Artificial Intelligence based Internet of Things Security

Mitra Pooyandeh Insoo Sohn

Division of Electronics & Electrical Engineering

Dongguk University

mitra.p@dongguk.edu isohn@dongguk.edu

Abstract

Artificial Intelligence (AI) and Internet of Things (IoT) is a soft smart revolution in industry 4.0. IoT is a world of sensors that connecting the physical objects such as computers, vehicles, appliances and other devices together and collect data over a wired or wireless network. On the other hand, these IoT systems are exposed to various types of cyber and physical attacks. As the modern threats continues to enlarge on, AI techniques, as intelligent methods which can learn and decide without the human intervention, have been widely used to enhance the IoT security in different ways. In this paper we survey the existing methods in which one of the AI methods has been used to defend against malicious attacks to IoT.

1. Introduction

The number of things connected to the Internet and using IoT technology is estimated at 14.2 billion as of 2019, and it reaches 25 billion by 2021 [1], and by 2025 more than 75 billion devices will be connected to the Internet [2]. Wireless Sensor Networks that monitor and control electric transmission tower, traffic lights, industrial machineries, and healthcare systems are kinds of IoT devices that attacks against them has bad influence on critical systems [3, 4]. Therefore, security is the greatest challenge for IoT. On the other hand, due to latency, transferring data to the cloud for processing is a time-consuming method. Hence, edge computing is an appropriate solution for transferring data processing to the edges. This causes to expose data to more attacks. One of the most recent approaches to enhance the IoT security is to utilize artificial intelligence (AI) methods. AI investigation continues to advance and it has gradually been applied to many fields of IoT security [2]. In this paper we review the most recent application of AI methods to increase the IoT security.

2. Materials

To know more about the probable security threats to IoT systems and existing AI methods to defend against different types of attacks, in this section, we explain briefly about the IoT systems, their security threats, and recent investigations about the application of AI for IoT security.

2.1. Internet of Things (IoT)

Internet of Things (IoT) now refers to billions of physical devices around the world that are connected to the internet, and which are collecting and sharing data with each other. Physical devices can refer to connected medical devices, a biochip transponder (think livestock), a solar panel, a connected automobile with sensors that alert the driver to a myriad of possible issues (fuel, tire pressure, needed maintenance, and more) or any object, outfitted with sensors, that has the ability to gather and transfer data over a network. Therefore, in the IoT the type of communication is machine-machine (M2M). IoT systems have three layers: *application layer* that provides service to users, *network layer* including GSM, WiFi, 3-5G, etc. ,and *perception layer* which consists of physical and MAC layer [5]. For successful implementation of Internet of Things (IoT), the important prerequisites including real time needs, availability of applications, data protection and user privacy, execution of the applications near to end users, and access to an open and interoperable cloud system.

2.2. IoT security threats

IoT systems exposed to different types of attacks including active and passive cyber attacks and physical attacks.
In the active attacks, malicious acts are carried out against data confidentiality as well as data integrity. They can also aim for unauthorized access and usage of the resources or the disturbance of an opponent's communications. There are variants of active attacks such as sybil, jamming, spoofing, Dos, data tampering, and malicious input attacks.
Passive attacks are performed in a way that it cannot be detected easily. This is due to the fact that the adversaries do not make any radio emissions. In passive attacks, attackers are typically hidden, and tries to collect data from communication lines. These types of attacks can be divided into different groups including eavesdropping, node malfunctioning, node tampering/destruction, and traffic analysis types [6]. Physical attacks refer to the attacks that physically damage IoT devices. The attackers do not need any network to attack the system. Therefore, this kind of attacks are subjected to physical IoT devices such as mobile, camera, sensors, routers, etc. by which the attackers interrupt the service.

2.3 AI used for IoT Security

As the modern threat landscape continues to enlarge on, adding artificial intelligence (AI) to a security strategy result in maintaining an effective security position. Considering the speed and complexity of modern cyber threats, network

security teams need the support of machine learning and other AI-based capabilities to detect, secure, and mitigate the attacks. Artificial Intelligence (AI) is classified to four major techniques: *machine learning* (ML), *fuzzy model*, *probabilistic models*, and *Metaheuristics* [7]. Recently, AI has enhanced the security of IoT in device authentication, DoS attack's defense, intrusion detection, and malware. AI techniques has unique solutions for these threats. The common processes of AI solutions are data collection, data pre-processing, model selection, data transformation, train and test, and model deployment [8]. Machine learning techniques provide the security for IoT by affecting the three layers of IoT with various methods such as Supervised, Unsupervised, and Reinforcement learning [9, 10].

In supervised learning the output is classified based on the input with a learning algorithm as in classification problems. In unsupervised learning there is not output for input data and the data is classified as what happens in clustering. In reinforcement learning the machine learns from interactions with human. Machine learning uses several techniques for IoT security such as classifying security attacks, Active learning for intrusion detection, security analytics learning-based malware detection system, learning-based authentication system, and hybrid intrusion detection system [11, 14].

Another AI method that is called Metaheuristic is a procedure which is designed to find a good solution to a difficult optimization problem. This algorithm is generally used for feature selection and tries to mimic biological, physical, and natural phenomena [12]. To increase the IoT security this method is used for intrusion detection and attack recovery.

There is also a fuzzy model technique that works based on fuzzy logic. Fuzzy logic is a method of reasoning which is similar to human reasoning. The approach of fuzzy logic includes all intermediate possibilities between digital values yes and no. This model is used for privacy and identify management, malware and attack detection by applying various methods such as clustering, classification, and ranking. The efficiency of security risk management depends on the speed and quality of clustering and classification of security threats [13].

Finally, the probabilistic model is a way to prove the existence of a structure with certain properties in combinations. The behavior of probabilistic systems modeled as discrete-time Markov chains (DTMCs), MDPs, or CTMCs. Indeed this model used for complex system attacks such as anomaly learning and detection, and security analytics.

3. Conclusion

In this paper we reviewed existing methods for enhancing the security of IoT devices and detection and mitigation techniques against attacks to IoT with AI techniques.

It turns out that various AI methods such as machine learning, fuzzy model, probabilistic model, and metaheuristics model have been used to make IoT secure against cyber and physical attacks. It has been deduced that AI-based methods have shown outstanding improvement in IoT security against cyber and physical attacks specifically in intrusion, anolamy, and malware detection. Certainly, in future due to artificial intelligence constant breakthroughs the IoT security will have a clear vision and it may soon offers the means to successfully secure the IoT.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRFK) funded by the Ministry of Education (2018R1D1A1B07041981).

References

[1] Seoyeon Kim, Jisu Park, Jaehyeok Jeong, Survay of IoT Platforms Supporting Artificial Intelligence, 2019.

[2] Massimo Merenda, Carlo Porcaro, Demetrio Iero, Edge Machine Learning for AI-Enabled IoT Devices: A Review, 2020.

[3] Kaviani, Sara, and Insoo Sohn. "Defense Against Neural Trojan Attacks: A survey." Neurocomputing (2020).

[4] Ioannis Stellios, Panayiotis Kotzanikolaou, Mihalis Psarakis, Cristina Alcaraz, Javier Lopez, A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services, 2018.

[5] Syeda Manjia Tahsien, Hadis Karimipour, Petros Spachos, Machine learning based solutions for security of Internet of Things (IoT): A survey, 2020.

[6] Martins O. Osifeko, Gerhard P. Hancke, and Adnan M. Abu-Mahfouz, Artificial Intelligence Techniques for Cognitive Sensing in Future IoT: State-of-the-Art, Potentials, and Challenges, 2020.

[7] He Fang, Xianbin Wang, Fast Authentication and Progressive Authorization in Large-Scale IoT: How to Leverage AI for Security Enhancement?, 2019.

[8] Hui Wu, Haiting Han, Xiao Wangof, Sengli Sun, Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey, 2020.

[9] Kotenko, I., Saenko, I., & Ageev, S. (2015, August). Countermeasure security risks management in the internet of things based on fuzzy logic inference. In *2015 IEEE Trustcom/BigDataSE/ISPA* (Vol. 1, pp. 654-659). IEEE.

[10] Abebe Abeshu Diro, Naveen Chilamkurti, Distributed attack detection scheme using deep learning approah for Internet of Things, 2018.

[11] Holzinger, Andreas. "Machine learning for health informatics." Machine Learning for Health Informatics. Springer, Cham, 2016. 1-24.

[12] Nahla Shatnawi, Qutaibah Althebyan, Wail Mardini, Detection of Insiders Misuse in Database Systems, 2011.

[13] Jiawei Su, Danilo Vasconcellos Vargas, Sanjiva Prasad, Lightweight Classification of IoT Malware based on Image Recognition, 2018.

[14] Kaviani, S., & Sohn, I., Influence of random topology in artificial neural networks: A survey. ICT Express, 6(2), 145-150 (2020).