Attack Detection and Mitigation in MEC-Enabled 5G Networks for AIoT

Shin-Ming Cheng, Bing-Kai Hong, and Cheng-Feng Hung

Abstract

In recent years, AIoT (Artificial Intelligence of Things) applications have received lots of attention since it exploits widely deployed IoT devices to collect data and perform an action while leveraging AI to obtain knowledge and insights. When deploying AIoT in 5G networks, Multi-access Edge Computing (MEC) is appropriate for enabling local management of IoT devices and computation of machine learning (ML) algorithms. Facing the multitude of threats in the ML data layer, IoT service layer, and 5G communications layer, MEC should enable corresponding detection and mitigation schemes to protect AIoT applications. In this article, we examine the existing security solutions located in each layer and discuss the interrelated challenges. For example, a network-traffic-based IDS solution in MEC might capture IoT malware but fail to identify a growing file-less attack. We suggest that firmware emulation in IoT endpoint should be included to provide system-level behaviors to network-based detectors in MEC so that file-less attacks can be distinguished. The potential of a backdoor attack aiming to poison data or corrupt ML models cannot be ignored in AIoT applications, and a corresponding detector should be implemented in MEC. Due to the rise of low-cost Software-Defined Radio (SDR), malicious attacks using rogue base stations (BSs) have become more popular. It implies that security protection at MEC in the communications layer is necessary. This article, therefore, proposes a novel platform, M3Inspector, where inspectors located in mobiles and AIoT machines collect information from surrounding BSs and provide them to MEC. MEC determines the rogue BS and makes a notification to users subscribing to the local service. A realistic 5G experimental platform with rogue BSs is developed. The results demonstrate that attack detection and mitigation can be implemented in the MEC paradigm to significantly improve the security protection of AIoT from the perspectives of rogue BS attacks and file-less attacks.

Introduction

With communications, computation, and storage capabilities, IoT devices in cyberspace could deeply interact with humans in the physical world. With the aid of AI (Artificial Intelligence), AIoT (Artificial Intelligence of Things) could deeply reason user behavior and provide what they need via various kinds of AI-empowered applications. The features of high transmission rate, low latency, and ubiquitous connectivity make 5G a promising communication bearer to support applications of AIoT. For example, an intelligent factory scenario in Non-Public Network (NPN) where AIoT devices with 5G connectivity are deployed in a factory to facilitate the high-precision operations of manufacturing. Moreover, AIoT integrated into a vehicle enables autonomous driving with the assistance of low latency and reliable 5G communications.

The combination of core technologies of 5G, AI, and IoT, on the one hand, opens the door to innovation but, on the other hand, amplifies the security threats originating from individual components. Moreover, due to short release timelines, the design flaw and vulnerability in AIoT applications or systems intensify negative effects via ubiquitous connected 5G AIoT devices. Adversaries or cybercriminals exploit a well-known or zero-day vulnerability in cyberspace to gain benefits in the physical world from the perspective of revenue or sensitive information. In this case, the safety and privacy of users who enjoy the AIoT applications might be significantly affected, and the security issue of AIoT in 5G has been an ever-increasing concern for academic researchers, industrial practitioners, and specification groups [1].

The challenges of providing security to AIoT in 5G networks are originated from following layers

- **IoT in the service layer.** The cruel competition of IoT products forces vendors to neglect security considerations to shorten release time, resulting in common weaknesses such as hard-coded passwords, unsafe random number processing, dangerous process execution, or dangerous memory operations [2]. The heterogeneous designs of firmware, protocols, controllers, peripherals, and chips in IoT devices hinder the development of general cybersecurity solutions. IoT endpoint devices' constrained resources and inaccessibility make traditional security protections for desktops inapplicable.
- **AI in the data and model layer.** By investigating the massive raw data captured from IoT devices using well-trained models, machine learning (ML) helps understand critical information and knowledge to facilitate AIoT application. Different kinds of ML schemes are built. For example, *federated learning* is designed for massively distributed training of ML models among AIoT devices without accessing their local training datasets so that privacy is preserved [3]. Moreover, *transfer learning* provides AIoT application developers without sufficient resources and effective ML models by transferring the learned knowledge of pre-trained models via fine-tuning. Since the accuracy of ML applications is data and model-dependent, adversaries could corrupt the learning model by launching data or model poisoning attacks to make the model ineffective. In particular, a backdoor is injected into the trained models in the above two scenarios to mislead the poisoned model

Shin-Ming Cheng is with National Taiwan University of Science and Technology, Taiwan and also with the Research Center for Information Technology Innovation, Academia Sinica, Taiwan.

Bing-Kai Hong and Cheng-Feng Hung are with National Taiwan University of Science and Technology, Taiwan.

This work was supported in part by the National Science and Technology Council (NSTC), Taiwan, under Grant 108-2628-E-011-007-MY3 and 111-2221-E-011-067-MY3.

Digital Object Identifier: 10.1109/IOTM.001.2100144

2576-3180/22/$25.00 © 2022 IEEE

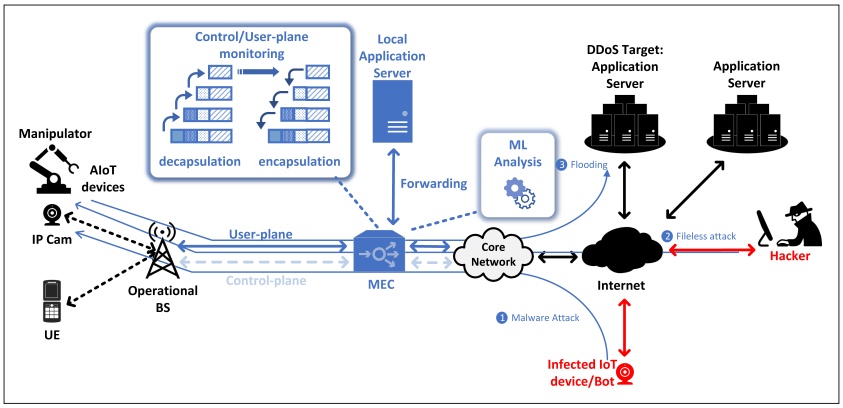

FIGURE 1. MEC-enabled network architecture for AIoT applications and IoT malware & file-less attacks.

to misclassify an input with a particular trigger.

- **5G in the communication layer.** The sophisticated Authentication and Key Agreement (AKA) procedures evolved from each generation of the cellular network provide mutual authentication as well as confidentiality and integrity protection between User Equipment (UE) and Core Network (CN). The public key protection for signaling messages exchanged before AKA make spoofing or relaying of message much more difficult. The appearance of cheap Software-Defined Radio (SDR) and 5G opensource enables the attack from rogue/fake Base Station (BS), where experimental 5G BS behaving same as the operational one misleads victim UE to achieve sensitive information stealing or service disabling [4].

In order to detect rogue BS attacks, vulnerable AIoT devices, or poisoned ML models, additional security functionality shall be included in 5G architecture, and the edge component, Multi-access Edge Computing, might be an appropriate position. MEC is designed initially to offload the task to the local edge servers for computation to improve latency requirements and reduce communication costs. Analytic techniques using AI and ML algorithms at MEC allow AIoT devices to obtain faster insights and feedback so that their operation is enhanced [5]. As a result, MEC can efficiently support computational intensive and resource-demanding AIoT applications. Researchers believe that the proximity to the users can compensate for the traditional end-to-end security mechanism. The hierarchical CN/MEC security architecture is regarded as one that strikes the right balance between effectiveness and efficiency [2, 5–8].

This article comprehensively investigates how MEC enables innovative attack detection and mitigation for AIoT devices. We will cover possible threats from the communications, service, and data layers to examine if the security mechanisms in MEC could capture the threat in time and alleviate the damage. To begin with, the attacks to logic flaws or software vulnerabilities of AIoT service are examined using a network-traffic detector located in MEC. Facing the stealthy file-less attacks, MEC might leverage the system-level monitoring information to decide with higher accuracy. It can be achieved by exploiting the recent innovation and firmware emulation in IoT endpoint. Also, a detector capturing a poisoned model for AIoT service is built on MEC so that backdoor attacks in the data layer can be identified. Finally, we propose a novel MEC service, named M3Inspector, to enable inspection of BS behavior at "M"obile UE and AIoT "M"achines. The sensed information is collected in "M"EC for the analysis to determine the rogue one. The result is notified to the users who subscribed to the service. The proposed detectors demonstrate that attack detection and mitigation can be implemented in the MEC paradigm to improve the security protection of AIoT significantly. Moreover, multiple layers of security controls to mitigate targeted attacks are recommended in MEC to provide complete protection for AIoT devices. The challenges of existing MEC detectors in service and data layers are also discussed, and possible solutions are suggested.

The rest of this article is organized as follows. we present MEC architecture for AIoT and also provides a review of existing security threats in AIoT from communications, service, and data layers. We address necessary security functionalities that should be included in MEC to detect and mitigate the mentioned threats. The challenges of the existing security schemes are also discussed. We propose a MEC service, M3inspector, to identify rogue BS and to notify subscribers with the aid of sensors in mobile and machines. An experiment is conducted in the MEC-enabled platform to examine the security functionality of the M3Inspector. Based on our empirical findings, we conclude this article and provides some implications.

MEC-Enabled Network Architecture

Figure 1 shows the MEC network architecture for AIoT. In addition to monitoring all traffic between RAN and CN, it is also closer to AIoT to help it analyze, predict, and respond in real-time. With the functionality of 5G communication and ML computation in IoT systems, AIoT could face multi-dimensional threats and attacks. The following subsections summarize the major ones launched at each layer.

Vulnerability Attacks in AIoT Service Layers

Since the Internet of Things system is not designed primarily for security but to maximize profits in cost, performance, power, and other aspects, many security threats are often caused by design defects, misconfiguration, and implementation bugs. However, the constrained computation resource makes the existing well-developed security tools impossible in IoT to resist security threats. The above unique properties open opportunities for adversaries to access AIoT devices through the following manners.

- **Malware infection.** Recently, IoT botnets and malware received lots of attention due to Mirai's significant damage to global websites. The source-code release of Mirai has given rise to several variants and sped up botnet creation. By leveraging similar tactics, these attacks targeting IoT endpoint devices search for unprotected ones, compromise them, turn them into bots, and harness the collective power to launch DDoS attacks. As shown in Fig. 1 (1), The infection is typically achieved by brute force password guessing. The malicious binary delivered to the victim will be executed so that the following infection and replication are also accomplished.
- **File-less attack.** Instead of downloading and executing malware files, hackers exploit existing or unknown vulnerabilities on the victim devices to achieve file-less attacks [9]. As shown in Fig. 1 (2), Without transporting the malicious binary and possessing it inside the hard drive, file-less attacks are harder to fingerprint and, thus, are highly suitable to conduct attacks such as privilege escalation, data theft, information exposure, or network compromise.

Nevertheless, many AIoT devices will be connected to the cellular network in the smart venue. MEC devices with a Malware detection mechanism can be deployed to protect the underlying infrastructure.

Backdoor Attacks in Data and Model Layers

In the AIoT paradigm, AIoT devices provide a large amount of sensing data for further recognition and understanding in AIoT applications. The accuracy of these applications highly depends on the collected data and ML models. In this case, malicious users could leverage this key dependency to influence the AIoT applications by manipulating models or poisoning data, especially with backdoor attacks.

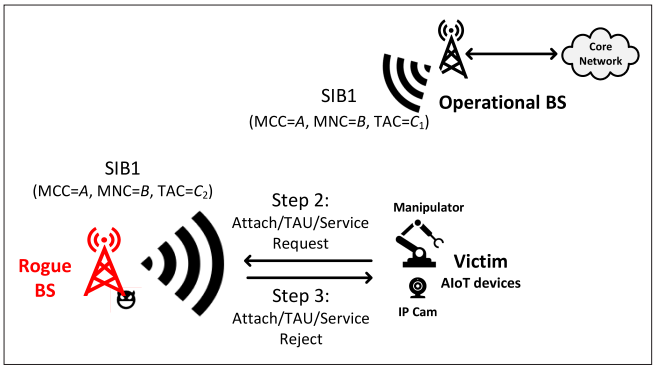

FIGURE 2. Procedure of rogue BS attacks.

Training Data Corruption. The adversary could directly modify the raw data collected for training to enforce the ML model to make a wrong prediction, classification, or inference. In particular, part of the training data is injected through backdoor triggers, and the labels of these poisoned samples are modified to the target category. The high correlation between the backdoor triggers and targets is enhanced during the training process, making the model misjudge the input samples with backdoor triggers.

Model Manipulation. In the popular federated learning and transfer learning scenarios, respectively, designed to preserve privacy and reduce computation cost, the ML model is accessible and then adjustable. In this case, the neurons in the neural network can be modified the original inference logic is manipulated. When a victim model transfers the learned knowledge of a pre-trained, the poisoned model, the backdoor inside the poisoned model, is also transferred.

The AIoT devices will send the parameters of their respective mods back to the central server through federated learning to generate better mods and then update them to each device. The advantage of MEC deployment location is that it can protect the transmission between devices.

Rogue BS Attacks in Communications Layer

As we mentioned earlier, the appearance of cheap Software-Defined Radio (SDR) makes rogue BS attacks back to their feet. Researchers could easily establish experimental 5G BSs using open-sourced 5G software (e.g., srsLTE and OAI). The rationale behind AKA implies that AIoT will trust the unprotected broadcast signals before AKA if the format of signals is correct, which are exploited by adversaries to launch rogue BS attacks. Rogue BS broadcasts the same messages as the operational cell and may use the same identity to make itself indistinguishable from the legitimate ones. Adversary could attract AIoT to connect itself by transmitting a more robust signal than those of the legitimate operational BSs. Following the instructions from the rogue BS, the victim AIoT devices might perform harmful actions, belief crafted information, or reveal their private information [4]

Figure 2 presents the steps of infamous DoS Attack via `Attach/TAU/Service Reject` message [4]. The details are described as follows.

- Step 1. The attacker (i.e., the rogue BS) attracts victim AIoTs to camp on itself by transmitting a stronger signal than legitimate operational BSs.
- Step 2. AIoT device connected to the rogue BS is unaware of the existence of rogue BS and makes normal operations. For example, they send the `Attach/TAU/Service Request` message to the connected BS depending on the current situation.
- Step 3. When receiving `Attach/TAU/Service Request` message from the victim AIoT device, the rogue BS injects "EPS Service Not Allowed" containing EMM cause #7 into the `Attach/TAU/Service Reject` message so that the victim AIoT device thinks that the requested service is invalid. Then the victim AIoT device will not actively connect to other legitimate BSs nearby until its 5G communication operation is restarted, thereby realizing a DoS attack.

Such a DoS attack damages AIoT applications, especially in intelligent factory scenarios. The availability is the first security requirement for industrial IoT devices since even the temporary shut down of operation will result in significant financial losses. The malicious competitor could easily launch a rogue BS attack to interrupt the regular operation without being spotted. As a result, a good approach to identifying a rogue BS attack and mitigating its impact is critical.

Due to the location advantage of MEC deployment, all the traffic transmitted between CN and RAN can be seen. Therefore, a series of malicious attack detection mechanisms can be designed on MEC, such as the detection mechanism of Rouge BS attack or even malicious traffic attack mechanism.

MEC Security Architecture

As the middle layer between the CN layer and the AIoT device layer, MEC enables data processing, analysis, and storage. Facing the various kinds of stealthy attacks from various layers mentioned in the previous section, the additional security functionalities should be developed in MEC to assess AIoT devices and their vulnerabilities, as well as to infer and characterize IoT-centric malicious activities, which is known as *detection*. Once exploitation attempts are identified, *mitigate* can be achieved to protect AIoT devices against multiple attacks. We summarized the necessary functionalities in each layer.

- **Service layer.** The security function in MEC will monitor the data plane payload decapsulated from the lower layer (i.e., 5G communication layer). For example, the ML model is utilized to understand the network behavior by monitoring the data plane traffic so that malware download, flooding attacks, or file-less attacks can be identified [6, 7]. In this case, MEC acts as an Intrusion Detection Systems (IDSs), monitoring the network and detecting malicious activities so that vulnerable AIoT devices are protected. For example, malware typically delivers malware using busybox or pipeline, MEC could checks specific commands in payloads of Telnet and SSH, such as `curl`, `wget`, `tftp` or `echo`, and investigates the downloaded binary following those commands [2, 9].

  By further leveraging the decapsulated control plane payload, MEC could determine the malicious attempts from users in RAN and take reaction in time [8]. In this case, MEC-level access control is achieved, where abuse of resources in MEC from unauthorized traffic is prevented.
- **Data and model layer.** In order to find out the manipulated data or model transferred from the malicious AIoT devices, MEC should be capable of understanding the training data and model [5, 7]. For example, MEC could analyze the inner neuron behaviors to determine the suspicious model. In particular, we supply appropriate stimulus to the model and check if neurons in the model substantially elevate the activation of a particular target label. The determination of compromised models in MEC could mitigate the negative impacts caused by the poisoned models.
- **Communication layer.** The 5G protocol monitoring function is an essential must for MEC so that fundamental traffic redirection or forwarding can be achieved. As shown in Fig. 3, MEC can decapsulate the data plane traffic from AIoT to get the payload in the IoT service layer. Depending on the intention of the packet sender, the payload will be forwarded to the local application server or encapsulated using 5G protocols for further delivery to CN. Sometimes, control plane packets also need to be decapsulated to offer payload to the upper layer to achieve complicated detection or mitigation [8].

Challenges

As shown in Fig. 3, to enable complete protection for AIoT

devices, MEC should be capable of detecting and mitigating attacks in all layers. The mechanism for detecting IoT Flow-based attacks is deployed on the gateway [10], which aggregates traffic from all devices and determines before an attack through ML. Due to the advantage of the MEC deployment location, all traffic from Control planes and User planes will pass through, so [8, 11] proposed to deploy a mechanism to detect malicious traffic is deployed on the MEC. This DDoS attack is triggered after the attack is detected and cannot be blocked earlier. We classified these and sorted them out in Table 1. Although many existing MEC-enabled solutions are proposed at the service and data layer, no communication-layer solution is designed in MEC to detect rogue BS attacks. Moreover, detecting poisoned data and ML models is far from mature and remains an open problem [5]. The high false alarm in malicious ML model detection will disturb the users, and the acceptance of the detector might not be explored.

The most critical problem for existing detectors in the service layer is that the sensed network packets might not completely reflect the attack behavior to vulnerable AIoT devices even with the aid of ML model [2, 9]. In particular, the malicious payloads generated by the sneaky malware or compromised devices are mixed with the regular traffic and are complex to determine precisely. The popularity of fileless attack without carrying recognizable payload make network-traffic-based IDS at the MEC much more challenging. If system-level monitors are involved, we can capture not only network traffic but also commands or system calls executed so that attack can be identified precisely [9].

By virtually re-hosting firmware into emulated IoT systems, the executions of service and application are decoupled from the IoT hardware. As a result, the vulnerability of IoT devices can be detected and analyzed based on virtualized machines. By integrating an advanced monitoring module in the virtualized system, system-level behavior can be captured so that attacks and malware can be identified more accurate fashion [2].

M3Inspector: Detection of Attacks

In order to alleviate the damage caused by rogue BS attacks, some protection or detection mechanisms are necessary and thus received lots of attention in recent literature [12–14]. Typically, the existing solutions deploy sensors to collect information sent from a targeted BS for distinction. In particular, sensors estimate the physical position of a targeted BS and check if its located in the appropriate position by comparing the location of legal operational BSs (e.g., FBS-Radar [12] and Crocodile Hunter [13]). Another example is that PHOENIX [14] investigate the sequence of Non-Access Stratum (NAS) message received at the sensors to determine the behavior of a targeted BS in an efficient approach.

In the 5G network, MEC is a perfect position to enable the detection and reaction of rogue BS since it could perform the corresponding actions in time. We propose a novel `M3Inspector`, where sensors in "M"obile UE and AIoT "M"achine cooperate with "M"EC to determine a rogue BS attack. In particular, we leverage information at different layers collected from sensors to provide high-accuracy detection results. We found that in addition to a much stronger power sent by the rogue BS for the victim attraction or a crafted NAS message sequence [14], RF properties due to limited physical capabilities in the low-cost hardware can be applied as feasible indicators of rogue BS. In particular, in the proposed detector, we investigate the behavior of signal power measured in particular RRC and NAS messages to identify if the transmitter is equipped with unstable RF hardware.

Network Architecture

As shown in Fig. 4, M3Inspector consists of the following components:

- An entire legitimate cellular network consists of AIoT devices, operational BS, MEC, and CN. We use two mainframes with the same Intel Core i5 6500 CPU, 4-core, and 24GB RAM, plus two SDR combined with four antennas to simulate an operational BS that can transmit or receive signals. USRP-B210 and srsRAN are respectively selected as SDR and 5G opensource. Moreover, MEC with redirection and en/decapsulation capabilities are implemented to connect operational BS and CN.
- An isolated rogue BS launching malicious attacks. It is implemented using SDR and srsRAN and is for the trustful evaluation of the detection effectiveness. We choose a representative DoS attack using a malicious `Attach/TAU/Authentication Reject` message sent from a rogue BS to disable victim AIoT devices practically. Please note that existing detection solutions like FBS-Radar [12] and Crocodile Hunter [13] did not implement rogue BS for the detection. They mainly investigated the identification of anomalies or misconfiguration.
- Sensors in machine and mobile for data collection. For the sensors in AIoT machine and mobile UE, we leverage respectively srsUE with USRP-B210 and Mobileinsight [15]. The information collected by the sensors will be delivered to MEC for rogue BS determination.
- The machine can be used for data collection and firmware

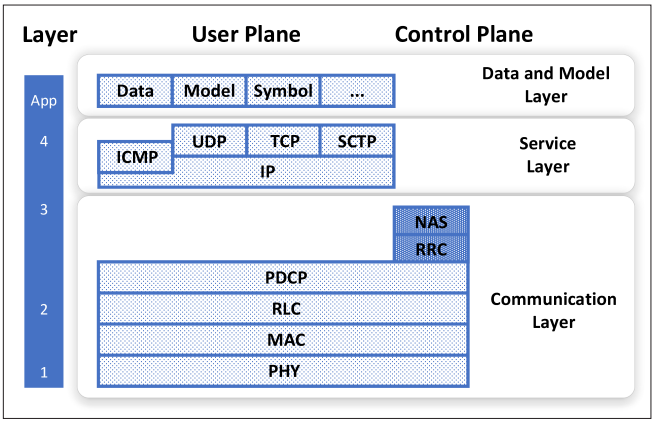

FIGURE 3. MEC protocol layers.

	Detecting the position	Feature	The Pre/ Post-attack
[10]	Gateway	Dependencies of IP MAC addresses ports	Pre-attack
[11]	MEC	Src/Dst IP,Port Protocol Packet Length	Post-attack
[8]	MEC	GTP Tunnel ID IP	Post-attack

TABLE 1. Current method of defending malicious traffic.

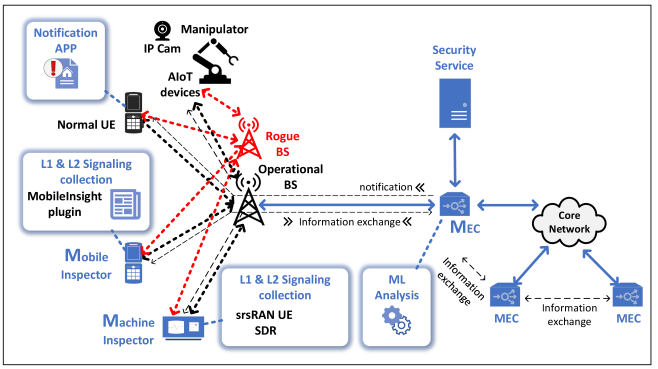

FIGURE 4. M3Inspector

	Accuracy	Precision	Recall	FPR
Malicious traffic	94.8%	67.9%	88.7%	73.89%
Rogue BS attacks	91%	91.83%	90%	8%

Table 2. The experimental results of detection.

simulation. User Plane traffic is imported into the simulation environment, and its traffic is analyzed and tested. If the traffic is detected as malicious, it can be blocked in the emulated environment, so it will not infect other devices.

Detection Mechanism

Malicious Traffic Detection. We conduct Malware attacks on this environment, collect data, and train it into a detection model. Devices that attack AIoT can also attack through file-less. Since most of the models used to detect malicious attacks are flow-based, it is impossible to accurately judge file-less attacks and know what happens after file-less attacks are launched. Due to space limitations, we are sorry that we cannot give a detailed description in the Collection phase and training phase of Malicious Traffic Detection. Therefore, we need to collect system layer information through Emulation so that we can detect the attack earlier and improve the overall security.

Rogue BS Attacks Detection. The rationale behind M3Inspector is that the unstable RF properties in the low-cost hardware are feasible indicators of rogue BS. We exploit signal strength of the base station and infamous NAS attack vector `Attach Reject`. The signal strength of these messages sent from rogue and operational BSs act differently, which is leveraged in our detector. Three phases are designed in M3Inspector to identify rogue BS.

- Collection phase. The mobile and machine inspectors are designed to receive messages from legitimate and rogue BSs. To collect real `Attach Reject` messages from operational BS, we use an expired commercial SIM card to request services from legitimate operators. We also launch a DoS attack on the rogue BS by sending malicious `Attach Reject`.
- Training phase. We observe that the signal strength sent by operational BS is small and stable while that for rogue BS is much larger. We found from the isolated rogue BS attack behavior that the rogue BSs must send a signal strength greater than all BSs in the environment to attract mobile or machine connections, so we collected one signal strength every 10 ms from the BS with the strongest signal strength in neighbors BSs, and then using the standard deviation to statistically measure the behavior of rogue and operational BSs in transmission power stability, we further make a threshold between two BSs.
- Detection phase. The mobile and machine inspector decodes the real-time signaling and transmits the corresponding strength to MEC, which determines whether the signal strength collected continuously by the mobile and machine is greater than the threshold calculated from the training dataset and detects the presence of `Attach Reject` in signaling by Mobileinsight. If yes, MEC will consider the message is from the rogue BS. The users who subscribed to the service will receive a notification from MEC to indicate a rogue BS attack.

Experimental Results

Malicious Traffic Detection: Detecting Malware attacks focus on what the attacker has done by compromising the device but ignores the traffic generated by the attacker prior to the attack [8, 11]. We trained the model using about the one million datasets generated by Malware and tested the traffic generated before the Malware attack. The results in Table 2 show that the Accuracy is 94.8 percent, but the Precision is only 67.9 percent because the malicious traffic in the test dataset is a minority, so when the model predicts wrongly, there is no significant performance in Accuracy, while in Precision, it can be seen that a lot of legitimate traffic is judged as malicious traffic, which is why the Precision is so low. Therefore, we can import the traffic into our M3Inspector Machine to help the model analyze the traffic through the emulated environment and ensure that other components are protected from malicious attacks.

Rogue BS Attacks Detection. The signal strength of the operational BSs is more stable than that of the rogue BSs [12–14], so we collect ten consecutive sets of datasets from the operational BSs in the training phase and select the worst value as the threshold value. We finally collect the signal strength of 500 sets of operational BSs and 500 sets of rogue BSs that send `Attach Reject` and predict the signal strength of 1000 datasets by the threshold value we calculated. The results are shown in Table 2. Table 2 shows that our detector has an accuracy of 91 percent in identifying `Attach Reject` attacks sent by rogue BSs. The experimental results prove that the chosen RF properties could reflect the capability of testing hardware, thereby acting as a more appropriate feature to distinguish behavior between rogue and operational BSs. By combining with the PHOENIX [14] who investigate the NAS message sequence, we believe M3Inspector can achieve higher accuracy.

Conclusion

Locating closer to the vulnerable AIoT devices in the 5G network, MEC is proved in this article as a suitable position to enable security functionality to detect and mitigate attacks in a timely manner. This article examines security threats and corresponding possible security mechanisms at MEC respectively in communications, service, and data layers for AIoT applications. The popular network-traffic-based IDS could capture the existence of infamous IoT malware attacks, while a detector in the data layer might identify poisoned models. Regarding the communications layer, we propose a novel platform, M3Inspector, where MEC utilizes the signal strength of RRC and NAS messages provided to determine rogue BS attacks. We conduct experiments in a MEC-enabled 5G environment to demonstrate the effectiveness of the M3Inspector. We also discuss ongoing research challenges and open research questions related to attack detection and mitigation in MEC. In summary, we provide the following two implications for how to enable more effective protection for AIoT devices at MEC.

- The full protections of AIoT devices are contributed by security efforts in all layers. Even though many existing solutions are proposed in the service layer to identify various classic attacks on AIoT devices, the unawareness of backdoor attacks on ML models still makes AIoT applications malfunction. In this case, MEC needs to consider threats and vulnerabilities from all aspects and design detection and mitigation schemes accordingly.
- The popularity of file-less attacks without obvious signatures makes service-layer detectors at MEC ineffective. We suggest that introducing IoT firmware re-hosting is a promising solution where system-level behavior can be captured and further analyzed to increase detection accuracy. Such a "system layer" solution in MEC acts as the fourth pillar to make detecting and mitigating AIoT threats more powerful and reliable.

References

[1] N. Neshenko *et al.*, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and A First Empirical Look on Internet-scale IoT Exploitations," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, 3rd Quarter 2019, pp. 2702–33.
[2] D. He *et al.*, "Toward Hybrid Static-Dynamic Detection of Vulnerabilities in IoT Firmware," *IEEE Network*, vol. 35, no. 2, Mar./Apr. 2021, pp. 202–207.
[3] M. A. Ferrag *et al.*, "Federated Deep Learning for Cyber Security in the internet of Things: Concepts, Applications, and Experimental Analysis," *IEEE Access*, vol. 9, Oct. 2021, pp. 138,509–42.
[4] A. Shaik *et al.*, "Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems," *Proc. NDSS 2016*, Feb. 2016.
[5] M. Mukherjee *et al.*, "Intelligent Edge Computing: Security and Privacy Challenges," *IEEE Commun. Mag.*, vol. 58, no. 9, Sept. 2020, pp. 26–31.
[6] S. Xu, Y. Qian, and R. Q. Hu, "Edge intelligence assisted gateway defense in cyber security," *IEEE Network*, vol. 34, July/Aug. 2020, pp. 14–19.
[7] M. Dai *et al.*, "An Edge-Driven Security Framework for Intelligent Internet of

Things," *IEEE Network*, vol. 34, no. 5, Sept./Oct. 2020, pp. 39–45.
[8] C.-Y. Li *et al.*, "Transparent AAA Security Design for Low-Latency MECintegrated Cellular Networks," *IEEE Trans. Vehic. Tech.*, vol. 69, no. 3, Mar. 2020, pp. 3231–43.
[9] A. Mudgerikar, P. Sharma, and E. Bertino, "Edge-Based Intrusion Detection for IoT Devices," *ACM Trans. Manag. Info. Systems*, vol. 11, no. 4, Oct. 2020.
[10] G. De La Torre Parra *et al.*, "Detecting Internet of Things Attacks Using Distributed Deep Learning," *J. Network and Computer Applications*, vol. 163, p. 102662, 2020.
[11] M. Gusatu and R. F. Olimid, "Improved Security Solutions for DDoS Mitigation in 5G Multi-Access Edge Computing," *CoRR*, vol. abs/2111.04801, 2021; https://arxiv.org/abs/2111. 04801.
[12] Z. Li *et al.*, "FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild," *Proc. NDSS 2017*, Jan. 2017.
[13] C. Quintin, "Detecting Fake 4G LTE Base Stations in Real Time," *Proc. USENIX Enigma 2021*, Feb. 2021.
[14] M. Echeverria *et al.*, "PHOENIX: Device-Centric Cellular Network Protocol Monitoring Using Runtime Verification," *Proc. NDSS 2021*, Jan. 2021.
[15] Y. Li *et al.*, "MobileInsight: Extracting and Analyzing Cellular Network Information on Smartphones," *Proc. ACM MobiCom 2016*, Oct. 2016, p. 202–15.

Biographies

Shin-Ming Cheng (smcheng@mail.ntust.edu.tw) received his B.S. and Ph.D. degrees in computer science and information engineering from the National Taiwan University, Taipei, Taiwan, in 2000 and 2007, respectively. Since 2012, he has been on the faculty of the Department of CSIE, National Taiwan University of Science and Technology, Taipei, where he is currently a professor. He is also a joint assistant research fellow with the Research Center for Information Technology Innovation, Academia Sinica, Taipei. His current interests are mobile network security and IoT system security. Recently, he investigates malware analysis and AI robustness. He has received IEEE Trustcom 2020 best paper awards.

Bing-Kai Hong (d10815003@mail.ntust.edu.tw) received his B.S. degree in computer science and information engineering from the National Taiwan University of Science and Technology, Taipei, Taiwan, in 2018. He is currently a Ph.D. candidate of the Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, Taipei. He visited EURECOM and NICT Cybersecurity Lab in 2018 and 2019, respectively. His research interests are secure system integration and development using virtualization technologies in mobile networks and IoT systems. He has received a 4-year scholarship of the Ministry of Science and Technology, CISC 2020 and TANET 2021 best paper awards.

Cheng-Feng Hung (d10915002@mail.ntust.edu.tw) received his B.S. degree in information technology and applications the college of science and engineering from the National Quemoy University, Kinmen, Taiwan, in 2019. He is currently a Ph.D. candidate in the Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, Taipei. He visited the Warsaw University of Technology in 2022. His research interests are MEC security in mobile networks.