but now ICS, sensors, and other controllers become IP-enabled and IIoT endpoints on the converged OT/IT network, which expand the attack surface and increase security risk for enterprises.

David C. Wyld et al. (Eds): CCSIT, SIPP, PDCTA, AISC, NLPCL, BIGML, NCWMC - 2021
pp. 77-82, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.110707

IIoT devices and ICS systems have become a primary attack target based on their importance to business operation and national security. ICS attacks became prevailing in this decade, ranging from power plants, gas pipelines, water cleaning, energy and petrochemical companies, financial sectors. In 2010, Stuxnet was the first known threat targeting specific ICS systems, followed by Dugu, Flame, and Gauss targeting specific ICS manufacturers in 2011 [3]. The attacks are expected to increase in number and sophistication. Therefore, critical infrastructure owners and operators must develop the ability to detect and recover from cyberattacks [4]. Therefore, protecting ICS and IIoT networks is critical for enterprises and industries.

Traditional IDS mostly work on a signature basis, and there are not many known signatures to detect attacks on ICS networks [5]. IDS for IT networks might not work sufficiently in such an emerging OT/IT environment, because ICS components and IIoT devices behave differently from IT devices.

This study proposes a classification method to detect anomalies in heterogeneous network environments. In the first phase, it identifies the network protocol of the traffic and detects anomalies in the second phase by applying the LSTM model, where LSTM is an artificial neural network architecture with feedback connections that can process single data points as well as sequences of data, such as time series traffic flows.

The remainder of this paper is constructed as follows. Section 2 reviews the previous related research. Section 3 presents the proposed detection method, followed by the performance evaluation in Section 4. The last section draws the conclusion remark and the future directions of this study.

2. LITERATURE REVIEW

A study [6] highlighted common characteristics of IoT networks, in which a multitude of different devices with different capabilities and different communication protocols communicate with each other. It categorizes IoT attacks by different network layers: physical, link, network, transport, and application layers. Another study [7] defined a taxonomy model for attacks on most used industrial communication protocols: Modbus and DNP3.

Some research identified anomalies based on the recurring network patterns of IIoT networks. A study [5] analyzed the network traffic from a water distribution system in order to understand how ICSs work and evaluated the off-the-self IDS solutions. It concludes that network traffic from an ICS is static and the off-the-self IDS solutions produced high false positives. A study [8] developed an open-source PLC for validating PLC logic execution and comparing PLC behaviors when under an injection attack with crafted packets. Another study [9] designed an approach that exploits traffic periodicity to detect traffic anomalies by sliding windows but also pointed out that changes in the traffic periodicity are not necessarily malicious.

A study [10] developed an anomaly event detection model for a water system controlled by ICS and evaluated the following six ML algorithms: logistic regression, Gaussian naïve Bayes, k-nearest neighbors, support vector machine, decision tree, and random forest. The experimental results discovered that the more recorded attack scenarios used for training, the more robust the detection model.

Neural Network (NN) is one of the most popular ML algorithms, which have been employed on anomaly detection. Radford et al. [11] showed that RNN can represent sequences of communications on a network and discover anomalous network traffic. Prasse et al. [12] analyzed HTTPS network flows, employed a natural language model to extract features from domain

names, and proposed an LSTM-based detection method. Their experimental results show that the LSTM classification model outperforms a random forest model. Kim and Ho [13] employed CNN to extract spatial features and LSTM temporal characteristics and proposed a neural network for detecting anomalies on web traffic.

3. PROPOSED METHODOLOGY

According to the literature review on the major ICS attack events [4], most of the attacks have involved abnormal network behaviors. On the other hand, the literature review also has demonstrated MLtechniques yield effective classification and LSTM is suitable for time-series data. Therefore, this study analyzes the ICS traffic and employs an LSTM detection model to identify anomalous traffic.

The IIoT devices on the converged OT/IT network communicate in multiple communication protocols; therefore, attack scenarios might be different based on the applied protocol. Our preliminary study discovers that the machine-learning model performs better on identifying anomalies of a single protocol than on identifying anomalies of different protocols.

To improve detection effectiveness, this study proposes a detection method that applies the LSTM classification model to identify malicious traffic. The raw network traffic in packets is captured from the network, and the module Preprocess merges packets into flows, where a flow is a sequence of packets from a source to a destination. The detail of the proposed method is explained below.

3.1. Protocol Categorization

The past research applied ML models [14-16] to identify network protocols, which requires intensive computation and training time. Although IIoT devices may communicate in heterogeneous network protocols, it is reasonable to assume that the protocols applied within an IIoT network environment are known so that the security control of network monitoring can be operated. Given the knowledge of the protocol formats and the valid range of each field in the headers, the module Protocol Categorization identifies the protocol by examining the header.

3.2. Feature Encoding

Feature encoding is a process of transforming a categorical variable, such as protocol type, into a continuous variable. The payload (Data segment) is represented in hex, and its entropy is included in the feature set.

The selected feature set consists of relevant features from the applied communication protocol. For the protocols over TCP/IP, the following TCP/IP features are included: source IP, destination IP, port, packet size. For a specific ICS communication protocol, all its header fields, payload, and payload entropy are included in the feature set. Transaction ID, Protocol ID, the size of the payload, Unit ID, Function Code, and the payload and its entropy are extracted.

3.3. Detection Model

ICS processes perform periodic tasks; therefore, the communication contents among the IIoT devices are stable and periodical. The LSTM is suitable for learning time series and periodic patterns according to the literature review. The loss function adopted is binary cross-entropy as it is a binary classifier, where cross-entropy loss increases as the predicted probability diverges

from the actual label and penalizes misclassification greatly to build a good detection model. Most model learning optimizers are based on the stochastic gradient descent technique. RMSprop [17] uses an adaptive learning rate, instead of treating the learning rate as a hyper-parameter, and is suitable for learning a model from a big or redundant dataset. The training data of this study contains repeated traffic patterns that fit the above description. Therefore, this study adopts RMSprop for model optimization.

4. EVALUATION AND DISCUSSION

This research adopts accuracy, precision, recall, and F1 score as performance measurements. Accuracy is the proportion of correct predictions among the total number of the examined cases; precision as known as positive predictive value is defined as the fraction of the true instances among the predicted instances; recall as known as sensitivity is the fraction of the total number of the correctly identified instances divided by the total number that were predicted to be positive instances; F1 score that combines precision and recall is the harmonic mean of precision to compare the two models in this study.

This study evaluates the proposed solution with the datasets from multiple sources [18-20] and divides them into training and testing with the ratio of 8:2. The dataset source [18] contains multiple datasets collected from power systems, a gas pipeline and water storage tank, and gas pipelines. The dataset CSET [21] was collected from an electrical network monitor system that consists of two MTUs and three SCADA controllers. The 4SICS Geek Lounge [20] contains an ICS lab with PLCs, RTUs, servers, and industrial network equipment (routers, switches, firewalls, network cameras).

4.1. Experiment : Effectiveness of the Classification Method

This experiment evaluates the performance of the proposed detection method that categorizes the network protocol of the traffic data and then identifies anomalies. Table 1 presents the results of the LSTM detection model with and without protocol categorization. The classification model achieves better performance, as attack patterns might be different on different protocols.

Table 1. The detection results with and without protocol categorization.

	LSTM
Accuracy	86.58%
Precision	95.81%
Recall	64.84%
F1	0.773371722

5. CONCLUSION

This study proposes a ML-based classification model to identify anomalies on heterogeneous IIoT network environments and demonstrates that the impact of imbalanced training data and the resampling on the detection performance. The proposed a detection method first categorizes the protocol types of traffic flows and then identifies the anomalies of each protocol type. Such an approach reduces the training time as well as improves the detection efficiency on the heterogeneous network environments.

Most past research has focused on improving performance by evaluating different ML models. Besides that, this study demonstrates that upsampling improves the efficiency of model learning and the basic unit of data resampling may affect detection performance.

The multi-layered IT/OT converged network environments expand the attack surface; hence, defense-in-depth [22] is recommended by implementing layers of defense mechanisms. This study identifies the attacks of the two low levels on the ICS environments. While targeted attacks become very stealthy and customized, future work can extend the detection by cross-correlating security alerts from different layers of ICS environments.

REFERENCES

[1] R. Best. "Converged OT/IT Networks Introduce New Security Risks." https://www.infosecurity-magazine.com/opinions/ot-it-networks-risks/ (accessed: 20 Dec., 2020).

[2] O. KOUCHAM, "Détection d'intrusions pour les systèmes de contrôle industriels." [Online]. Available: https://tel.archives-ouvertes.fr/tel-02108208/document

[3] K. E. Hemsley and E. Fisher, "History of industrial control system cyber incidents," Idaho National Lab.(INL), Idaho Falls, ID (United States), 2018.

[4] K. Hemsley and R. Fisher, "A history of cyber incidents and threats involving industrial control systems," in International Conference on Critical Infrastructure Protection, 2018: Springer, pp. 215-242.

[5] J. Angséus and R. Ekbom, "Network-based intrusion detection systems for industrial control systems," Master Thesis, Department of Computer Science and Engineering, Chalmers University of Technology, 2017.

[6] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: current solutions and future challenges," IEEE Communications Surveys & Tutorials, 2020.

[7] Z. Drias, A. Serhrouchni, and O. Vogel, "Taxonomy of attacks on industrial control protocols," in 2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS), 2015: IEEE, pp. 1-6.

[8] T. Alves and T. Morris, "OpenPLC: An IEC 61,131–3 compliant open source industrial controller for cyber security research," Computers & Security, vol. 78, pp. 364-379, 2018.

[9] R. R. R. Barbosa, R. Sadre, and A. Pras, "Towards periodicity based anomaly detection in SCADA networks," in Proceedings of 2012 IEEE 17th International Conference on Emerging Technologies & Factory Automation (ETFA 2012), 2012: IEEE, pp. 1-4.

[10] H. Hindy, D. Brosset, E. Bayne, A. Seeam, and X. Bellekens, "Improving SIEM for critical SCADA water infrastructures using machine learning," in Computer Security: Springer, 2018, pp. 3-19.

[11] B. J. Radford, L. M. Apolonio, A. J. Trias, and J. A. Simpson, "Network traffic anomaly detection using recurrent neural networks," arXiv preprint arXiv:1803.10769, 2018.

[12] P. Prasse, L. Machlica, T. Pevný, J. Havelka, and T. Scheffer, "Malware detection by analysing network traffic with neural networks," in 2017 IEEE Security and Privacy Workshops (SPW), 2017: IEEE, pp. 205-210.

[13] T.-Y. Kim and S.-B. Cho, "Web traffic anomaly detection using C-LSTM neural networks," Expert Systems with Applications, pp. 66-76, 2018.

[14] C. Jeong, M. Ahn, H. Lee, and Y. Jung, "Automatic Classification of Transformed Protocols Using Deep Learning," in International Conference on Parallel and Distributed Computing: Applications and Technologies, 2018: Springer, pp. 153-158.

[15] J. Xue, Y. Chen, O. Li, and F. Li, "Classification and identification of unknown network protocols based on CNN and T-SNE," in Journal of Physics: Conference Series, 2020, vol. 1617, no. 1: IOP Publishing, p. 012071.

[16] R. Lin, O. Li, Q. Li, and Y. Liu, "Unknown network protocol classification method based on semi-supervised learning," in 2015 IEEE International Conference on Computer and Communications (ICCC), 2015: IEEE, pp. 300-308.

[17] G. Hinton, N. Srivastava, and K. Swersky, "Neural networks for machine learning lecture 6a overview of mini-batch gradient descent," vol. 14, no. 8.

[18] U. Adhikari, S. Pan, and T. Morris. "Industrial Control System (ICS) Cyber Attack Datasets." https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets (accessed: 18 Dec., 2020).

[19] A. Lemay. "A SCADA Dataset." https://github.com/antoine-lemay/Modbus_dataset (accessed: 18 Dec., 2020).
[20] 4SICS Geek Lounge. "Capture files from 4SICS Geek Lounge." https://www.netresec.com/?page=PCAP4SICS (accessed: 18 Dec., 2020).
[21] A. Lemay and J. M. Fernandez, "Providing SCADA network data sets for intrusion detection research," in 9th Workshop on Cyber Security Experimentation and Test, 2016.
[22] A. Fielder, T. Li, and C. Hankin, "Defense-in-depth vs. critical component defense for industrial control systems," in 4th International Symposium for ICS & SCADA Cyber Security Research 2016 4, 2016, pp. 1-10.