The Journal of Supercomputing (2022) 78:13554–13563
https://doi.org/10.1007/s11227-022-04408-4

Industrial network-based behavioral anomaly detection in AI-enabled smart manufacturing

HyunJin Kim[1] · **Taeshik Shon**[1,2]

Accepted: 24 February 2022 / Published online: 21 March 2022

Abstract

Existing manufacturing systems are isolated from the outside world to protect their sites and systems. However, following the trend of the 4th Industrial Revolution, manufacturing systems have also increased the connectivity of various domains and the convergence of numerous technologies. These systems are referred to as smart manufacturing systems. However, this trend has increased the challenge of network anomaly detection methods, which are a major approach to network security in smart manufacturing. Existing methods define normality under the premise that network components are static, and network operation is periodic compared to the information technology environment. Therefore, comprehensive and volatile network environments require significant time, cost, and labor to define normality. Consequently, artificial intelligence (AI)-based anomaly detection studies have been actively conducted to solve this problem. However, such studies require manual analysis based on expert knowledge of each site during the preprocessing stage to extract the learning features from the collected network data. To solve the above problems, this study proposes a protocol reverse engineering method corresponding to the preprocessing stage of exiting AI studies. Through this method, existing AI-based anomaly detection studies can directly use the collected network data to learn normality without expert knowledge of the site. Furthermore, non-polling or reporting network operating environments that are rarely studied in the manufacturing security domain are targeted. Finally, we propose an anomaly detection method that uses an external signature, time information, the pattern of time intervals, and classified messages. Thus, the proposed method can detect anomalies in the encrypted contents of the manufacturing protocols.

Keywords Smart manufacturing system · Network security · Anomaly detection

✉ Taeshik Shon
tsshon@ajou.ac.kr

[1] Department of Artificial Intelligence Convergence Network, Ajou University, Suwon, Korea

[2] Department of Cyber Security, Ajou University, Suwon, Korea

1 Introduction

Traditional manufacturing is an isolated environment in which systems are constructed using products from specific companies and communicated using their own protocols. However, following the trend of the 4th Industrial Revolution, the domains of various manufacturing systems are being converged, and new technologies are being integrated, such as the existing information and communication technology (ICT), the Internet of Things (IoT), the cloud, and artificial intelligence (AI). Moreover, the application of digitalization and automation is accelerating as COVID-19 has necessitated changes in the working environment of manufacturing systems. The foundation of this change is that various devices in the manufacturing system must be connected to the network and communicate with one another. Consequently, existing field devices that are connected via serial lines are also connected to the network using ICT or industrial IoT technologies. Specific company protocols to Ethernet-based open standard protocols for data exchange between various devices. At present, Ethernet-based industrial communication protocols include the EtherNet/IP, Modbus/TCP, EtherCAT, and PROFINET protocols.

Although the increase in the connectivity of manufacturing systems and the convergence of various technologies have provided operational advantages and management convenience, security difficulties have also increased. To address this problem, various security studies are being conducted in the manufacturing domain. However, such studies require experts with prior knowledge in the field of data collection as well as substantial time in the pre-analysis process. Furthermore, existing network-based security studies have targeted polling mechanism protocols such as Modbus/TCP. However, large manufacturing systems often use reporting mechanisms that periodically transmit the status and measurements from slave devices to master devices, except in specific situations such as connection initialization, management, alarms, and error handling.

Therefore, this study proposes a method for detecting anomalies in the reporting mechanism of manufacturing networks without the meanings and detailed packet fields in advance. We present an approach for detecting anomalies based on time information and periodic packet patterns. The remainder of this paper is organized as follows. Section 2 provides a brief overview of manufacturing-related anomaly detection studies. The proposed method is described in Sect. 3. Section 4 presents the experiments and results. We discuss future studies in Sect. 5.

2 Related works

Recent manufacturing security studies can be divided into security studies on the hardware itself and those on the communication between devices. The research area of the hardware itself includes hardware system security and digital forensics

[1–3]. However, many network security studies are being conducted because there is less impact on the communication network configuration and target operation in the application of data collection and proposal methods.

Several studies have targeted the polling mechanisms of manufacturing networks. Studies on manufacturing-network-based anomaly detection methods often involve network packets that are collected during normal operations. In general, the features of the normality definition can be classified into packet headers, packet payloads, and flow features. The packet header feature focuses on the meaning of the packet field. Header feature-based studies are similar to firewall rule-generation studies in the IT network environment. However, the detail signature field of the target manufacturing protocol has been analyzed and used for rule generation [4, 5]. Some studies have proposed signature or traffic pattern modeling based on the detailed meanings of the packet fields [6–8]. In recent years, active studies have applied deep learning for anomaly detection or increased efficiency [9–12]. Therefore, certain studies have applied these methods to manufacturing domains. Some studies have focused on protocol payloads that contain the actuator status and sensor measurement value [13–16]. A machine or deep learning algorithm was used for each status, and sensor values were employed for predicting the following normal values. Other studies have proposed anomaly methods based on protocol reverse engineering [17]. However, these studies focused on the polling mechanism, in which the master device must send a request message, following which the slave device respond to the requested message. Therefore, these methods are not suitable for reporting mechanisms. However, there is a lack of studies regarding the reporting mechanisms of manufacturing networks. Lin et al. [18, 19] proposed anomaly detection for non-polling mechanisms, which they named spontaneous traffic, based on the timing attributes of IEC-60870-5-104 protocols. They focused on the interval time and correlation of each message. However, this method requires knowledge of target protocol as well as the payload structure and meanings of the fields for each site to be analyzed in advance. This consumes a significant amount of time and labor. Furthermore, the compatibility and scalability are low because the detection models must be customized for each site and protocol.

3 Proposed methodology

The proposed methodology classifies the reporting protocol messages without prior knowledge of each site and protocol. This classification includes external signature classification and time interval classification. The cycle pattern modeling is based on the interval time sequence of each message, as illustrated in Fig. 1. Details of each stage are provided in this section.

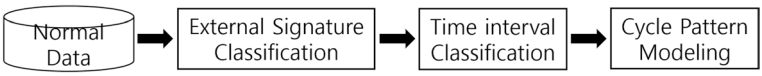

Fig. 1 Proposed message classification and modeling method for anomaly detection

3.1 A. External signature-based classification

In external signature-based classification, the packets are classified using standard header field information to achieve a high probability of the same message. As each field device in the manufacturing performs a predefined role in managing the process loop, the similarity and periodicity of the messages that are transmitted between the same devices are high. Two types of reporting operation protocols are available that deliver messages over L2 layers (e.g., MAC) and UDP protocols. Therefore, the MAC address of the L2 layer, which is the unique identification field of the device, and the IP address of the L3 layer, which is the device identification field of the network, were used. Moreover, the protocols and service types were identified using the EtherType field value of L2 and port number of L4. The packets were classified according to the message length because this was the minimum information required to identify the same message, as indicated in Fig. 2.

3.2 B. Interval time-based classification

Following the external signature-based classification, most existing studies have reclassified messages based on the internal signature of the messages on each 1:1 channel. The internal signature is the command/instruction code or connection/session identification that is contained in the header field of each industrial communication protocol. However, this approach requires pre-analysis for each protocol, and it is difficult to apply encrypted data. Therefore, in this study, message classification was performed using the packet interval time. If each unique reporting message is classified and grouped, the time interval is the same as the period of the reporting message. However, if various messages are mixed, a method is required to identify the period of each reporting message through the interval time of the packets. The differences between the two cases are shown in Fig. 3. In this study, it was assumed that each unique message has one period with slight jitter, and the period of each message was identified through fast Fourier transformation (FFT). In the field of signal processing, a Fourier series is used to decompose complex signals into periodic sub-signals. The traffic of each message can be mapped as a periodic pulse train. Therefore, this stage used FFT which is a mathematical algorithm of discrete

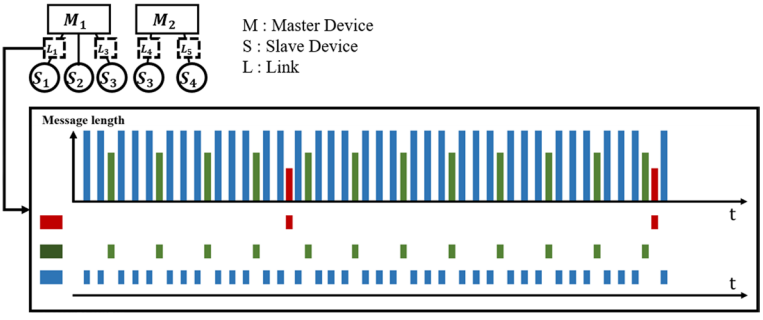

Fig. 2 Overview of external signature classification

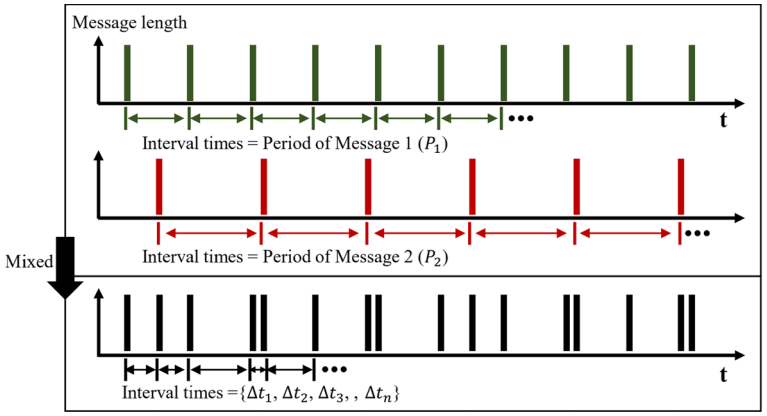

Fig. 3 Difference between interval time means of two cases

Fourier transforms for considering the computational speed. Several approaches have been proposed to detect anomalous traffic using FFT and autocorrelation function methods [20, 21].

First, we identified the smallest interval times in the mixed traffic and set the sampling rate according to the Nyquist rate, as follows:

$$\text{Sampling rate/second} \geq \frac{1}{\min\{\Delta t_1, \Delta t_2, \Delta t_3, \ldots, \Delta t_n\}} \times 2$$

Subsequently, the record time of each message was synchronized based on the sampling rate and frequency analysis was performed through FFT. The maximum time difference caused by the synchronization was half of the smallest interval time. The differences between the FFT results of the single-message traffic and mixed traffic with three messages are depicted in Fig. 4.

The FFT was performed with low-pass filter about the frequency based on the longest interval time because the shortest period time of the messages was larger than the largest interval time. The low-pass filter value is defined as follows:

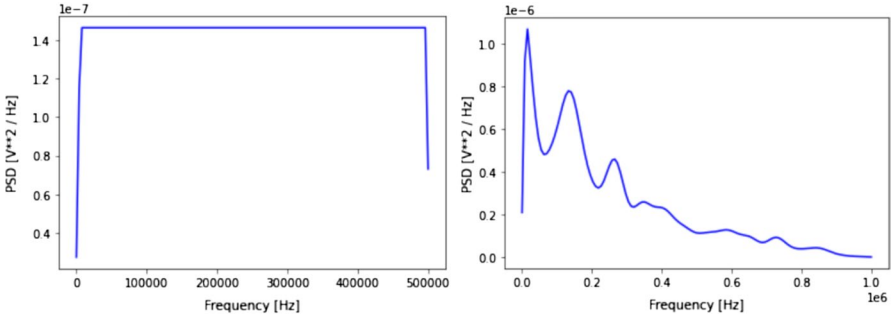

Fig. 4 Power spectral densities (PSD) based on FFT results

$$\text{Low pass filter} = \max\left\{\Delta t_1, \Delta t_2, \Delta t_3, \ldots, \Delta t_n\right\}$$

Finally, the messages were classified using a Gaussian mixture model (GMM) based on the frequency distribution of the FFT results. Each message was classified as a frequency distribution with the highest probability among the k frequency distributions through the GMM. The k value was selected using the Akaike information criterion and Bayesian information criterion scores of each GMM.

3.3 C. Cycle pattern modeling

In the previous classification stage, the messages were classified using the packet length and interval time on a 1:1 communication channel. The message cycle patterns between messages were identified and modeled in this stage. Messages exhibit a cycle pattern when they are generated by a process loop. As the internal content of the message is unknown, the pattern is checked through the sequence of messages and the probabilities of message transition. Thus, low-probability message transition was deleted from the entire graph, and the pattern was derived through a cycle detection algorithm (Fig. 5).

3.4 D. Proposed anomaly detection methodology

The proposed method for anomaly detection is an extension of an existing study [16]. The study proposed timing-based anomaly detection of the manufacturing target by using the sample mean and sample range for the interval time of each repeated message. The movement of central trends was detected through the sample mean values, and the changes in dispersion were determined through the sample range. This resulted in effective detection flooding, injection, and TCP sequence prediction attacks. However, we extended the existing method to detect anomalous traffic in environments where messages have cycle patterns of multiple interval times, as illustrated in Fig. 6.

First, the target message was checked for anomalies using the eight-tuples {destination/source MAC, EtherType, source/destination IP, source/destination port, message length} used in the external signature-based classification. This is very simple,

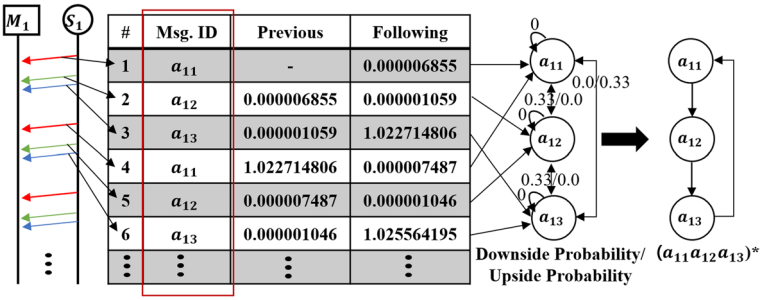

Fig. 5 Overview of cycle pattern modeling

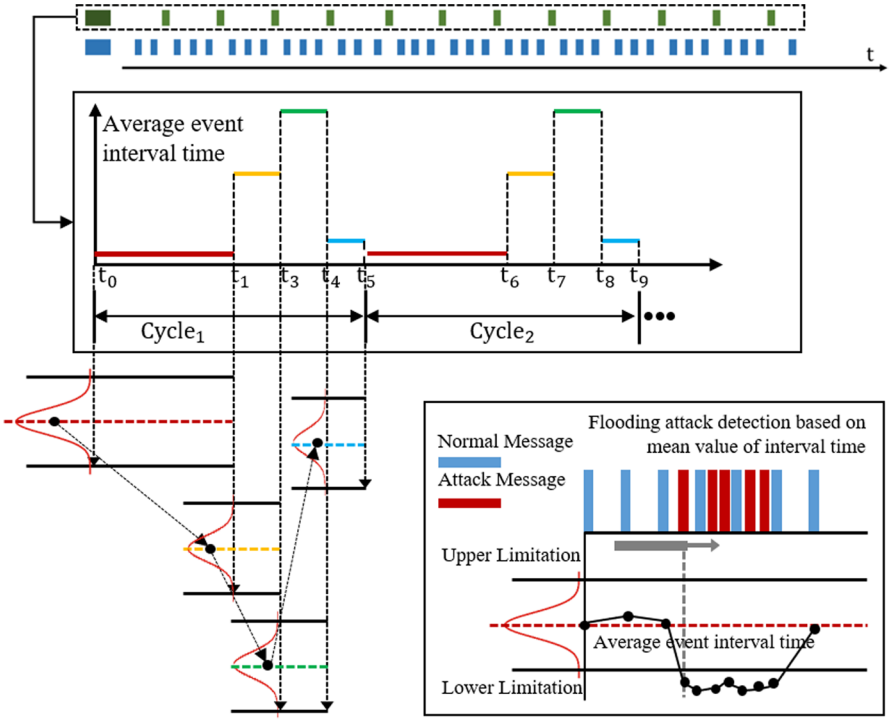

Fig. 6 Anomaly detection methodology for multiple interval times with cycle pattern

but very effective in manufacturing, where the network components, connections, services, and messages used are limited and static. Subsequently, we ensured that the message was appropriate for the periodic pattern order and had an appropriate interval time. The message was then checked with the order pattern and interval time pattern of the messages.

4 Experiment

The effectiveness and performance of the proposed anomaly detection method for message reporting were investigated using the P. Biswas public dataset [22]. This dataset is a substation network dataset consisting of 4 buses and 18 LEDs. Certain line feeders are connected to other loads, whereas others are connected to other substations. IEDs communicate with one another using the GOOSE protocol defined in IEC 61,850. The network architecture of the dataset is presented in Fig. 7. This dataset was used in the experiments because it uses a reporting message method, and it is similar to the manufacturing network environment.

The dataset provided network data (pcap files) during normal operation and denial of service (DoS) attacks. The GOOSE protocol messages were extracted from the dataset, and each dataset is summarized in Table 1.

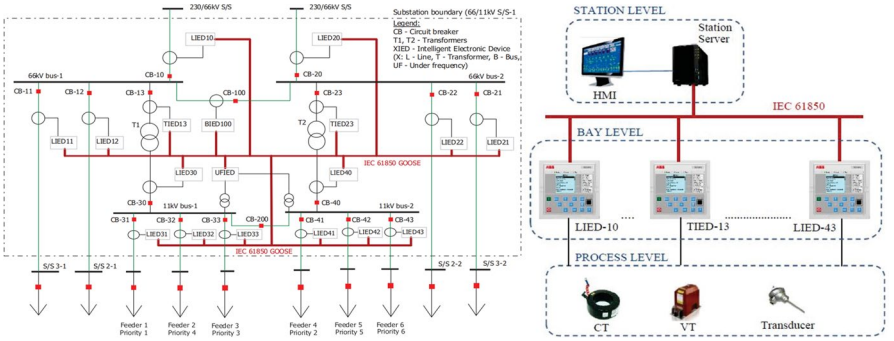

Fig. 7 Network architecture of dataset [22]

Table 1 Experimental datasets

Categorized	Total number of packets	Number of DoS packets
Normal	31,800	0
DoS	41,800	10,000

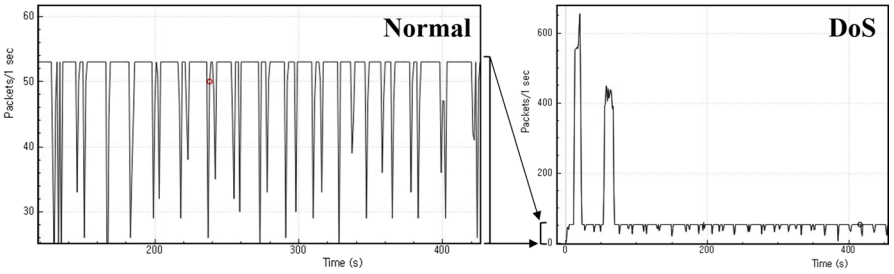

Fig. 8 Traffic comparison of two datasets

In the normal dataset, all traffic exhibited patterns. However, in the DoS datasets bust packets were observed for a short period. A traffic comparison between the two datasets is shown in Fig. 8.

The normal dataset was used to derive the eight-tuples, message, period times of each message, cycle patterns of the messages, and cycle patterns of the time interval. Subsequently, each message in the DoS dataset was sequentially investigated based on the rules and cycle pattern models that were derived from normal dataset. The detection performance of the proposed method is presented in Table 2. The proposed method detected all the DoS attack messages. It was found that the length and order of the DoS attack messages were not used in a normal operating environment. In contrast, some normal messages were detected as attacks. It was confirmed that the packet was the first packet or was transmitted after a DoS attack, resulting in an increase in the packet period. The F1-score of the proposed method was 0.99.

Table 2 Performance of proposed method

Symbol	Positive (normal)	Negative (attack)
Positive	31,791	9
Negative	0	10,000

5 Conclusions

In manufacturing, the polling method is used only for initial connection and management, whereas the reporting method is used for other tasks that require rapid real-time operations. Therefore, we have proposed a method for detecting anomalies without expert knowledge regarding message contents, protocol format, and field meanings. The proposed method can be applied directly to a manufacturing site because it manipulates the original network data instead of the separated field values that are extracted through preprocessing. Moreover, anomaly detection methods that use interval time patterns and time information have been designed to respond to attacks. The proposed method can reduce the analysis time and cost because it does not require expert knowledge of each site. Furthermore, the method has high compatibility because it corresponds to preprocessing stage of existing anomaly detection methods for manufacturing networks.

In the future, the proposed method can be extended to manufacturing environments with a combination of polling and reporting network operations, and it can be considered to demonstrate anomaly detection efficiency through various types of attacks.

Acknowledgements This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF), funded by the Ministry of Science, ICT & Future Planning (NRF-2018R1D1A1B07043349).

References

1. Jo W et al (2019) Digital forensic practices and methodologies for AI speaker ecosystems. Digit Investig 29(Supplement):S80–S93
2. Shin Yeonghun et al (2020) Certificate injection-based encrypted traffic forensics in AI speaker ecosystem. Forensic Sci Int Digt Investig 33(Supplement):301010
3. Lee S et al (2020) ExtSFR: scalable file recovery framework based on an Ext file system. Multimed Tools Appl 33:16093–16111
4. Yang Y et al (2013) Intrusion detection system for IEC 60870-5-104 based SCADA networks. In: 2013 IEEE Power & Energy Society General Meeting, pp 1–5
5. Wong K et al (2017) Enhancing Suricata intrusion detection system for cyber security in SCADA networks. In: 2017 IEEE 30th Canadian conference on Electrical and Computer Engineering (CCECE), pp 1–5
6. Goldenberg N et al (2013) Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. Int J Crit Infrastruct Prot 6(2):63–75
7. Yoon MK et al (2014) Communication pattern monitoring: improving the utility of anomaly detection for industrial control systems. In: NDSS workshop on security of emerging networking technologies
8. Kwon S et al (2020) IEEE 1815 1-based power system security with bidirectional RNN-based network anomalous attack detection for cyber-physical system. IEEE Access 8:77572–77586

9. Jiang Feng et al (2018) Deep learning based multi-channel intelligent attack detection for data security. IEEE Trans Sustain Comput 5(2):204–212
10. Rathore MM et al (2016) Hadoop based real-time intrusion detection for high-speed networks. In: 2016 IEEE Global Communications Conference (GLOBECOM), pp 1–6
11. Du H et al (2021) Network anomaly detection based on selective ensemble algorithm. J Supercomput 77:2875–2896
12. Choi H et al (2019) Unsupervised learning approach for network intrusion detection system using autoencoders. J Supercomput 75:5597–6562
13. Inoue J et al (2017) Anomaly detection for a water treatment system using unsupervised machine learning. In: 2017 IEEE international conference on Data Mining Workshops (ICDMW). IEEE
14. Goh J et al (2017) Anomaly detection in cyber physical systems using recurrent neural networks. In: 2017 IEEE 18th international symposium on high assurance systems engineering (HASE). IEEE
15. Kravchik M et al (2018) Detecting cyber attacks in industrial control systems using convolutional neural networks. In: Proceedings of the 2018 workshop on cyber-physical systems security and privacy
16. Kim SungJin et al (2020) APAD: autoencoder-based payload anomaly detection for industrial IoE. Appl Soft Comput 88:106017
17. Kim H et al (2021) Unknown payload anomaly detection based on format and field semantics inference in cyber-physical infrastructure systems. IEEE Access 9:75542–75552
18. Lin CY et al (2017) Timing-based anomaly detection in SCADA networks. In: International conference on Critical Information Infrastructures Security, vol 10707. Springer, pp 48–59
19. Lin CY et al (2019) Timing patterns and correlations in spontaneous {SCADA} traffic for anomaly detection. In: 22nd international symposium on research in attacks, intrusions and defenses (RAID 2019), pp 73–88
20. Glynn Earl F et al (2006) Detecting periodic patterns in unevenly spaced gene expression time series using Lomb-scargle periodograms. Bioinformatics 22(3):310–316
21. Liu W et al (2019) A novel network intrusion detection algorithm based on fast fourier transformation. In: 2019 1st international conference on Industrial Artificial Intelligence (IAI), pp 1–6
22. Biswas PP et al (2019) A synthesized dataset for cybersecurity study of IEC 61850 based substation. In: 2019 IEEE international conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pp 1–7