Intrusion Detection with Wireless Sensor Network (WSN) Internet of Things

Aria Hendrawan, April Firman Daru , and Alauddin Maulana Hirzan
Faculty of Information Information Technology and Communication, Universitas Semarang.
ariahendrawan@usm.ac.id

***Abstract*— The development of network technology is growing rapidly; in the past, all devices were connected using cables as communication media. But since wireless technology was introduced, all of these devices began to adapt the wireless technology. Internet of Things is an example of a device that relies on wireless technology. The device uses wireless technology to communicate with each other. However, despite the many benefits gained by this wireless technology, there are great hidden danger. If this wireless technology is not properly protected by the network, it is vulnerable to being target of active network attacks such as Denial of Service (DoS). DoS attacks can paralyze targets on the network. In addition, this attack is also able to disable the IoT devices that are connected directly to it and thus cause the device to be unable to send vital information to users of IoT device. This research has successfully produced a sensor system that can detect active network attacks, and subsequently generate reports through the MQTT protocol.**

***Index Terms*— Internet of Things; Intrusion Detection System; Wireless Sensor Network.**

I. INTRODUCTION

Wireless technology is a technology where communications between two or more devices are performed without cable as media. This technology is now widely used for various types and purposes, such as: sharing a printer, sending data from one device to another, even as a local network game can be served using this technology. WIFI is a wireless technology that is implemented in several electronic devices such as laptops, netbooks, mini PCs, and the Internet of Things (IoT). IoT is a technology in which all devices are connected. To connect, IoT devices use wireless technology, namely Bluetooth and WIFI.

Figure 1: Internet of Things connectivity

Most of the sensors in IoT technology also use wireless technology to connect with central processing system. Data sent from the IoT sensor uses the MQTT standard which is known for the ease of sending information.

But behind the large benefits of this wireless technology, some dangers turn out to be quite risky. There are so many problems that may arise in the use of this wireless technology [1-3].

Many intrusions within the network such as Denial of Service attacks, Middleman, Cryptography Attack, Identity Theft, and Network Injection often occur on this wireless network [4-5]. Attacks that cause network paralysis can be called a flooding attack where the target device is flooded with many packets of data that are not useful.

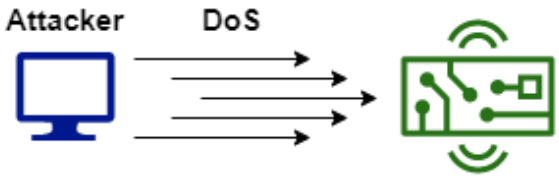

Figure 2: Illustration of Denial of Service

The target device is forced to process the incoming data. Internet attacks such as Denial of Service itself have various types of variations and ways to knock out targets. PING of Death is a way of flooding a target by flooding the target with lots of packets from the ping tool.

So, the target becomes paralyzed and must be restarted to restore the device. The flooding attack itself exists in both IP version 4 and IP version 6 protocol. Hence whatever protocol is used on the IoT device, flooding attacks cannot be avoided.

The intrusion detection within a wireless network, a special Intrusion Detection System (IDS) is designed for detecting specific packets of intrusion. These IDS will do its job as Wireless Sensor Network (WSN) to capture, detect, and report malicious packet that flows to the IoT devices. This research aims to illustrate the extent to which wireless network security can protect from active attacks and design prototypes to detect active attacks using one of the Raspberry Pi devices.

This WSN can detect any intrusion within the wireless network and report them back to the administrator computer. By notifying the administrator about the intrusion, he can start the mitigation process to protect the data against data loss caused by the intrusions. There are several theoretical benefits from implementing the WSN technology, such as providing other researchers deeper IPv6 packet information, and data safety for the stakeholders that implement IoT technology.

The current state-of-the-art of Wireless Sensor Network has been successfully implemented this security technology in many fields. One of the researchers proposed a smart grid communication model to detect a cyber attack within the network. The model in the research offered an intrusion detection system with an effective energy management system [6].

The next research in the Wireless Sensor Network proposed a detection model with the Logo Pattern Matching

(LPM) method to detect intrusions. This method is an improvement from a Signature-based detection to reduce false alerts. The detection result of this model has fewer false alerts than normal signature-based IDS [7].

Unlike the previous research that used a signature to detect intrusions, the next research proposed a new WSN model that implements a Support Vector Machine algorithm and static signature to detect intrusions within a distributed network. The proposed WSN model was implemented in a Raspberry Pi board to detect intrusions. The experiment results of the research found that the model can effectively fulfill its role as an Intrusion Detection System in a constrained device like Raspberry Pi boards [8].

However, implementing data mining and signature-based detection on a constrained device is difficult. The device has limited processing capability, and less memory to store the process. To avoid this problem the next research proposed a trust-based distributed detection method. Unlike previous researches that relied on the algorithm, the next research preferred the neighbor reputation approach to detect the intrusions. The proposed model in the research capable to located malicious host that sends intrusion to the network [9].

The heterogeneous IDS found in the next research focused on an IDS that capable to detect intrusion in a heterogeneous environment of IoT. The IDS was based on the automata model, and capable to detect 3 (three) different intrusions such as reply-attack, false-attack, and jam-attack [10].

However most of the IDS made by previous researches were not focused on IPv6 intrusions, one of many features in IPv6 was used for Denial of Service attacks in IPv6 [11]. IPv6 intrusions carried a similar impact as a normal intrusion, but the protection against it is still not completed yet. The research of Snort-based IDS with Deep Packet Inspection (DPI) embedded inside the Mikrotik router found that the designed IDS capable to detect intrusion effectively and efficiently [12]. However, the designed IDS cannot detect IPv6 intrusion and reporting the system to the Administrator. As a solution to this problem, this research proposed IPv6 Intrusion Detection System which capable to detect and report every intrusion within a wireless network.

II. Research Method

To collect the information and evaluating the intrusion detection system, a certain experiment setup is needed. In this experiment, a computer and a Raspberry Pi 3B must be connected through a wireless network using IPv6 addressing. This setup will be the topology network for collecting data before designing the IDS for IoT. The intrusion tools used in this experiment are THC-IPv61. These tools are penetration tools used only for the IPv6 environment, where security experts can test their system specifically in the IPv6 network.

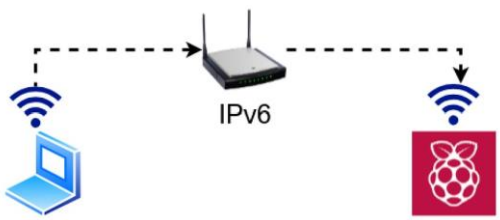

Figure 3: Experiment setup for collecting data

The topology above consists of two devices with specified roles such as a computer as the intrusion initiator, and Raspberry Pi as a victim and intrusion reporter. This research chose a Raspberry Pi board as the victim because this board has sufficient processing power to process both intrusion and reporting mechanisms.

The intrusions used in this experiment are a flooding attack type, where the intrusion will flood the network with a specially crafted packet toward the target. This research utilized ICMPv6 and TCP protocols as the main flooding attacks [13-16]. Hence, the used intrusions for the experiments are listed in the following table:

Table 1
Used Intrusions' Information

No.	Intrusion Name	Description
1	Denial6	Flood target with Denial of Service
2	RandICMP6	Flood target with random ICMPv6 packets
3	THCSync6	Flood with customized TCP packets

These intrusions will attack the victim, and all activities during the flooding will be captured using a network capture tool. The captured data (network packets) are analyzed to get the characteristic of each packet. These characteristics will be used as a signature database for IoT wireless sensor networks.

Table 1
Intrusion Characteristic Information

No.	Intrusion Name	Parameter	Value
1	Denial6	Payload Length	30
		Router Alert	05 02 00 00
		Next Header	3A
		Data	83 00 b0 0b 00 00 00 00 00 00 00 00 00 00
2	RandICMP6	Payload Length	16
		Type	01
		Reserved	00 00 00 00
		Data	00 00 00 00 00 00 00 00
3	THCSyn6	Payload Length	20
		Flags	50 10
		Window Size	40 38
		Urgent Pointer	00 00

This information can be obtained by analyzing each captured packet and store the similar or repeating pattern in each packet. The analysis process must follow the documentation that is already defined by *the Internet Engineering Task Force* (IETF). Both Denial6 and RandICMP6 were defined with ICMPv6 message format, meanwhile, THCSyn6 was defined with TCP Specification. Each of the documentation contains information on how the datagram can be extracted from too many portions such as the Header and Payload datagram. Both protocols have two major parts called Header and Payload datagram, and each of them carries information that might contain intrusion patterns. The signature is implemented inside the IDS (tight coupling) using a basic tree structure of nested IF(s). The use of nested IF(s) is to simplify the process and increase the detection speed. Compared to the external signature definition, the internally defined signature is safe against accidental delete but must edit the whole system when adding a new signature.

III. RESULT AND DISCUSSION

The experiment in this research implemented a Wireless Sensor Network to act as an Intrusion Detection System to a Raspberry Pi version 3B (short: RPi3). This board has enough processing power compared to another single-board computer and equipped with standard networking features such as Wireless Fidelity, Bluetooth, and Ethernet jack.

The designed IDS must be able to detect the intrusion by using data or string searching. If a packet that arrived in the IoT device contains something similar to the signature, then the IDS will display a notification within its application. This design of the algorithm explains how the prototype of IDS does the packet capture, datagram splitting, and pattern similarity check.

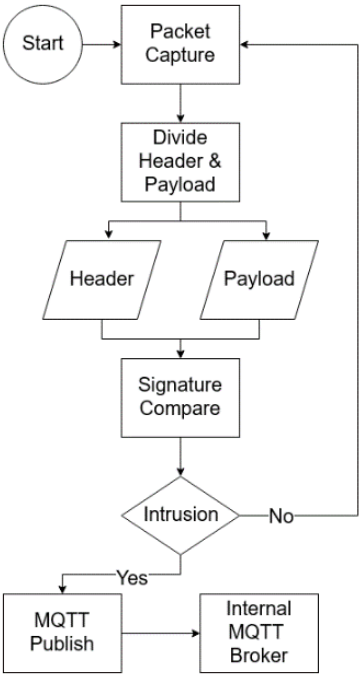

Figure 4: Detection flowchart of IDS

The packet from the attacker must be captured. The captured packet(s) will be divided into two portions (header, and payload). Each of the portions contains information that can be used for intrusion detection with the signature. The reporting process is explained below:

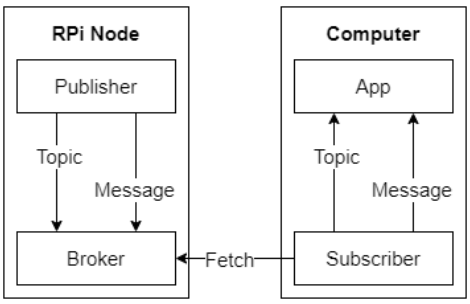

Figure 5: Report fetching process

If the packet(s) is indicated as an intrusion, then the IDS will send a report by using the MQTT protocol to the main computer. Through MQTT Broker, all detections made by the IDS are sent to the Subscriber (Computer Side).

The IDS was implemented inside the Raspberry Pi 3 device and executed in real-time through SSH remoting service [17]. The designed Intrusion Detection System tested using the same experimental setup with an additional network. This additional network offers less power usage compared to the Wi-Fi network. This additional network is made using Bluetooth Personal Area Network (PAN) which is limited in range and speed rate connecting both IoT devices and the main computer [18]. Hence the full setup for the testing phase:

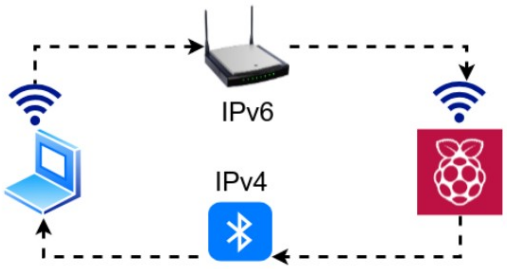

Figure 6: Testing experiment configuration

Basically, in this testing phase, two indicators dictate the success of intrusion detection. There is a detection backlog written in the IDS system and the received report on the main computer. The reporting mechanism inside the IDS system will be triggered when the detected intrusion reached a certain number of packets. Due to the difference between intrusion flooding packets, the threshold for each intrusion will be different. The testing experiment was conducted for each intrusion resulting in the detection shown in the table.

Table 3
Intrusion Detection Result

No.	Intrusion Name	TP	TN	FP	FN
1	Denial6	✓	x	x	x
2	RandICMP6	✓	x	x	x
3	THCSyn6	✓	x	x	x

The intrusion packet of Denial6, RandICMP6, and THCSyn6 are detected as True Positive (TP). And there is no packet detected in field True Negative (TN), False Positive (FP), and False Negative (FN). This means that the IDS capable to detect IPv6 intrusion effectively. The next result of the test is the result of the reporting mechanism sent by IDS to the main computer. The reporting mechanism was sent using MQTT protocol through the secondary network which safe from intrusion.

Table 2
Report Status

No	Intrusion Name	Report Received
1	Denial6	✓
2	RandICMP6	✓
3	THCSyn6	✓

The table shown above, explains that the main computer successfully receives the report through a secondary network built using Bluetooth PAN. However, each intrusion has different flooding packets so the trigger threshold for each report is different.

IV. CONCLUSION

Based on the findings from the test, the wireless sensor system can effectively detect IPv6 intrusions where no packets fall into True Negative, False Positive, or False Negative. Since all neutral packets do not contain an intrusion characteristic, then those packets are automatically included in the False Negative category. Besides the detection itself, the reporting mechanism also has an important role in the IDS. Since the main network is crowded with the intrusions, the IDS is unable to send reports through that network. Therefore, the secondary network setup with Bluetooth PAN offers a secondary network for the report submission to the main computer. And the test result shows that the report successfully reached to the main computer.

ACKNOWLEDGMENT

We thank *Lembaga Penelitian dan Pengabdian Kepada Masyarakat* (LPPM) Universitas Semarang for the financial support and the wisdom.

REFERENCES

[1] A. Aarthy Devi, A. K. Mohan, and M. Sethumadhavan, "Wireless Security Auditing: Attack Vectors and Mitigation Strategies," 2017, doi: 10.1016/j.procs.2017.09.153.

[2] M. Bijone, "A Survey on Secure Network: Intrusion Detection & Prevention Approaches," Am. J. Inf. Syst. Vol. 4, 2016, Pages 69-88, 2016, doi: 10.12691/AJIS-4-3-2.

[3] Y. Zhang and X. Huang, "Security and privacy techniques for the industrial internet of things," in Advanced Sciences and Technologies for Security Applications, 2019.

[4] Z. A. Khan and P. Herrmann, "A trust based distributed intrusion detection mechanism for internet of things," Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA, no. March 2017, pp. 1169–1176, 2017, doi: 10.1109/AINA.2017.161.

[5] A. A. Gendreau and M. Moorman, "Survey of intrusion detection systems towards an end to end secure internet of things," 2016, doi: 10.1109/FiCloud.2016.20.

[6] L. Chhaya, P. Sharma, G. Bhagwatikar, and A. Kumar, "Wireless sensor network based smart grid communications: Cyber attacks, intrusion detection system and topology control," Electron., vol. 6, no. 1, 2017, doi: 10.3390/electronics6010005.

[7] J. P. Ananth, S. Balakrishnan, and S. P. Premnath, "Logo Based Pattern Matching Algorithm for Intrusion Detection System in Wireless Sensor Network," Int. J. Pure Appl. Math., vol. 119, no. 12, pp. 753–762, 2018, [Online]. Available: https://acadpubl.eu/hub/2018-119-12/articles/7/1636.pdf.

[8] A. Sforzin, F. G. Marmol, M. Conti, and J. M. Bohli, "RPiDS: Raspberry Pi IDS - A Fruitful Intrusion Detection System for IoT," 2017, doi: 10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0080.

[9] Z. A. Khan and P. Herrmann, "A trust based distributed intrusion detection mechanism for internet of things," 2017, doi: 10.1109/AINA.2017.161.

[10] Y. Fu, Z. Yan, J. Cao, O. Koné, and X. Cao, "An Automata Based Intrusion Detection Method for Internet of Things," Mob. Inf. Syst., 2017, doi: 10.1155/2017/1750637.

[11] A. S. Ahmed, R. Hassan, and N. E. Othman, "Denial of service attack over secure neighbor discovery (SeND)," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 8, no. 5, pp. 1897–1904, 2018, doi: 10.18517/ijaseit.8.5.6427.

[12] A. Sagala and R. Pardosi, "Improving SCADA security using IDS and MikroTIK," J. Telecommun. Electron. Comput. Eng., vol. 9, no. 1–4, pp. 133–137, 2017.

[13] O. E. Elejla, B. Belaton, M. Anbar, and A. Alnajjar, "Intrusion Detection Systems of ICMPv6-based DDoS attacks," Neural Comput. Appl., vol. 30, no. 1, pp. 45–56, 2018, doi: 10.1007/s00521-016-2812-8.

[14] O. E. Elejla, M. Anbar, B. Belaton, and B. O. Alijla, "Flow-Based IDS for ICMPv6-Based DDoS Attacks Detection," Arab. J. Sci. Eng., vol. 43, no. 12, pp. 7757–7775, 2018, doi: 10.1007/s13369-018-3149-7.

[15] A. Mishra, S. Sharma, and A. Pandey, "A Review on DDOS Attack, TCP Flood Attack in Cloud Environment," SSRN Electron. J., vol. 8, no. 1, pp. 110–116, 2020, doi: 10.2139/ssrn.3565043.

[16] M. S. Al-Hawawreh, "SYN flood attack detection in a cloud environment based on TCP/IP header statistical features," ICIT 2017 - 8th Int. Conf. Inf. Technol. Proc., no. January, pp. 236–243, 2017, doi: 10.1109/ICITECH.2017.8080006.

[17] A. Uddin, "Design and Analysis of Real-time Network Intrusion Detection and Prevention System using Open Source Tools," Int. J. Comput. Appl., vol. 138, no. 7, pp. 6–11, 2016.

[18] S. M. Darroudi and C. Gomez, "Bluetooth low energy mesh networks: A survey," Sensors (Switzerland). 2017, doi: 10.3390/s17071467.