AI-based Network Security Enhancement for 5G Industrial Internet of Things Environments

Jonghoon Lee, Hyunjin Kim, Chulhee Park, Youngsoo Kim, Jong-Geun Park
Cyber Security Research Division
Electronics and Telecommunications Research Institute
Daejeon, Korea
{mine, be.successor, chpark0528, blitzkrieg, queue}@etri.re.kr

2022 13th International Conference on Information and Communication Technology Convergence (ICTC) | 978-1-6654-9939-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICTC55196.2022.9952490

***Abstract*—The recent 5G networks aim to provide higher speed, lower latency, and greater capacity; therefore, compared to the previous mobile networks, more advanced and intelligent network security is essential for 5G networks. To detect unknown and evolving 5G network intrusions, this paper presents an artificial intelligence (AI)-based network threat detection system to perform data labeling, data filtering, data preprocessing, and data learning for 5G network flow and security event data. The performance evaluations are first conducted on two well-known datasets—NSL-KDD and CICIDS 2017; then, the practical testing of proposed system is performed in 5G industrial IoT environments. To demonstrate detection against network threats in real 5G environments, this study utilizes the 5G model factory, which is downscaled to a real smart factory that comprises a number of 5G industrial IoT-based devices.**

Keywords—5G Network Security, 5G Edge Security, Intelligent Network Intrusion Detection, AI-based Intrusion Detection, 5G Model Factory

I. INTRODUCTION

Fifth generation (5G) networks provide advanced networking infrastructure to enable new applications in many areas. The 5G networks are not only an evolution of the previous 4G cellular networks but also a networking architecture with many new service capabilities [1]. Most 5G research are aimed at supporting various advanced characteristics, such as higher capacity and density of mobile broadband users than that of previous 4G networks, and massive device-to-device communications [2]. In particular, 5G private networks for business-to-business (B2B) applications are fundamentally based on the characteristics of 5G network-oriented massive devices, reliable low latency for communication, and enhanced mobile broadband using 5G new radio technologies [3,4].

Therefore, in 5G networking environments, intelligent network security against constantly evolving attacks on massive Internet of Things (IoT) devices, user equipment (UE), and various edge services has become increasingly important. The instantaneous recognition of network intrusions closer to suspicious network activities or behaviors is one of the most critical challenges in maintaining the security and reliability of 5G devices. Hence, artificial intelligence (AI)-based systems for detecting network intrusions and cyber threats have been further improved in the field of 5G security.

The remainder of this paper is organized as follows. Section II introduces the security issues related to the proposed 5G network security system, Section III describes the proposed system, and Section IV presents the testing and demonstration of real 5G environments. Finally, Section V presents the conclusions.

II. SECURITY ISSUES FOR THE PROPOSED 5G NETWORK

This section presents the security issues related to the proposed 5G network security system. In [2,3,4,5], various issues and challenges regarding 5G network security were presented. In [1,5,6], the security solutions are introduced that were based on the security services provided, such as authentication, availability, data confidentiality, key management, and privacy. In addition to various security challenges in previous studies, the issues related to this study are discussed further.

First, although a high false alert rate has been demonstrated, the use of an anomaly-based method for network intrusion detection can help recognize previously unknown cyberattacks [7]. In 5G network environments, the collection of numerous false alerts is extremely costly and a substantial amount of effort is required from security analysts to investigate such alerts.

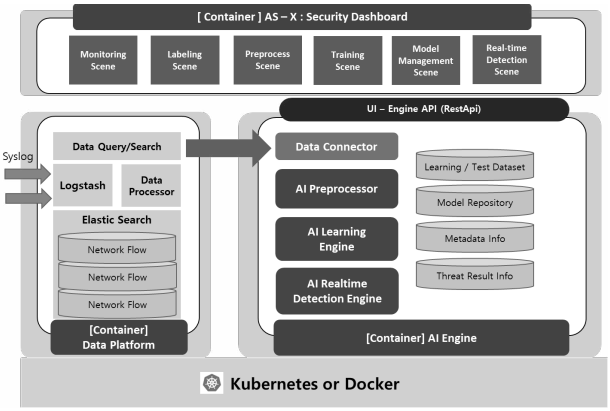

Fig. 1. Proposed AI-based 5G-NTD System

Second, network intrusions have evolved in more intelligent and varying ways. Some hackers can perfectly mask their malicious attacks by continuously evolving their suspicious behaviors and activity patterns. Although appropriate AI models can be used to detect these malicious activities, continuously changing attack patterns can make them undetectable. Moreover, almost all network intrusion detection solutions focus on analyzing short-term network security event logs and alerts. To defend against the continuously evolving malicious activities of hackers, security systems must analyze correlated security events associated with longer periods of time. Moreover, the most obvious way to detect malicious behavior and operations is to instantly apply a similar pattern based on a comparison with long-term data [8].

Third, in 5G networks, two-way authentication for the UE and base station, as well as service providers, can protect

against man-in-the-middle (MITM) attacks. Nevertheless, this cannot prevent a false base station from sniffing the traffic of the UE that connects directly to it [6]. However, a defect in the 5G standard described in [6] allows an attacker to reuse authentication keys from the previous session to create a false base station. This can create problems with surveillance devices, such as the ISMI catchers used in previous 4G networks. In particular, for security threat analysis, many studies are being conducted on various attack types, and vulnerability analysis is performed using rogue base stations and malicious UE that try to connect abnormally to 5G core networks. In [6], the authors presented that in addition to authentication issues, insufficient protection of DNS traffic from interception can create a host of issues. Changing the legitimate DNS requests to return malicious IP addresses will allow the attacker to perform MITM attacks, steal credentials, and deploy remote malware.

III. Intelligent Security for 5G Networks

This section presents the proposed system for AI-based threat detection, and briefly describes the performance evaluation of the proposed system.

A. 5G AI-based Network Threat Detection System

To address the above challenges, an AI-based network security enhancement model is proposed in this study. The model is based on a combination of correlation-based security event profiling and mutual correlation analysis of security events using a fully connected neural network (FCNN), convolutional neural network (CNN), and long short-term memory (LSTM), as shown in Figure 1. Thus, we develop and implement a 5G AI-based network threat detection system, called the 5G-NTD, in four phases.

First, to enable a required labeled dataset to employ a supervised learning method, data labeling is performed according to the correlated information included in the detected intrusion result report (e.g., threat start time, threat ending time, victim IP address, and attacker IP address information). Second, in the preprocessing stage, an event vector is converted from an event set, and the final event profile of the correlated events is transformed by event embedding from an event vector. Subsequently, the resulting collection that comprises pattern profiles is fed into the implemented deep learning engine, such as an FCNN, CNN, and LSTM, executed in the 5G-NTD system. Finally, the models generated by learning are stored in a model repository and can be operated after loading the model from the repository for real-time network intrusion detection.

B. Contributions of the 5G-NTD System

The 5G-NTD system employs various deep learning techniques with a data-preprocessing mechanism that enables the handling of large-scale 5G network data. Specifically, by executing multiple analysis engines, the main goal of the 5G-NTD system is to automatically analyze network security events and network flows related to true security alerts for detecting network intrusions. It also utilizes the processing capability of several graphical processing unit (GPU) cores for faster and parallel analysis.

For this, the system aims to apply an embedding procedure to convert a large number of collected IPS security events and raw network data into statistical pattern profiles of concurrent events and network flow, respectively. Next, the goal of the system is to classify raw events into normal or threat classes using correlation-based event profiling and machine learning models.

The system focuses on a generalizable security event analysis method by learning the network intrusion patterns and network flow based on the features of data within a particular time window. The 5G-NTD system includes an event pattern extraction method, called correlation-based security event profiling, by aggregating the simultaneously occurring frequency of events and correlating a set of events in the collected data.

TABLE I. Evaluation of the NSL-KDD Dataset

DL Method	NSL-KDD Dataset			
	TPR	FPR	Accuracy	F-measure
FCNN	0.941	0.029	0.958	0.952
CNN	0.926	0.028	0.952	0.945
LSTM	0.919	0.025	0.950	0.943

TABLE II. Evaluation of the CICIDS 2017 Dataset

DL Method	CICIDS 2017 Dataset			
	TPR	FPR	Accuracy	F-measure
FCNN	0.982	0.002	0.995	0.987
CNN	0.985	0.011	0.988	0.971
LSTM	0.978	0.011	0.986	0.967

C. System Performance

This study compares two well-known datasets (NSL-KDD and CICIDS 2017) that are commonly used in the field of network intrusion detection. The NSL-KDD [9] dataset comprises four available partitions: two files for training and two files for testing. Each file was composed of 42 features, including the label information. The CICIDS 2017 [10] dataset was collected over a period of five days, and the number of data instances was approximately 2.8 million with 85 network features containing label information. Although the first day log contains only normal captured activity, the other days contain the data points for various malicious attack activities, including a DoS, web attack, and port scan.

To evaluate the performance of the system, four prominent metrics are used: true-positive rate (TPR), false-positive rate (FPR), accuracy, and F-measure, which are commonly applied in machine learning methods. Moreover, considering only one metric as the criteria for the performance evaluation of the system is not sufficient. Evaluation results of each metric indicated that the 5G AI-based network threat detection system using three learning models achieved sufficient performance in data classification during the experiments.

The values for each metrics for the two datasets are as follows; in the case of NSL-KDD dataset, the accuracy of the proposed system increased from 0.95 to 0.96, the TPR increased from 0.91 to 0.95, and the FPR increased from 0.025

to 0.029, as shown in Table 1. Similarly, for the CICIDS 2017 dataset, the accuracy of the proposed system improved from 0.98 to 0.99, the TPR was also close to 0.97, and all F-measures were over 0.96. More detailed results are presented in [8].

IV. Test In Real 5G Environments

A. 5G Model Factory

For testing, we utilized a purpose-built testbed to demonstrate detection against network threats similar to real 5G industrial IoT environments, which comprises several programmable logic controller (PLC) devices, control robots, and control servers that are based on 5G networks.

The 5G model factory is a small testing factory that is downscaled to a real smart factory that comprises a number of industrial 5G IoT-based devices. Inside the model factory, there are several PLC devices, one mobile robot, and several sensors that use 5G UE for URLLC services. In addition, to control and manage them, the model factory has a robot control server, MEC platform, and SCADA server. In particular, to interconnect via radio resources and efficiently support data transmission, a 5G wireless network developed in [11] was provided and configured in the model factory between the UE and gNB.

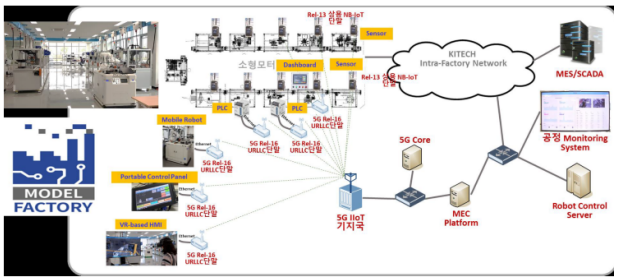

Fig. 2. Model factory for the small 5G testing environments

B. Test Environments

For real environments, when network attacks are detected, we collect the security events generated by the 5G IPS system and the network dump data by network mirroring between 5G UE and the 5G core network. For this, the network collector and one IPS system are deployed between the gNB and UEs, and the IPS system sends security events to the 5G-NTD system using the syslog protocol. For supervised learning and model creation by the 5G-NTD system, data labeling is performed by utilizing the time information when the attack began and ended.

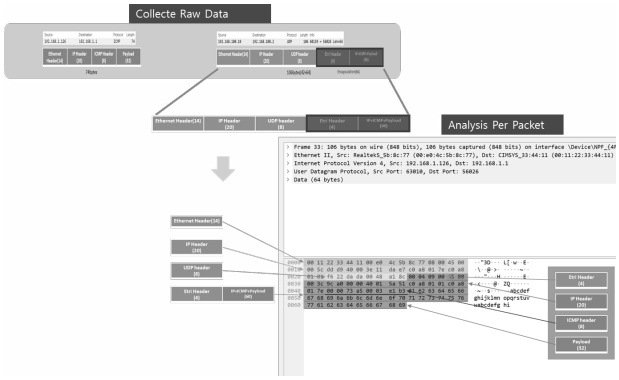

Fig. 3. Investigation network PCAP file for the proof of network attack

C. System Demonstration against attacks

In this study, we applied not only the network collector and one IPS system but also the 5G-NTD system to a model factory. The detection performance of the system when a fake attacker executes a network attack, such as a slowloris attack, was also measured. The slowloris attack is a type of denial-of-service attack that allows a single machine to take down another machine's web server with minimal bandwidth and side effects on unrelated services and ports [12]. Additionally, before proceeding to conduct a real attack, the collected data was synthetically investigated to extract the proof of the network attack. Looking at the network pcap data, as shown in Figure 3, it was determined that the response time increased, unlike in the normal state, as shown in Figure 4.

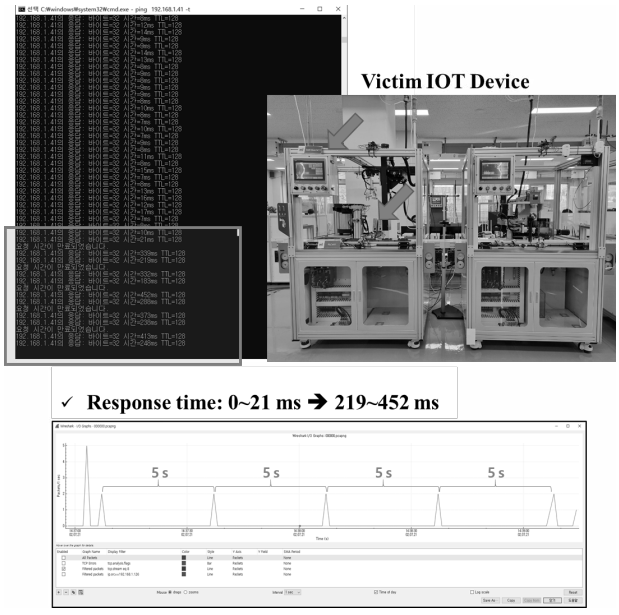

Fig. 4. Increasing ICMP Response Time during Network Attack

D. Results of Demonstration

Figure 5 shows the main configurations for the test and demonstration. The network collector is placed to collect the network traffic information, and the IPS system generates a security event based on the security policy. Furthermore, the 5G-NTD system detects and recognizes a network intrusion

through two types of data collection and accordingly requests the 5G core block for UE detachment

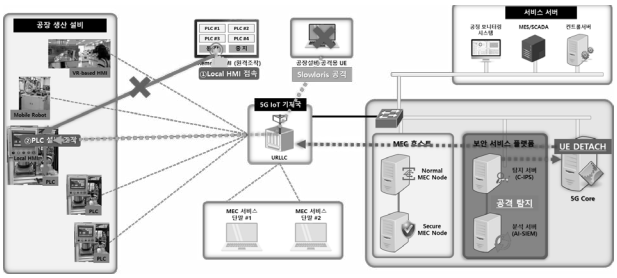

Fig. 5. Environments for Test and Demonstration

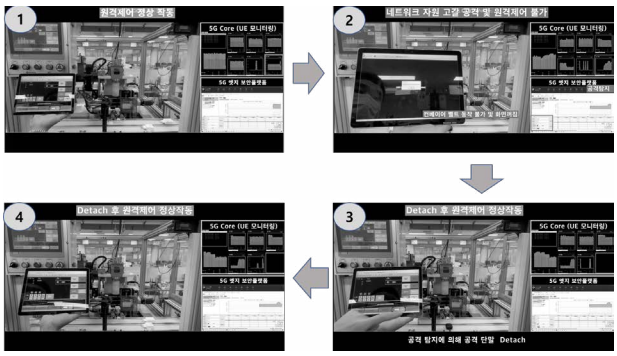

Fig. 6. Four Main Procedures during Testing

As shown in Figure 6, the test procedure was performed in four phases. First, in the stable and normal phases, we closely examined whether the PLC device was controlled and operated normally. Second, the simulated slowloris attack was performed using one attacker UE for approximately half hour, and the exhaustion of the network resource was checked by the UE monitoring system; it was observed that the PLC dashboard system was blocked and the PLC device was running slowly. Third, the 5G-NTD system instantly recognized the network intrusion through the activated AI models and requested the 5G Core network function for detachment of the malicious UE; the results indicated that the 5G core successfully performed the detachment procedure. In the final stage, it was demonstrated that the victim PLC device returned to a normally stable state.

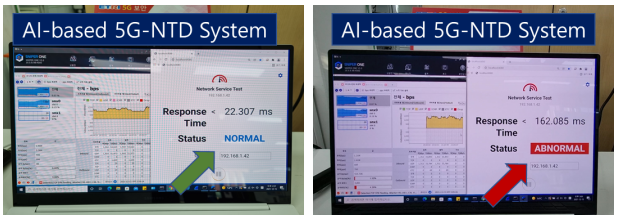

Fig. 7. The System Screen for Testing

Figure 7 shows the system screen used for testing. When the current state is normal, it is displayed as 'NORMAL'. However, once the 5G-NTD system recognizes a network intrusion, its status is marked as 'ABNORMAL'. A more detailed network flow status and detected security event can be displayed by the 5G-NTD dashboard as shown in Figure 8.

Fig. 8. Dashboard Screen-captures of the Monitoring System

V. Conclusions

One of the major challenges in detecting intelligent network intrusions is the provision for an AI-based detection technique; it is also an important challenge in 5G networks. Therefore, to detect 5G network intrusions and respond to malicious UE, we developed an AI-based network threat detection system in this study. We demonstrated the system performance in a 5G model factory, which was an existing smart factory that was downscaled to a model factory. Through a simulated network attack, we demonstrated the promising results of a real attack detection using the AI model. In the future, to address the evolving problem of cyberattacks in 5G networks, the network intrusion detection capability will be enhanced using unsupervised artificial intelligence models. Further, we will perform more number of varied network attacks in 5G model factories to improve system performance.

Acknowledgment

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2020-0-00952, Development of 5G Edge Security Technology for Ensuring 5G+ Service Stability and Availability).

References

[1] D. Fang, Y. Qian and R. Q. Hu, "Security for 5G Mobile Wireless Networks," in IEEE Access, vol. 6, pp. 4850-4874, 2018, doi: 10.1109/ACCESS.2017.2779146.

[2] J. Park et al, "3GPP 5G Security Architecture Features and Major Improvements," The Korea Institute of Information Security and Cryptology, Vol.29, No.5, pp.21-30, 2019.

[3] Y. Kim, J. G. Park and J. -H. Lee, "Security Threats in 5G Edge Computing Environments," 2020 International Conference on Information and Communication Technology Convergence (ICTC), 2020, pp. 905-907, doi: 10.1109/ICTC49870.2020.9289521.

[4] L. Fernández Maimó, Á. L. Perales Gómez, F. J. García Clemente, M. Gil Pérez and G. Martínez Pérez, "A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks," in IEEE Access, vol. 6, pp. 7700-7712, 2018, doi: 10.1109/ACCESS.2018.2803446.

[5] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila and A. Gurtov, "Overview of 5G Security Challenges and Solutions," in IEEE

Communications Standards Magazine, vol. 2, no. 1, pp. 36-43, MARCH 2018.

[6] Shane Fonyi. 2020. Overview of 5G security and vulnerabilities. Cyber Defense Rev. 5, 1 (2020).

[7] N.Hubballiand V.Suryanarayanan,‘‘False alarm minimization techniques in signature-based intrusion detection systems: A survey,’’ Comput. Commun., vol. 49, pp. 1-17, Aug. 2014.

[8] J. Lee, J. Kim, I. Kim and K. Han, "Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles," in IEEE Access, vol. 7, pp. 165607-165626.

[9] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu and Ali A. Ghorbani, "A detailed analysis of the kdd cup 99 data set," In Proc. of the Second IEEE Int. Conf. Comp. Int. for Sec. and Def. App., pp. 53-58, 2009.

[10] Kurniabudi, D. Stiawan, Darmawijoyo, M. Y. Bin Idris, A. M. Bamhdi and R. Budiarto, "CICIDS-2017 Dataset Feature Analysis With Information Gain for Anomaly Detection," in IEEE Access, vol. 8, pp. 132911-132921, 2020.

[11] Y. Hwang, S. Kang and J. Shin, "A study of Efficient Small Data Transmission in Industry IoT based 3GPP NB-IoT System," 2020 International Conference on Information and Communication Technology Convergence (ICTC), 2020, pp. 1848-1850.

[12] en.wikipedia.org “Slowloris (computer security),” [Online] Available: https://en.wikipedia.org/wiki/Slowloris_(computer_security)