INVESTIGATION AND PENETRATION OF DIGITAL ATTACKS ON ZIGBEE-BASED IOT SYSTEMS

Fal Sadikin [1)*], Nuruddin Wiranda [2)]
[1)] PJJ Informatics Engineering, Amikom University Yogyakarta
Jl. Ring Road Utara, Ngringin, Condongcatur, Kec. Depok, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55281
[2)] Computer Education Study, FKIP, Lambung Mangkurat University
Jl. Brigjen Jalan Hasan Basri, Pangeran, Kec. Banjarmasin Utara, Kota Banjarmasin, Kalimantan Selatan 70123
e-mail: fal_sadikin@amikom.ac.id[1)], nuruddin.wd@ulm.ac.id[2)]
[*]e-mail korespondensi : fal_sadikin@amikom.ac.id

ABSTRACT

The market for Internet of Things (IoT) products and services has grown rapidly. It has been predicted that the deployment of these IoT applications will grow exponentially in the near future. However, the rapid growth of IoT brings new security risks and potentially opens up new types of attacks for systems and networks. This article outlines various techniques to carry out attacks on ZigBee-based IoT systems. We conducted penetration experiments on various possible attacks on Zigbee-based IoT. The purpose of this experiment's results is for reference in developing an Intrusion Detection System (IDS) specifically for ZigBee-based IoT.

Keywords*: Penetration of attacks on Zigbee IoT, Detection Method Reference, Attack Survey on ZigBee.*

I. INTRODUCTION

Deployment of the internet of things (IoT) has increased quickly. In many different application fields, including industrial automation systems, safety systems, home automation, and building automation systems, it has emerged as a top technology for providing innovative solutions. This IoT also has the potential to introduce new security issues because of the marriage of two crucial elements of the IoT-based system, namely large-scale deployment and the nature of devices with limited capabilities. To overcome this issue, the researchers introduced an innovative intrusion detection technique designed exclusively for IoT systems using ZigBee.

Intrusion Detection Systems (IDS) are the top technology for spotting attacks and rule violations in interconnected digital systems, according to numerous security frameworks and standards. To address specific challenges in the large-scale deployment of IoT systems, we surveyed and penetrated possible digital attacks on ZigBee-based IoT. The data results from this experiment can be used as a reference in the development of IDS for ZigBee-based IoT.

II. RESEARCH METHODS

In order to obtain accurate results, the researchers used a combination of concept study methods and experiments (practice) in this study.

A. Concept Investigation and Digital Attack Experiments

To build a structured research concept, the researchers conducted a comprehensive study of how the ZigBee protocol works and how its communication architecture is implemented in IoT systems. Furthermore, the researchers also investigated all potential digital attacks that might occur, then validated the potential attacks with penetration experiments on examples of ZigBee-based IoT applications.

B. Related Research

In general, a security system can be implemented through three stages, starting with organizational policy rules, prevention with authentication and access control techniques, then monitoring and detection. The following were examples of organizational policy rules [1], [2]. Prevention with authentication techniques and access control could be seen from examples [3]–[9]. Then, monitoring and detection could be adopted through methods [10]–[21].

Intrusion Detection for IoT Systems covered a number of research subjects, including machine learning, wireless technologies, network analysis, data analysis, and detection methods. This section summarized the latest IDS technologies for IoT systems, focusing on research from the previous two years at the time this article was written.

Various methods were used to analyze and detect attacks on IoT device systems, including using data analysis methods for various connection modes such as WiFi, ZigBee, and Bluetooth [22]–[28], [28], [29], [29]–[44].

The Intrusion Detection System methodology has, in brief, been comprehensively investigated using a variety of existing technologies, such as rule-based detection, anomaly-based detection, machine learning, and deep learning detection methods. To the best of the researchers' knowledge, however, none of them specifically addressed the issue of presenting a detection mechanism for a range of attack and exploit scenarios on substantial ZigBee-based IoT systems.

III. RESULTS AND DISCUSSION

A. ZigBee Protocol

The architecture of the ZigBee stack and the network topologies described in the ZigBee specifications released by the ZigBee Alliance are succinctly outlined in this section by the researchers [18]. Creating ZigBee intrusion detection required an understanding of the various ZigBee stack tiers.

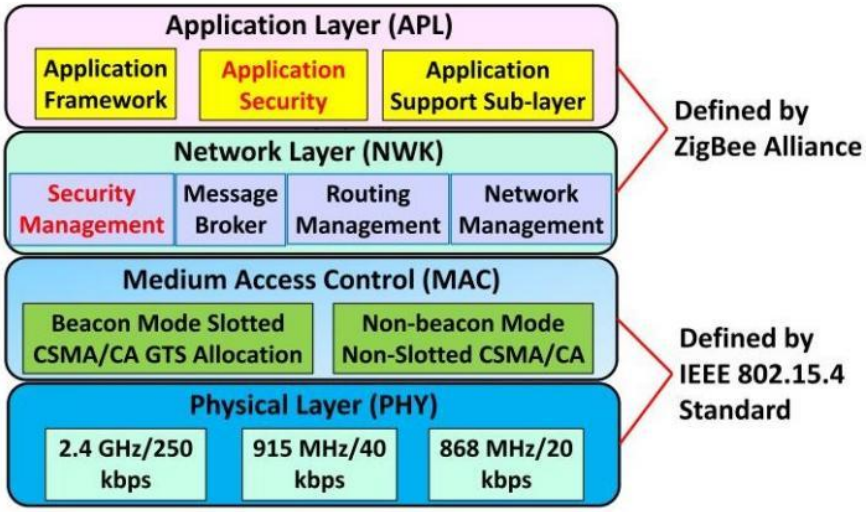

Figure 1. ZigBee Protocol

1) ZigBee Stack Architecture

The ZigBee Alliance has created wireless communication protocols for incredibly affordable, power-efficient devices, as stated in the ZigBee Specification. Consumer electronics, home and building automation, industrial control, medical sensor applications, and gaming all use ZigBee-based solutions.

There are several layers in the stack of the ZigBee protocol. For the layers above and below it, every layer provides a certain set of services. An illustration of the ZigBee Stack Architecture can be found in Figure 1. On top of two standards, the ZigBee Stack architecture was created. The IEEE 802.15.4 standard specified the bottom layers, particularly the Physical Layer (PHY) and Medium Access Control (MAC). The Network Layer (NWK) and Application Layer (APL), respectively, were the higher layers that the ZigBee Alliance defined. The ZigBee network layer and application layer provided security features like message encryption and detection.

ZigBee utilized three distinct frequency ranges. Europe used the lower frequency range at 868 MHz, whereas the United States, Australia, and other nations used the higher frequency band at 915 MHz. The 2.4 GHz higher frequency band was utilized on a global scale. 16 unique 2.4 GHz ZigBee channels were shown in Figure 2, ranging in frequency from channel 11 at 2405 MHz to channel 26 at 2480 MHz.

2) ZigBee Network Topology

Network topologies including star, tree, and mesh are defined by the ZigBee specification. A single ZigBee coordinator device managed the network when it was organized in a star topology. For initiating and managing devices on the network, the ZigBee Coordinator was in charge. Direct communication with the ZigBee coordinator is used by all other devices, often known as end devices.

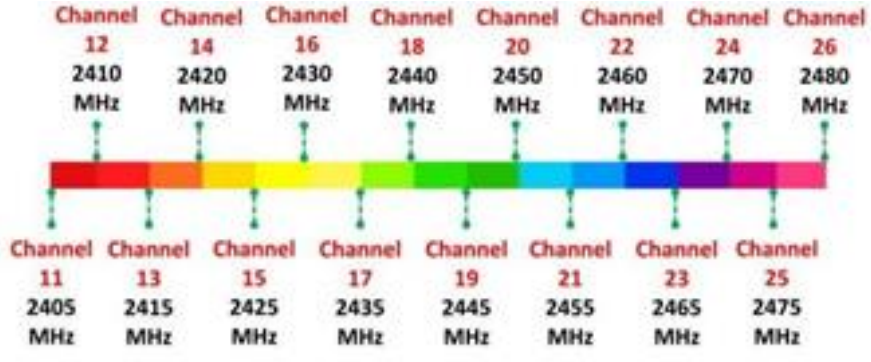

Figure 2. ZigBee Channel Frequency

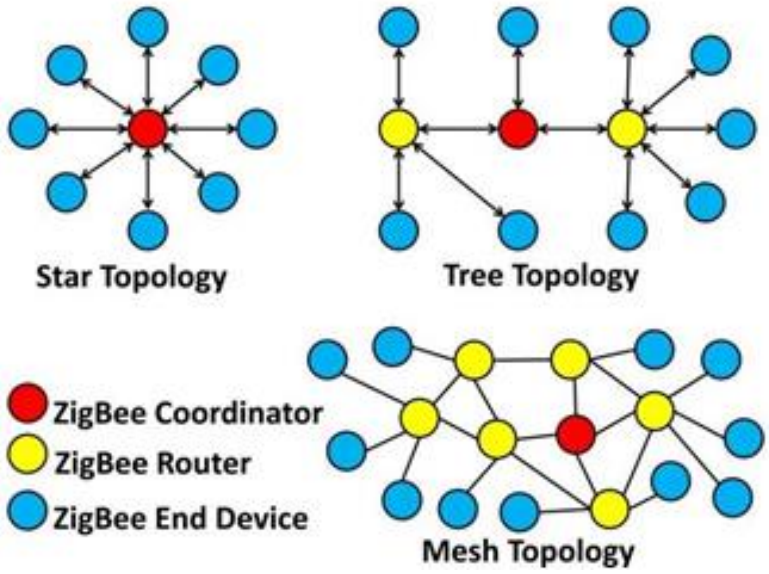

Figure 3. Zigbee Network Topology

In mesh and tree topologies, a single ZigBee coordinator was in charge of setting up the network and choosing a few important network settings. However, the network could grow by using ZigBee routers. A hierarchical routing approach was used by routers in a tree network to move data and regulate messages through the network. Beacon-oriented communication, as outlined in the IEEE 802.15.4 specification, could be used in tree networks. Peer-to-peer communication was possible thanks to the mesh network. The ZigBee Network Topology was shown in Figure 3.

B. Attack Scenario

The lower layer of the ZigBee protocol stack, which is specified by IEEE 802.15.4, and the higher layer, which is defined by the ZigBee Alliance, are depicted in Figure 1 as the two main layers of the protocol stack. This paragraph discussed different ZigBee device attacks. The researchers categorized the following four types of threats in ZigBee-based IoT systems:

- **Reconnaissance**: The antagonist attempted to use its devices to scan the ZigBee network in order to gather information for additional attacks.
- **Denial-of-Service (DoS)**: An adversary attempted to stop the ZigBee IoT system from performing certain functions or services.
- **Malicious Control**: An adversary attempted to pretend to be a trustworthy device in order to operate a ZigBee device without authorization and misuse it..
- **Device Hijacking**: Enemy attempted to hijack authorized devices. In this instance, successful piracy under duress can result in the genuine user losing control of their device.

The researchers discussed several vulnerabilities and potential exploitation scenarios on ZigBee IoT devices in this section. The researchers focused on two attack types in particular: attacks on the ZigBee MAC and Network Layer and attacks employing ZigBee Inter-PAN instructions. Figure 4 displayed a taxonomy of potential ZigBee IoT device attacks.

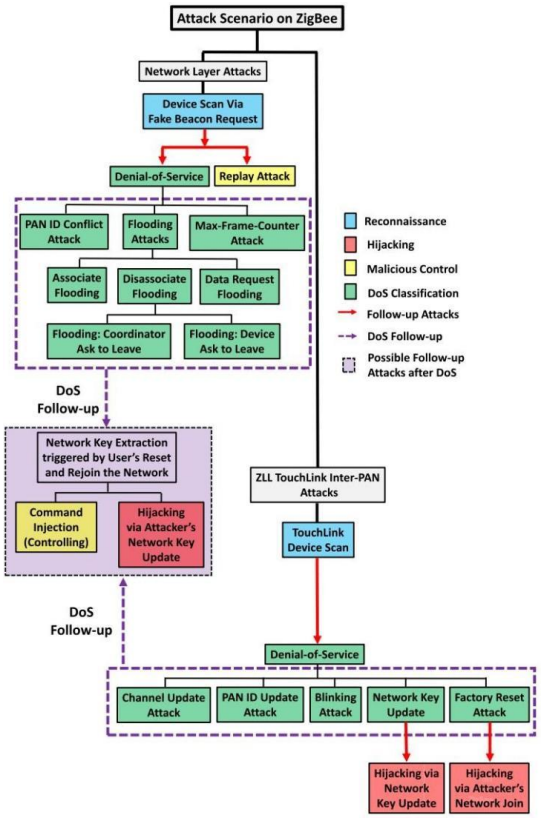

Figure 4. Attack taxonomy and exploitation scenarios on ZigBee devices

1) ZigBee MAC and Enemy Network Layer Attacks

An adversary could damage the ZigBee protocol's capabilities at the MAC and NWK layers to launch a range of assaults, including reconnaissance, denial of service, malicious control, or hijacking to seize control of a user's device.

a) Enemy Reconnaissance

The information from every active ZigBee device within wireless range could be easily gathered by an enemy. This may be done, for instance, by listening in on every ZigBee communication on a particular ZigBee channel. An attacker might also bundle a ZigBee Beacon_Request and broadcast it on the ZigBee channel that the original ZigBee device used. The researchers identified the enemy's bogus beacon request as a Fake_Beacon_Request. To locate the target device, adversaries could broadcast a Fake_Beacon_Request on all ZigBee channels. The coordinator and router gadgets within ZigBee wireless range would respond with a beacon frame after receiving this message. By gathering all beacon frames, the adversary might learn vital details about the network and its constituent devices. The enemy can utilize the data acquired to carry out additional attacks. The procedure for reconnaissance was shown in Figure 5.

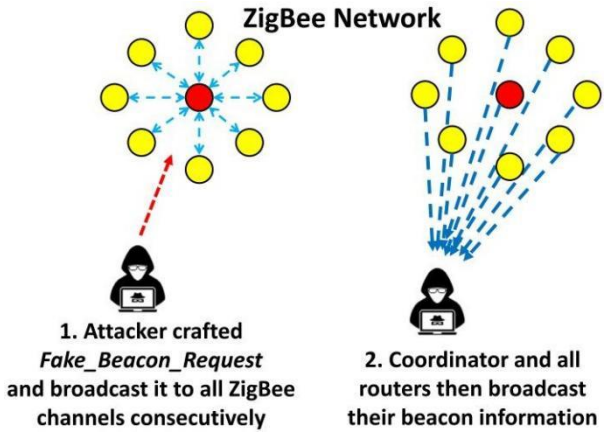

Figure 5. Reconnaissance by faking beacon requests

By collecting mail responses from coordinators and routers in the ZigBee network, adversaries could get the

following information:

- **Channel information**: The target network's channel could be revealed by adversaries by broadcasting a Fake_Beacon_Request to all ZigBee channels (channels 11-26) and waiting for the device to respond. These exposed channels were important information that could be used by enemies for a variety of purposes, including finding targets and carrying out further attacks.
- **Protocol Version**: The ZigBee coordinator and router's response to the beacon frame included details on the network's protocol version. In order to determine the types of potential attacks and exploitation scenarios that could be carried out further, the protocol version was queried. Furthermore, based on the protocol version, adversaries could reveal the type of ZigBee application.
- **PAN ID**: A PAN ID was used by ZigBee to identify a PAN (personal area network). This was a 16-bit address that needed to be distinct throughout an interconnected ZigBee network. The enemy would require the target network's PAN ID to successfully launch additional attacks.
- **Extended PAN ID**: In a ZigBee network, a network's Extended PAN ID (EPID) was used to identify it specifically. It may also be used to resolve PAN ID conflicts across different networks. The EPID feature could be used by adversaries to launch DoS attacks (such as PAN ID conflict attacks) among other things.
- **List of all active devices**: An attacker needs to obtain details about all currently operating devices, including their corresponding short ZigBee addresses and MAC addresses, in order to identify a target.
- **Device Capability**: Information on device and network capabilities was included in the beacon response (e.g., coordinator, end device, and router capability). These details could be gathered by adversaries in order to plan attacks on the ZigBee network.
- **Signal Strength**: Each ZigBee device's range or location from observers (such as advertising devices) was represented by its signal strength. The ZigBee network's topology might therefore be understood by enemies using this information.

Adversaries could be able to get useful information by collecting ZigBee beacons from networked devices. This knowledge was crucial for identifying targets and formulating follow-up strike plans.

b) Hazardous Control After Obtaining Sufficient System Information

Through reconnaissance activity, adversaries could discover the device's role in the ZigBee network. The enemy might then select targets and construct harmful scenarios such as rogue control. There were numerous techniques for rogue control, one of which was to use previously received ZigBee frames from authorized devices. This type of attack was known as a replay attack.

The enemy intercepted ZigBee frames delivered by authorized devices on the network during a replay assault. The adversary used the sniffer to collect the frame (such as a ZigBee command frame) and retransmitted it at a later time to pass for the authorized device. If the receiving device didn't check the frame counter or had deleted the sender's most recent frame counter from its memory, this kind of attack might be successful. In this scenario, the authorized device was tricked into believing that the frame was sent from a real network device. For example, if an enemy sniffed and replicated a command transmitted by an authorized user (e.g. a command to unlock a door), an adversary could resend a command to open a door when the user was not at home.

c) Denial-of-Service

The adversary could conduct a variety of denial of service attacks after gathering enough information about the target device. The researchers covered some of the methods for conducting DoS attacks in brief in the list that follows. Each ZigBee network in a region must have a distinct PAN ID, per the requirements of the ZigBee specification. As long as their PAN IDs are distinct from one another, various ZigBee networks can therefore function on the same channel. In a ZigBee network with a coordinator, the coordinator assigned a special PAN ID to the network. A node in the ZigBee network could send a Net work_Report Command frame of type PAN_Identifier_Conflict to alert its coordinator if it discovered another node was using the same PAN ID given by a different coordinator. After receiving network reports from their nodes, the coordinator disseminated a PAN ID realignment to all devices on their network in order to address PAN ID conflicts. This PAN ID dispute resolution method may be exploited by an adversary by faking a ZigBee beacon frame with the same PAN ID but a different extended PAN ID. In this instance, the same PAN ID was used to fool all ZigBee devices on the target network into believing that it was also being utilized by another network. In order to inform their coordinator of a fake beacon frame, all devices that received one sent a Network Report Command frame of type PAN Identifier Conflict. Figure 6 showed the experiment in which the researchers forged a beacon frame and all nodes that detected a conflict attempted to notify their coordinator using PAN_Identifier_Conflict.

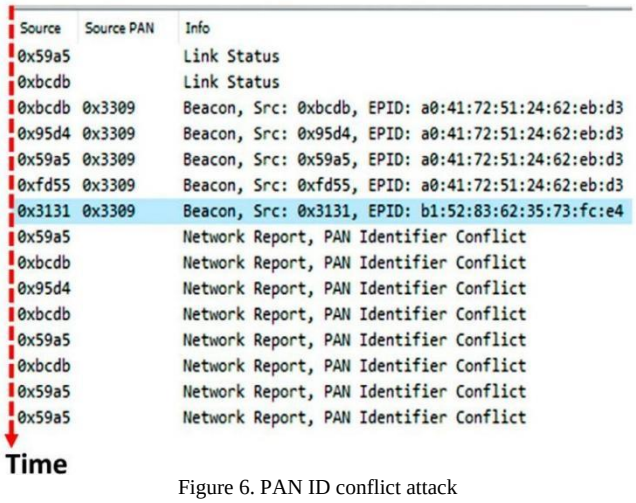

Figure 6. PAN ID conflict attack

In this experiment, a coordinator and four ZigBee nodes (0x95d4, 0x59a5, 0xbcdb, and 0xfd55) were used to construct an authorized network with PAN ID 0x3309 (and extended PAN ID a0:41:72:51:24:62:eb:d3). The malicious beacon frame was then faked with the source address of node 0x3131, which belonged to a network with the same PAN ID (0x3309) but a different extended PAN ID (b1:52:83:62:35:73:fc:e4). This was done to make the malicious beacon frame appear legitimate. In this instance, all authorized nodes informed their coordinator that a PAN ID dispute had been found.

The antagonist employed two ZigBee devices to launch a PAN ID conflict attack in order to be successful. To determine the PAN ID of the target network, the first device served as a listener. The second device was employed to repeatedly send bogus beacon frames to the target network using the discovered PAN IDs. In other words, while the second device kept transmitting erroneous beacons, the first device was listening for PAN ID changes. In this situation, the coordinator was constantly asked to modify its PAN ID by every node that received the bogus signal. This problem kept the coordinator busy by changing the PAN ID of the network and causing a DoS.

d) Max Frame Counter Attack

According to the ZigBee specification, a device's stored frame counter is increased whenever it receives a legitimate network layer or application layer message. The ZigBee device that is receiving frames compares the incoming frame counter value to the frame counter value that is saved for the sender. As a result, the packet is deleted and not further processed if the received frame counter value is not higher than the value that was previously received.

Max-Frame-Counter Attacks are a sort of DoS attack that adversaries might use this capability to launch. To achieve this, false packets are created using one of the valid source addresses, and the counter is set to its highest value. The following packet from the authorized device is discarded if the target device adjusts the frame counter's stored value to the highest value received because it has the same frame counter as the spoof packet that the adversary previously provided. If the target device wrongly verifies the MIC (Message Integrity Code) or if the implementation makes use of a crypto-suite without integrity protection, an adversary may be successful in executing this attack. If an opponent obtains access to the network key from the ZigBee network, it can also successfully set the frame counter to the highest number.

e) Flood Attack

There were numerous methods that may be used to launch a DoS assault. One of them included various flooding attacks, where the target device was repeatedly bombarded with numerous packets or fictitious requests. Due to its busy state in responding to the request, the target device would be unable to reply to requests from authorized devices. There were numerous packets or frames in a ZigBee network that could be utilized to carry out flooding attacks, including:

- **Association Request Flood**: When a ZigBee node enters a ZigBee network, it sends a certain kind of request known as an association request. To overwhelm the target network and its coordinators in a flood assault, the adversary continuously inundated the network with bogus Association_Request packets. As a result, the coordinator became overburdened with malicious requests, preventing it from responding to valid requests.
- **Data Request Flooding**: Nodes send data request frames to their parent or network coordinator throughout the join process to ask for data collection. By spoofing and overwhelming the ZigBee coordinator or router with Data_Requests, adversaries could undermine this capability.

- **Disassociate Request Flood**: With the help of a disassociation request, ZigBee also offers a method for leaving the network. There were two ways to disconnect from the network. The coordinator could first ask the device to disconnect from the network by sending a disassociation request. Second, a device that wants to disconnect from the network can do so by sending a request to the coordinator. The target nodes could be inundated with leave requests from adversaries posing as network coordinators. The converse of this situation would be for adversaries to pose as legitimate nodes and flood the target coordinator with leave requests.

Therefore, the target device (that was, the target node or coordinator) crashed because it was busy responding to flooded requests.

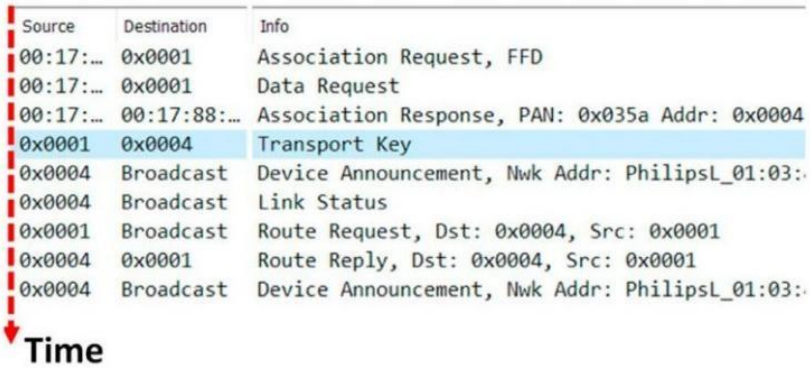

Figure 7. Network integration procedure

2) ZigBee Touchlink Inter-PAN

The ZigBee specification includes a capability called inter-PAN communication. Nodes can communicate with other nodes on various networks (with various PAN IDs) using this feature. In other words, this characteristic enables network communication. Inter-PAN communication does not use network layer security.

Lighting systems with connectivity come with some very specific criteria. ZigBee created the ZigBee Light Link (ZLL) application profile to satisfy these specifications. To enable lighting use cases where a device with limited capabilities, like a portable remote control, can commission a lighting unit, ZLL introduced TouchLink Commissioning via Inter-PAN connection. Using Touchlink Commissioning, a number of functionalities, including network settings, may be managed.

As seen in Figure 4, adversaries could use Inter-PAN TouchLink instructions to launch a variety of attacks in addition to other MAC layer and network layer attacks. Various sorts of denial of service attacks, malicious control, and reconnaissance are examples of such assaults. Reconnaissance attacks aim to hijack users' access to their devices and collect network and device information.

3) Follow-up Attack after DoS

A ZigBee network could be subject to different DoS attacks, as was covered in the section before this one. Authorized users were unable to manage their devices if a DoS attack was successful. In this case, the user could reset the gadget to factory settings and reconnect it to a working network. By intercepting ZigBee traffic during recommissioning, adversaries could take advantage of this user behavior to acquire and recover genuine network keys. The fact that the keys were frequently encrypted using a well-known global key and transferred during the network join process made this attack possible. The test of stealing keys while using a regular network connection is shown in Figure 7. In this test, network integration was carried out by first sending Associate_Request and Data_Request to the coordinator/bridge (0x01, for instance). Upon receiving the request, the coordinator sends an Associate_Response to give the device the network key via the Transport_Key command and the device's ZigBee network address, which is typically 0x04. An international key specified by the ZigBee standard was used to encrypt Transport_Key for earlier devices. With the use of recovered network keys, adversaries might launch command injection attacks on other approved targets or employ key upgrades to take control whole networks.

a) Command Injection

If an adversary successfully recovered the network key (e.g., via key transport sniffing), it might successfully impersonate an authorized device and take control of the target device. The adversary might then use the retrieved keys to encrypt/decrypt communications and join the network. Due to this, attackers were able to send requests (like "unlock the door" or "turn on the light") that seemed legitimate to other network devices. These orders might be acknowledged by the target device if they were encrypted and authenticated using a network key, depending on the ZigBee device's settings.

b) Piracy Through Key Renewal

An adversary may impersonate a lawful device and carry out any action that seemed legitimate to other network devices after obtaining the network key. In this attack scenario, the attacker might take the role of a coordinator for ZigBee and provide the target node instructions to update its network key to a value of their choosing. The Network_Key_Update command was sent to the target device by the pretend coordinator in order to accomplish this. The target device then changed to the enemy's network key after receiving the network key update. The device was no longer controllable by devices on the approved network once it joined the adversary's network and could only be controlled by the adversary.

IV. CONCLUSION

This article had demonstrated various techniques for carrying out attacks on ZigBee communication systems. The researchers conducted various digital attack penetration experiments that might occur on a ZigBee-based IoT system, ranging from types of attacks aimed at reconnaissance of IoT equipment, sabotaging network systems on ZigBee, to hijacking the control system of IoT equipment. The researchers used the data from this penetration to develop a more accurate IDS system capable of detecting various types of attacks that might occur on a ZigBee-based IoT system.

ACKNOWLEDGMENTS

The authors would like to thank all parties involved for the support of the success of this research. The authors would especially want to thank the universities included during the work process, PJJ Informatics Engineering of Amikom Yogyakarta University as well as the Computer Education Study Program of FKIP ULM Banjarmasin.

REFERENCES

[1] F. S. Mohammad, "FRAMEWORK UNTUK MENYUSUN NETWORK POLICY PADA INSTITUSI PENDIDIKAN," *Telematika*, no. 8, 2011.

[2] M. F. Sadikin, "Framework untuk menyusun Network Policy pada institusi Pendidikan," in *Seminar Nasional Informatika (SEMNASIF)*, 2015.

[3] M. F. Sadikin and M. Kyas, "Efficient key management system for large-scale smart RFID applications," in *2015 1st International Conference on Industrial Networks and Intelligent Systems (INISCom)*, IEEE, 2015, pp. 126–132.

[4] M. F. Sadikin and M. Kyas, "Security and privacy protocol for emerging smart RFID applications," in *15th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, IEEE, 2014, pp. 1–7.

[5] M. F. Sadikin and M. Kyas, "Efficient Security and Privacy Protection for Emerging Smart RFID Communications," *Int. J. Networked Distrib. Comput.*, vol. 2, no. 3, pp. 156–165, 2014.

[6] M. F. Sadikin and M. Kyas, "Light-weight Key Management Scheme for Active RFID Applications," *EAI Endorsed Trans. Ind. Netw. Intell. Syst.*, vol. 2, no. 5, pp. e4–e4, 2015.

[7] M. F. Sadikin and M. Kyas, "RFID-tate: Efficient security and privacy protection for active RFID over IEEE 802.15. 4," in *IISA 2014, The 5th International Conference on Information, Intelligence, Systems and Applications*, IEEE, 2014, pp. 335–340.

[8] M. Fal Sadikin and M. Kyas, "IMAKA-Tate: secure and efficient privacy preserving for indoor positioning applications," *Int. J. Parallel Emergent Distrib. Syst.*, vol. 30, no. 6, pp. 447–463, 2015.

[9] M. F. Sadikin, "Efficient Security and Privacy Protection for Large-scale Wireless Indoor Positioning Applications," PhD Thesis, https://refubium.fu-berlin.de/handle/fub188/12552, 2015.

[10] F. Sadikin and S. Kumar, "Zigbee IoT intrusion detection system: A hybrid approach with rule-based and machine learning anomaly detection.," in *IoTBDS*, 2020, pp. 57–68.

[11] F. Sadikin, T. Van Deursen, and S. Kumar, "A ZigBee intrusion detection system for IoT using secure and efficient data collection," *Internet Things*, vol. 12, p. 100306, 2020.

[12] F. Sadikin, T. van Deursen, and S. Kumar, "Corrigendum to'A ZigBee intrusion detection system for IoT using secure and efficient data collection'Internet of Things, Volume 12, December 2020, 100,306," *Internet Things*, vol. 19, p. 100523, 2022.

[13] F. Sadikin, T. van Deursen, and S. Kumar, "A ZigBee intrusion detection system for IoT using secure and efficient data collection (vol 12, 100,306, 2020)," *INTERNET THINGS*, vol. 19, 2022.

[14] M. F. SADIKIN, "Analisis kinerja infrastruktur jaringan komputer Teknik Elektro Universitas Gadjah Mada," PhD Thesis, Universitas Gadjah Mada, 2008.

[15] N. Wiranda and F. Sadikin, "Pembelajaran Mesin untuk Sistem Keamanan-Literatur Review," *IJEIS Indones. J. Electron. Instrum. Syst.*, vol. 12, no. 1.
[16] J. Mueller, Y. Al-Hazmi, M. F. Sadikin, D. Vingarzan, and T. Magedanz, "Secure and efficient validation of data traffic flows in fixed and mobile networks," in *Proceedings of the 7th ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks*, 2012, pp. 159–166.
[17] M. F. Sadikin, "Cyber-security Defense in Large-scale M2M System: Actual Issues and Proposed Solutions," in *Proceedings of the International Conference on Security and Management (SAM)*, The Steering Committee of The World Congress in Computer Science, Computer …, 2013, p. 1.
[18] M. F. Sadikin, "Monitoring and Optimization in computer networks services at Faculty of Electrical Engineering UGM," 2009.
[19] N. Wiranda and F. Sadikin, "Machine Learning for Security and Security for Machine Learning: A Literature Review," in *2021 4th International Conference on Information and Communications Technology (ICOIACT)*, IEEE, 2021, pp. 197–202.
[20] M. F. Sadikin, S. S. Kumar, and M. M. Siraj, "A lighting device." Google Patents, Aug. 25, 2022.
[21] M. F. Sadikin and F. Estevez, "Apparatus and method or filtering advertisements in wireless networks." Google Patents, Feb. 16, 2023.
[22] A. Heidari and M. A. Jabraeil Jamali, "Internet of Things intrusion detection systems: A comprehensive review and future directions," *Clust. Comput.*, pp. 1–28, 2022.
[23] M. A. Ferrag, L. Shu, O. Friha, and X. Yang, "Cyber security intrusion detection for agriculture 4.0: machine learning-based solutions, datasets, and future directions," *IEEECAA J. Autom. Sin.*, vol. 9, no. 3, pp. 407–436, 2021.
[24] Z. K. Maseer, R. Yusof, S. A. Mostafa, N. Bahaman, O. Musa, and B. A. S. Al-rimy, "DeepIoT. IDS: hybrid deep learning for enhancing IoT network intrusion detection," *Comput. Mater. Contin.*, vol. 69, no. 3, pp. 3945–3966, 2021.
[25] X. Zou *et al.*, "Current Status and Prospects of Research on Sensor Fault Diagnosis of Agricultural Internet of Things," *Sensors*, vol. 23, no. 5, p. 2528, 2023.
[26] A. Rizzardi, S. Sicari, and A. Coen-Porisini, "Analysis on functionalities and security features of Internet of Things related protocols," *Wirel. Netw.*, vol. 28, no. 7, pp. 2857–2887, 2022.
[27] K. Ntafloukas, D. P. McCrum, and L. Pasquale, "A Cyber-Physical Risk Assessment Approach for Internet of Things Enabled Transportation Infrastructure," *Appl. Sci.*, vol. 12, no. 18, p. 9241, 2022.
[28] D. G. Akestoridis, "Security Tools for Attacking and Monitoring Low-Power Wireless Personal Area Networks," PhD Thesis, Carnegie Mellon University Pittsburgh, PA, 2022.
[29] D.-G. Akestoridis and P. Tague, "HiveGuard: A network security monitoring architecture for Zigbee networks," in *2021 IEEE Conference on Communications and Network Security (CNS)*, IEEE, 2021, pp. 209–217.
[30] G. Parimala and R. Kayalvizhi, "An effective intrusion detection system for securing IoT using feature selection and deep learning," in *2021 international conference on computer communication and informatics (ICCCI)*, IEEE, 2021, pp. 1–4.
[31] X. Dang *et al.*, "Wireless Sensing Technology Combined with Facial Expression to Realize Multimodal Emotion Recognition," *Sensors*, vol. 23, no. 1, p. 338, 2022.
[32] W. Ding, W. Zhai, L. Liu, Y. Gu, and H. Gao, "Detection of packet dropping attack based on evidence fusion in IoT networks," *Secur. Commun. Netw.*, vol. 2022, 2022.
[33] M. Alkasassbeh and S. Al-Haj Baddar, "Intrusion Detection Systems: A State-of-the-Art Taxonomy and Survey," *Arab. J. Sci. Eng.*, pp. 1–44, 2022.
[34] A. F. J. Jasim and S. Kurnaz, "New automatic (IDS) in IoTs with artificial intelligence technique," *Optik*, vol. 273, p. 170417, 2023.
[35] J. Ren, "Data File Security Strategy and Implementation Based on Fuzzy Control Algorithm," *Secur. Commun. Netw.*, vol. 2022, 2022.
[36] W. Ruichen, "The Basic Principles of Marxism with the Internet as a Carrier," *Math. Probl. Eng.*, vol. 2022, 2022.
[37] A. Tedyyana and O. Ghazali, "Real-time Hypertext Transfer Protocol Intrusion Detection System on Web Server using Firebase Cloud Messaging," 2023.
[38] A. Tedyyana, O. Ghazali, and O. W. Purbo, "A real-time hypertext transfer protocol intrusion detection system on web server," *TELKOMNIKA Telecommun. Comput. Electron. Control*, vol. 21, no. 3, pp. 566–573, 2023.

[39] H. H. Hettiarachchige and H. Jahankhani, “Holistic Authentication Framework for Virtual Agents; UK Banking Industry,” in *Challenges in the IoT and Smart Environments: A Practitioners’ Guide to Security, Ethics and Criminal Threats*, Springer, 2021, pp. 245–286.
[40] T. Oshio, S. Okada, and T. Mitsunaga, “Machine Learning-based Anomaly Detection in ZigBee Networks,” in *2022 IEEE International Conference on Computing (ICOCO)*, IEEE, 2022, pp. 259–263.
[41] G. G. Gebremariam, J. Panda, and S. Indu, “Detection and Analysis of Flooding Attacks in Wireless Sensor Networks,” 2022.
[42] J. E. Rubio Cortés and others, “Analysis and design of security mechanisms in the context of Advanced Persistent Threats against critical infrastructures,” 2022.
[43] E. W. Lussi, H. V. Sampaio, C. A. de Souza, and C. B. Westphall, “A lightweight fog-based internal intrusion detection system for smart environments,” *Int. J. Intell. Internet Things Comput.*, vol. 1, no. 4, pp. 287–299, 2022.
[44] B. P. Padma and S. B. Erukala, “Keys Distribution Among End Devices Using Trust-Based Blockchainsystem for Securing Zigbee-Enabled Iot Networks,” *Available SSRN 4392416*.