Efficient IoT Attack Detection in The Fog Layer

Edna M. Chaar Santana, Doctoral Student
Polytechnic University of Puerto Rico
ednachaar@gmail.com

Jeffrey Duffany, Ph.D.
Ana G. Mendez University
jeffduffany@uagm.edu

Abstract

The use of Internet of Things devices has grown significantly by 2021, making it more attractive for attackers to damage the system by stealing information, physically attacking the equipment, stopping working correctly, blocking access, and many other possible attacks. These attacks can occur on IoT equipment in businesses or an individual's residential environment. Currently, there is a crucial need to have an efficient intrusion detection system (IDSs) designed for this environment of IoT devices and to be able to mitigate attacks. This research will help find an efficient way to detect attacks on IoT devices in the fog layer with a signature-based intrusion detection system. We analyze four scenarios with attacks and no malicious nodes in Contiki OS with Cooja Simulator to measure the results.

Keywords: Internet of Things, Fog Layer, Attack Detection, Cybersecurity, Signature-based detection

Introduction

The internet of things (IoT) is a growing topic since almost everything is being created to work wirelessly and independently. The IoT is a paradigm that allows communication between electronic equipment and sensors through the internet to facilitate our lives; It also uses intelligent devices and the internet to provide innovative solutions for related problems in various businesses (Kumar et al., 2019). The number of Internet of Things (IoT) devices worldwide is forecast to almost triple from 8.74 billion in 2020 to more than 25.4 billion IoT devices in 2030; In 2020, the highest number of IoT devices will be found in China 3.17 billion devices. IoT devices are used in all types of industry verticals and consumer markets, with the consumer segment accounting for around 60 percent of all IoT-connected devices in 2020. This share is projected to stay at this level over the next ten years (Transforma Insights, 2020).

There is a problem of attacks on IoT devices due to the increase in utility of this equipment in our daily lives in residences and all types of businesses. This increase is also due to the situation experimented on from the COVID-19 pandemic, which creates a perfect environment for hackers (Paul, 2021). Currently, two teams are connected to the internet every three minutes (Waheed et al., 2021). Cyber threats are multiplying, making the existing security and privacy measures inadequate (Waheed et al., 2021). A lot of data is also stored in the cloud network, which can cause delay and congestion problems in the cloud (Rashid et al., 2020). A recent example of a cybersecurity attack is the Mirai botnet, which exploited the default passwords in May IoT devices like IP Cameras digital video recorders and coordinated a distributed denial of service (DDoS) attack to many targets (Ioulianou et al., 2018). According to research by Kaspersky, Internet of Things devices is more vulnerable to cyberattacks than they ever have been before. The data shows that more than 1.5 million attacks occurred on IoT equipment in the first six months of 2021,

identifying a more significant increase of 100%. Kaspersky data also revealed that hackers use these compromised devices to mine for cryptocurrency, launch DDoS attacks, or steal confidential data (Paul, 2021).

This research will help find an efficient way to detect attacks on IoT devices in the fog layer with a signature-based intrusion detection system. There is an advantage of seeing attacks in the fog layer before the attack reaches the network cloud where the computer's data is stored (Anwer et al., 2021). These advantages are that the Internet service provider and the network administrator can apply some measures to stop the destruction of the network attack (Anwer et al., 2021). There are many ways to detect these attacks, and with this research, you will be able to evaluate the best alternative of accuracy in detection. There is a lot of research on attack detection with different types of Signature-based detection, anomaly-based, and specification-based (Liao et al., 2013).

This Signature-based intrusion attack detection system can detect anomaly-based attacks where it tries to recognize malicious behavior; to be able to achieve this, it is required to have a previous creation of profiles to define the expected behavior of users, hosts, and networks; the profile is created considering functionalities and security policies of the systems and is consulted periodically (Ioulianou et al., 2018).

Attacks

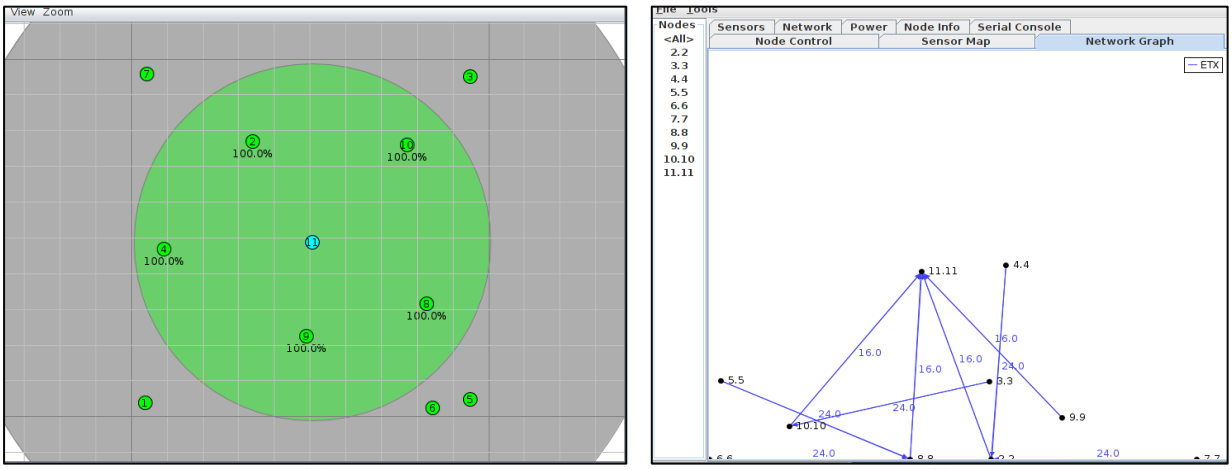
There are different attacks on these IoT devices where the attacker can change the firmware and access the recorded or in-transit data. One of the attacks that can happen is the non-network side-channel attack; It is another method to exploit the hardware, the DoS attacks is another threat such as battery draining and resources exhaustion; also, another attack can arise where the attacker can clone the node and the packets can be modified and redirected and the level of connectivity that it was an encounter the eavesdropping attack in which the attacker sniffs network packets and tries to export critical information (Yang et al., 2017). To carry out an intrusion detection system as a security measure, there are many challenges since different network structures, power of smart devices, and various developed protocols of IoT devices (Zarpelão et al., 2017).

IoT equipment can be used for DoS attacks against the selected target. Also, another example of an attack is when they attacked the security cameras to proceed with the DoS and DDOS attacks that caused the fall of Twitter. These attacks demonstrate that IoT devices are not a hardware solution but a component of the physical environment, hardware, and connection to the internet (Koupaei & Nazarov, 2020).

Methodology

In this investigation, the method used to analyze the literature of articles related to the attacks in IoT devices and the vulnerability of being attacked. To design an effective IDS, it must first implement a scenario of attacks and observe their impact on the individual devices; various detection techniques were implemented to be tested and improved (Ioulianou et al., 2018). A scenario of Denial of Service (DoS) attacks on IoT equipment was also carried out using a Cooja Simulator through a virtual machine with VMware Fusion was created to install Contiki 2.7 (Linux) as the operating system.

To use the Cooja Simulator, it was used a topology attack on Routing Protocol for Low power and Lossy Network (RPL) being a protocol for 6LoWPAN network, to bring the concept of Internet of Things (IoT) to real-life (Le et al., 2016). In the RPL protocol, a topology was recreated in the network of nodes connected to a node and done with benign nodes and others with malicious ones. In each of the scenarios, the following data was used as a comparative method: from the sensors, the average temperature was compared, in the network area packets received over time and per node were compared, and finally, the characteristics of the power were studied in the average power consumption of each of the nodes. Figure 1 shows the results of the network (a) of scenario one and its network graph (b). In this scenario, it can see half of the nodes outside the radius range of the sink node, and in the middle with the number eleven is the sink node.



(a) *(b)*

Figure 1 Scenario one Network and Sensor Map

In the following table 1, the four scenarios worked on in this investigation in the Cooja Simulator are identified. In Scenario one, it was used ten nodes, and one sink was used where 50% of the nodes were Inside the radio range of the sink node and the other 50% outside the range. In the second scenario, nine nodes were used, one malicious node and one sink node. In this scenario, the malicious node was outside the radio range of the sink node. In scenario three, seven nodes were used, one sink node and three malicious were studied outside the sink's radius range. In the last scenario, number four, it was worked with five nodes, one sink node, and one malicious node where the malicious nodes were located outside the radius range of the sink node. These scenarios were used to see the results and compare them when an attack occurs versus when it was used a no malicious node.

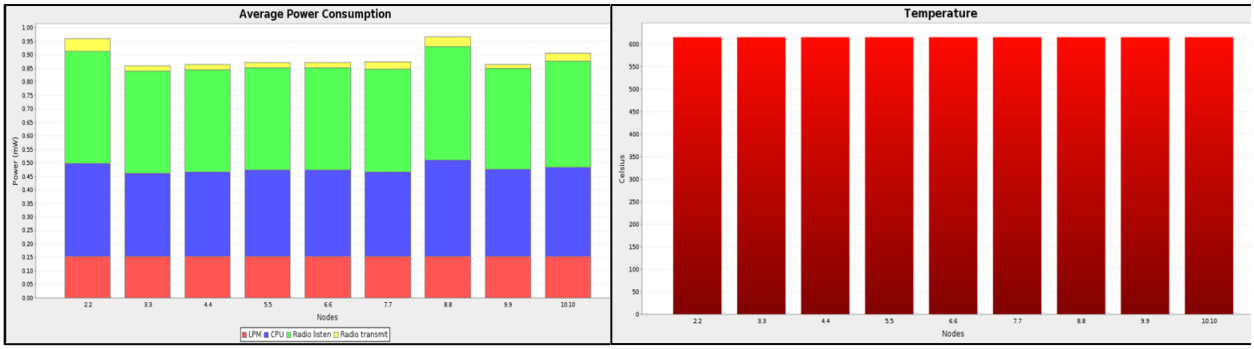
Table 1: Types of Scenarios

Four Scenarios	Description
Scenario One	10 Nodes 1 Sink Node 50% Inside Radio Range of Sink Node and 50% Outside (No malicious Nodes- All nodes are Legitimate)
Scenario Two	9 Nodes 1 Sink Node and 1 Malicious Node 10% Outside Radio Range of Sink Node (Malicious Node)
Scenario Three	7 Nodes 1 Sink Node and 3 Malicious Node 30% Outside Radio Range of Sink Node (Malicious Node)
Scenario Four	5 Nodes 1 Sink Node and 5 Malicious Node 50.0% Outside Radio Range of Sink Node (Malicious Node)

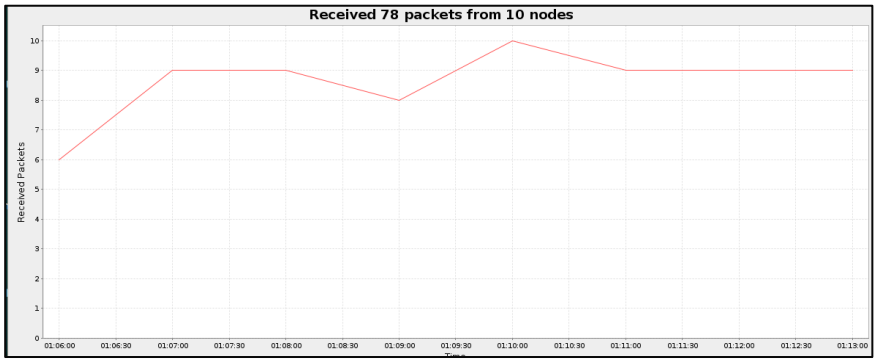
Results and Conclusion

The four scenarios studied in the Cooja Simulator increase its average power consumption when the node is under attack. The attacked nodes receive a higher number of packets than those not infected. The more energy and power the network uses, the shorter its lifetime (Le et al., 2016). Also, when the experiment with attacks was carried out, to have the result of the metrics used in each one of the nodes, it took a little more time than the tests that were carried out without attacks.

In conclusion, when the node is attacked, it creates congestion in the network and high energy consumption in the node that has been attacked. Figure 2 shows the performance of scenario one, and it can be seen how the nodes make a regular consumption of average power consumption (a), as well as the temperature (b) and the packets received, were adequate with no malicious node (c).



(a) (b)



(c)

Figure 2: The performance of scenario one

Future Work

It will be considered to expand the investigation with other IoT devices attack simulation software and reach a real-world IoT environment.

Acknowledgment

This material is based upon work supported by, or in part by the National Security Agency (NSA) under contract/award H98230-20-1-0411

References

Anwer, M., Khan, S. M., Farooq, M. U., & Waseemullah, W. (2021). Attack Detection in IoT using Machine Learning. *Engineering, Technology & Applied Science Research*, *11*(3), 7273–7278. https://doi.org/10.48084/etasr.4202

Ioulianou, P. P., Vassilakis, V. G., Moscholios, I. D., & Logothetis, M. D. (2018). A Signature-based Intrusion Detection System for the Internet of Things. *IET Conference Publications*, *2018*(CP747). https://doi.org/10.1049/cp.2018.1419

Koupaei, A. N. A., & Nazarov, A. N. (2020). Security Analysis Threats, Attacks, Mitigations, and Its Impact on the Internet of Things (IoT). *Synchroinfo Journal*, *6*(4), 36–41. https://doi.org/10.36724/2664-066x-2020-6-4-36-41

Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. *Journal of Big Data*, *6*(1). https://doi.org/10.1186/s40537-019-0268-2

Le, A., Loo, J., Chai, K. K., & Aiash, M. (2016). A Specification-Based IDS for Detecting Attacks on RPL-Based Network Topology. *Information (Switzerland)*, *7*(2). https://doi.org/10.3390/info7020025

Paul, D. (2021). *IoT Devices See More Than 1.5bn Cyberattacks so Far This Year*. DIGIT. https://www.digit.fyi/iot-security-kaspersky-research-attacks/

Rashid, M. M., Kamruzzaman, J., Hassan, M. M., Imam, T., & Gordon, S. (2020). Cyberattacks detection in IoT-based smart city applications using machine learning techniques. *International Journal of Environmental Research and Public Health*, *17*(24), 1–21. https://doi.org/10.3390/ijerph17249347

Transforma Insights. (2020). *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030 (in billions) [Graph]*. Statista. https://ezproxy.pupr.edu:2087/statistics/1183457/iot-connected-devices-worldwide/

Waheed, N., He, X., Ikram, M., Usman, M., Hashmi, S. S., & Usman, M. (2021). Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures. *ACM Computing Surveys*, *53*(6). https://doi.org/10.1145/3417987

Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, *84*(September 2016), 25–37. https://doi.org/10.1016/j.jnca.2017.02.009