INTRUSION DETECTION SYSTEM FOR ZIGBEE-BASED IOT USING DATA ANALYSIS RULES

Fal Sadikin [1)*], Nuruddin Wiranda [2)]
[1)]PJJ Informatics Engineering, Universitas Amikom Yogyakarta
Jl. Ring Road Utara, Ngringin, Condongcatur, Kec. Depok, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55281
[2)]Computer Education Study Program, FKIP, Universitas Lambung Mangkurat
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 new types of attacks for systems and networks. This article outlines various techniques for detecting known attacks in ZigBee-based IoT systems. We introduced an Detection System (IDS) specific for ZigBee using data analytics method, that are used to provide an accurate detection method for known attacks. This article looks at our IDS implementation covering a wide variety of detection techniques to detect known attacks ZigBee IoT systems.

***Keywords**: Data Analytics, Internet of Things, ZigBee Intrustion Detection System.*

I. INTRODUCTION

Internet of Things (IoT) deployment has expanded rapidly. It has become a prominent technology for providing innovative solutions to numerous application domains, including industrial automation systems, safety systems, home automation systems, and building automation systems. The combination of two essential aspects of such IoT-based systems, namely widespread deployment and the nature of devices with limited capabilities, has the potential to introduce new security concerns. To address these issues, we present a new intrusion detection technique designed particularly for ZigBee-based IoT systems.

Diverse security frameworks and standards recommend intrusion detection systems (IDS) as the most effective technology for detecting attacks and policy violations in connected digital systems. Regarding the development of detection techniques, IDSs employ either a predefined set of misconduct rules or machine learning (ML). IDS based on predefined rules is a strategy in which detection methods are developed using man-made rules to detect both known and unknown attacks (using man-made anomaly rules). ML-based IDS is a technique that employs ML technology to generate detection rules derived from the system's ML model for both normal (benign) and abnormal behavior. Consequently, ML-based IDS can detect both known and unknown forms of malicious behavior.

Combining rule-based intrusion detection and machine learning-based anomaly detection, we introduce our novel ZigBee intrusion detection technique to address the specific challenges of vast deployment of IoT systems. This method enables a secure, efficient, specific, and reliable IDS solution for large-scale ZigBee-based IoT deployments with the following characteristics:

- Accurate detection that aims to overcome common false positive challenges in IDS.

- In the prototype we developed, we analyzed all of the ZigBee protocol's features to determine data analysis criteria for detecting known attacks.

Specifically, this article makes the following contributions:

-Reproduction of numerous attack scenarios and their effects on network conditions in ZigBee-based IoT systems.
a novel rule-based attack detection method designed for IoT systems based on ZigBee.

II.METHOD

In this study, we employed a combination of concept study and experimental (practical) methodologies in order to obtain accurate results.

A. Developing a ZigBee IoT System

To develop a structured research concept, we conducted a thorough investigation into how the ZigBee protocol operates and how its communication architecture is implemented within IoT systems. We implemented a ZigBee-based IoT system for intelligent lighting applications. As reference material for implementing IoT attack detection, we acquire real data, particularly communication data, from the implementation of this IoT system.

B. Relevant Studies

In general, security systems can be implemented in three phases, beginning with organizational policy rules, followed by prevention using authentication and access control techniques, and concluding with monitoring and detection. Following are examples of organizational policy regulations [1], [2]. Examples [3]–[9] illustrate the use of authentication and access control techniques for prevention purposes. The monitoring and detection methods [10]-[21] can then be utilized.

Intrusion Detection for Internet of Things (IoT) systems impacts on numerous research fields, including wireless technology, network analysis, data analysis, machine learning, and detection techniques. This section provides a summary of contemporary IDS technologies for IoT systems.

Intrusion Detection for Internet of Things (IoT) systems impacts on numerous research fields, including wireless technology, network analysis, data analysis, machine learning, and detection techniques. This section summarizes the state-of-the-art IDS technologies for IoT systems, focusing on the most recent two years of research at the time this article was written.

Several techniques are used to analyze and detect attacks on IoT device systems, including data analysis techniques for various connection modes such as wifi, zigbee, and Bluetooth. [22]-[28], [28], [29], [29]-[44].

In conclusion, numerous Intrusion Detection System approaches, including rule-based detection, anomaly-based detection, machine learning, and deep learning detection methods, have been extensively studied. To the best of our knowledge, none of them specifically addresses the problem of providing detection mechanisms for various attack and exploitation scenarios on large-scale ZigBee-based IoT systems..

III. Result and Discussion

Providing reliable attack detection for both known and unknown attacks was an important aspect of the deployment of the IoT system. This section discussed our proposed solution for attack detection using an intrusion detection system (IDS) specifically designed for the massive deployment of ZigBee-based IoT systems. We further introduced our test setup, which was used as an experimental facility for various purposes. Using our test setup, we could also collect data on the normal behavior of the IDS.

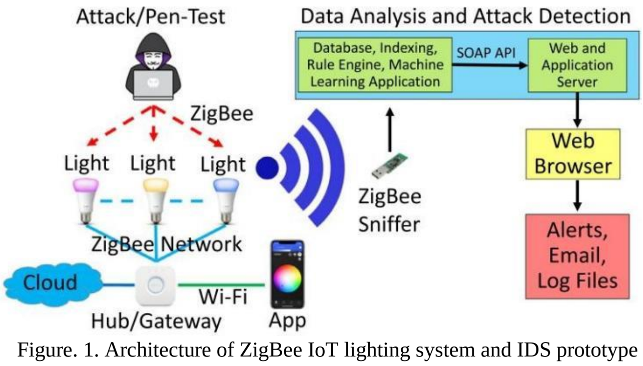

Figure. 1. Architecture of ZigBee IoT lighting system and IDS prototype

In addition, it assisted us to perform a variety of attacks to acquire data sets containing anomalies. This section concluded with a discussion of various rule-based and machine learning-based attack detection techniques.

A. Evidence of the Concept

We used a commercial ZigBee IoT lighting system as an experimental testbed to build a realistic representation of an IoT system. Authorized users in this testbed can control lights on the network using a mobile app. This includes dimming, adding additional bulbs to the network, altering the color of the lights, or turning them on and off. One gate (0x01) and three light bulbs (0x02, 0x03, and 0x04) make up the testbed.

We examined every ZigBee packet in order to compile a realistic data set, and we then stored the information in the rule engine for later analysis. We send all legal orders from the app and employ a sniffer to gather ZigBee communication in order to capture the realistically typical behavior of a valid user. In this instance, the app was frequently used to control the lights while behaving normally. Various attacks were then launched on the testbed. This made it possible to gather a realistic assortment of harmful data sets, which was helpful for precise attack detection and categorization.

In order to categorize typical and abnormal behavior, data analysis was done after gathering a large enough data set. Figure 1 depicts the ZigBee IoT IDS prototype and the design of our lighting testbed. The rule engine in the prototype was equipped with machine learning and rule-based detection techniques.

We tested the implementation of the IDS by rerunning the testbed with normal behavior and simulating the attack scenario after the rule-based detection approach and machine learning had been implemented in the rule engine. This was accomplished by relaunching each attack on the testbed and operating the lighting system via the app. In this instance, if the IDS prototype discovered an attack or unusual behavior, it would raise an alarm.

B.Rule-Based IDS

An intrusion detection technique known as "rule-based" makes use of rules that people have developed based on their expert knowledge. Human specialists can manually evaluate data sets or log files to generate rules. By developing anomaly detection rules that characterize malicious activity, rule-based intrusion detection can be utilized to identify both existing attacks and prospective future attacks.

C.Detection of Attacks

By analyzing data sets from various assault scenarios and comparing them to data sets of legitimate user behavior, it may be possible to identify a number of known attacks. Thus, the various assault types depicted in Figure 4 as well as the typical behavior of authorized users could be classified.

1) Pattern of Signal Strength

Patterns of Received Signal Strength Indication (RSSI) can be analyzed to infer malicious activity. Certain RSSI patterns, for instance, may imply malicious command injection. Each active device in standard wireless networks such as ZigBee measures the RSSI of received packets (Rx), including Rx unicast and Rx broadcast. Depending on the distance between the sender and receiver, the Rx RSSI transmitted by each adjacent device takes on a specific form. Variations in the RSSI pattern can be caused by a number of external factors, including signal reflections, human movement, and the number of people in the vicinity of the wireless network.

If an adversary attempts command injection, the legitimate device's identity (i.e., sender address) can be spoofed. By acting as a legitimate device, the adversary can convince the target device that the command was sent by a legitimate device. Due to the adversary's inability to readily forge the RSSI pattern received by the target device, there will be an atypical change in the Rx RSSI pattern. A malicious command injected by the adversary modifies the device's Rx RSSI pattern (0x03), as depicted in Figure 2. This results in a pattern spike if the adversary transmits the command from a device closer to the legitimate device than the adversary, or a pattern dip if the adversary sends the command from a device further away than the legitimate device.

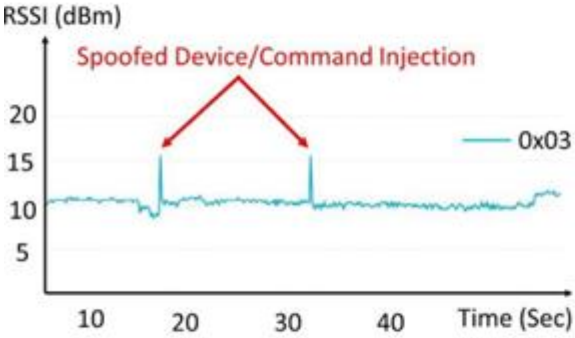

Figure. 2. Command injection and fake device detection

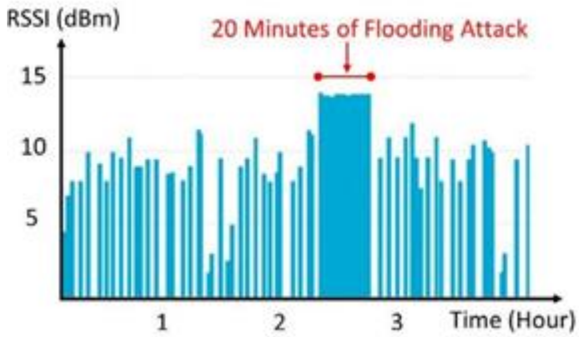

Figure. 3. RSSI pattern under flooding attack

The adversary may attempt to transmit commands with a different signal strength than the authorized device. However, it will still have an effect on the RSSI pattern, which changes as a result of external factors surrounding valid and distinct RX RSSI patterns detected by other devices.

In addition, particular RSSI patterns may be indicative of specific assaults, such as various types of flooding attacks. In other words, an RSSI value that remains stable over time is an unmistakable indicator of a deluge attack. Figure 3 depicts the assault scenario data set for a flooding attack in which the RSSI value of a device remains stable for a certain amount of time (for instance, 20 minutes). This flooding attack is carried out by spoofing the address of a single legitimate device (i.e., 0x03) and flooding the coordinator with a large number of packets with this originating address.

2) Frame Counter

By monitoring the frame counter of received ZigBee packets, it is possible to detect the presence of counterfeit devices and/or malicious command injection. According to the ZigBee specification, the value of the packet frame counter is incremented with every new transmission by the sender. In a command injection attempt, the adversary attempts to impersonate a legitimate device by spoofing the device ID and injecting commands with a higher frame counter in order to convince the target device to accept the commands. However, this type of attack scenario is detectable, as the subsequent frame from the legitimate device will have a reduced frame counter value. Figure 4 depicts the attack scenario data set for a command injection attack in which one of the injected packets has a significantly higher frame counter value.

In a replay attack, the adversary captures the original transmission from a valid device and then replays it. This type of attack could be detected by comparing the frame counter of the packet to the value of the last packet received. If the value of the frame counter is equal to or less than zero, the adversary may replay the transmission. Figure 5 depicts the data set of a replay attack scenario in which an adversary repeatedly replicates pre-recorded packets sent by a valid device (0x03).

3) Color/grayscale image

Traffic rate patterns may be indicative of certain attack symptoms. Various forms of flooding attacks could be identified by monitoring the packet rate. There was a specific pattern of normal network packet exchange in the original network traffic. Flooding attacks could be detected by determining a threshold and comparing the monitored transmission rate to this threshold. Figure 6 depicts a dataset of flooding attacks with a distinct metric, packet rate. This was the same flooding dataset depicted in Figure 3, in which the attack consisted of consistently flooding a large number of packets over a 20-minute period.

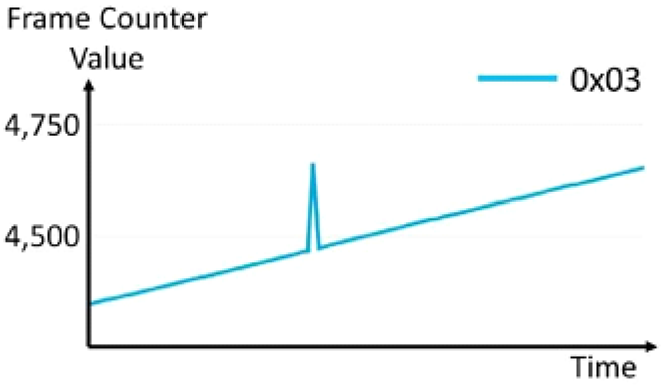

Figure. 4. Symptoms of a command injection attack

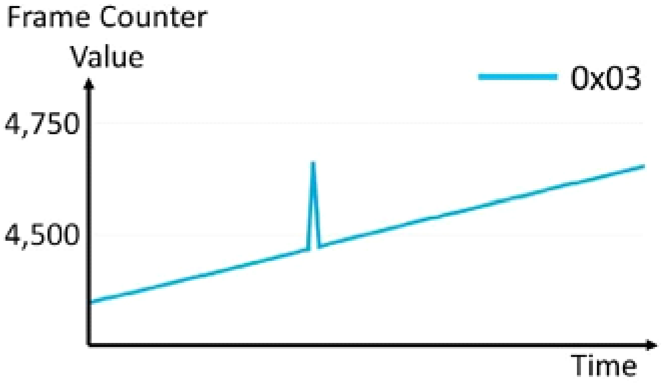

Figure. 5. Frame counter pattern during repeat attack

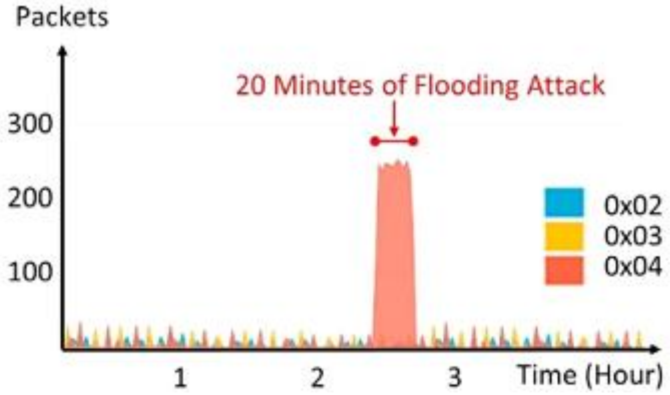

Figure. 6. Traffic Rate During Flooding Attack

4) Package Frame Format

ZigBee defines a variety of packet frame types. Some of them include data frames, command frames (e.g., network report, route request, route reply, network status, network update, etc.), and inter-PAN frames. Certain command sequences may indicate that an attacker is attempting to breach the security of the ZigBee network. For instance, the presence of inter-PAN command frames during normal operation indicates an inter-PAN TouchLink attack. TouchLink Inter-PAN is unlikely to be present during normal operation; consequently, the IDS should raise the alarm. The data set for the TouchLink Inter-PAN attack scenario is depicted in Figure 7.

TouchLink inter-PAN attacks can be classified further, and the approximate location of the adversary or malicious device can be estimated. This can be accomplished by comparing the TouchLink command identifier to the RSSI value to determine the adversary's distance. The TouchLink Inter-PAN Identifier data set transmitted by the adversary is depicted in Figure 8. In this data set, the adversary attempts multiple types of attacks by sending multiple TouchLink commands, including Scan Request (0x00), Network Update (0x16) to change the channel, Factory Reset (0x07), Request Identification (0x06) to instruct the flashing light, and Network Join Router (0x12) to hijack the device.

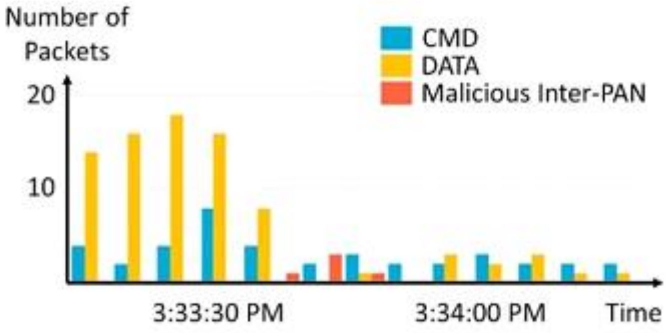

Figure. 7. Packet frame format data set

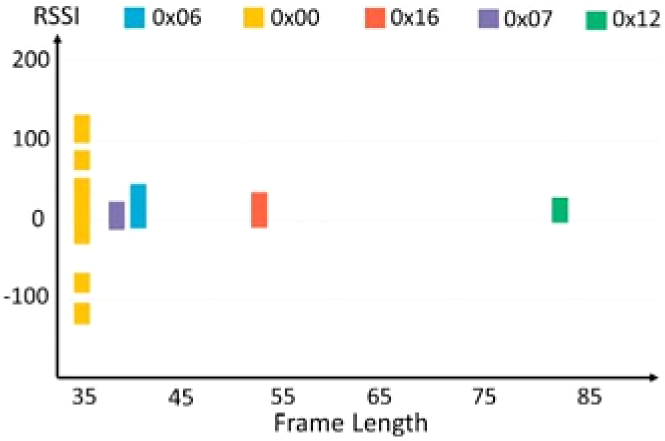

Figure. 7. TouchLink Inter-PAN Identifier distribution

IV. CONCLUSION

This article demonstrates a variety of techniques for detecting known attacks in ZigBee IoT systems. Specifically, we introduced methodologies for detecting intrusions using analysis data. We have demonstrated that rule-based methods with analysis data provide the most accurate detection mechanism for known attacks.

ACKNOWLEDGEMENT

The authors would like to thank all parties involved, for their support in the success of this research. In particular, we would like to thank the University where we work, PJJ Informatics Engineering, Amikom University Yogyakarta, and the Computer Education Study Program, 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*.