ANOMALY DETECTION IN ZIGBEE-BASED IOT USING SECURE AND EFFICIENT DATA COLLECTION

Fal Sadikin [1)*], Nuruddin Wiranda [2)]
[1)]PJJ Informatics Engineering, University of Amikom Yogyakarta
Jl. Ring Road Utara, Ngringin, Condongcatur, Kec. Depok, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55281
[2)] Computer Education Program Study, FKIP, Lambung Mangkurat University
Jl. Brigjen Jalan Hasan Basri, Pangeran, Kec. Banjarmasin Utara, 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

This article outlines various techniques for detecting types of attacks that may arise in ZigBee-based IoT system. The researchers introduced a hybrid Intrusion Detection System (IDS), combining rule-based intrusion detection and machine learning-based anomaly detection. Rule-based attack detection techniques are used to provide an accurate detection method for known attacks. However, determining accurate detection rules requires significant human effort that is susceptible to error. If it is done incorrectly, it can result in false alarms. Therefore, to alleviate this potential problem, the system is being upgraded by combining it (hybrid) with machine learning-based anomaly detection. This article expounds the researchers' IDS implementation covering a wide variety of detection techniques to detect both known attacks and potential new types of attacks in ZigBee-based IoT system. Furthermore, a safe and efficient meth-od for large-scale IDS data collection is introduced to provide a trusted reporting mechanism that can operate on the stringent IoT resource requirements appropriate to today's IoT systems.

***Keywords**: Anomaly Detection, Internet of Things, secure and efficient data collection, ZigBee Intrusion Detection System.*

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 systems, and building automation systems, it has emerged as a leading technology for providing innovative solutions. IoT also has the potential to introduce new security issues because of the marriage of two crucial elements of the IoT-based system, namely widespread deployment and the nature of devices with constrained capabilities. To solve this issue, the researchers developed a novel intrusion detection method exclusively for ZigBee-based IoT devices.

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. For IDS, there are two different strategies for developing detection techniques: based on predetermined sets of abuse criteria and based on Machine Learning (ML). IDS based on predefined criteria is a technique in which the detection is made using artificial rules to identify both known and unidentified attacks (using artificial anomaly rules). ML-based IDS is a technique that uses ML Technology to develop detection criteria for both typical (benign) and abnormal behavior that are derived from the system's ML model. So both known aberrant activity and novel attack types can be found using ML-based IDS.

To address specific issues with large-scale deployments of IoT systems, the researchers developed a new ZigBee intrusion detection technique that combines rule-based intrusion detection with anomaly detection based on machine learning. In large-scale ZigBee-based IoT deployments, this technique allows an IDS solution that is secure, effective, precise, and reliable, with the following characteristics:

- Accurate detection to combat IDS issues with false positives on a regular basis.
- Accurate unidentified assault detection through trustworthy anomaly detection.
- Effective and practical IDS data gathering for ZigBee IoT systems with limited resources. Large-scale IoT deployments face a hurdle since IDS data gathering can use up more resources (such as bandwidth and processing resources) and obstruct the functionality of IoT applications.
- Reliable IDS data collecting aims to overcome difficulties in data logging security where extensive IDS data gathering can provide a danger of data reporting alteration and falsification.
- The built prototype was used to examine every aspect of the ZigBee protocol in order to create rules for rule-based detection and train an ML model to recognize assaults.

II. RESEARCH METHODS

This study employed a combination of concept study methods and experiments (practice) to get accurate results.

A. Building a ZigBee IoT System

The researchers conducted a comprehensive study of how the ZigBee protocol works and of how its communication architecture is implemented in IoT systems to build a structured research concept. In the implementation, the ZigBee-based IoT system for smart lighting applications was built. The real data from the implementation of this IoT system were collected, especially communication data as a reference for implementing attack detection on IoT.

B. Related Research

A security system in general can be implemented through three stages, namely organizational policy rules, prevention with authentication and access control techniques, monitoring and detection. This study cited some examples of organizational policy rules from Mohammad [1] and Sadikin [2], and several examples of prevention with authentication techniques and access control from Sadikin and Mkyas [3]–[9]. The monitoring and detection was adopted from the previous research [10]–[21].

Numerous study areas, including wireless technology, network analysis, data analysis, machine learning, and detection techniques, have examined the subject of intrusion detection for Internet of Things systems. This section summarizes the latest IDS technologies for IoT systems, especially the last two years of when this study conducted.

Various methods are used to analyze and detect attacks on IoT system, one of which is data analysis method on various connection such as Wifi, Zigbee, and Bluetooth [22]–[28], [28], [29], [29]–[44].

In conclusion, numerous existing methods, including rule-based detection, anomaly-based detection, machine learning, and deep learning detection, have been used to thoroughly study the Intrusion Detection System methodology. To the best of the researchers' knowledge, however, none of them specifically address the issue of offering a detection mechanism for a variety of attack and exploit scenarios on large-scale ZigBee-based IoT systems.

III. RESULTS AND DISCUSSION

Implementing an IoT system requires reliable attack detection for both known and unidentified assaults. This section discusses the researchers' suggested approach for spotting intrusions using an intrusion detection system (IDS) especially created for wide-scale ZigBee-based IoT system deployment. The test environment, which serves as an experimental laboratory for a variety of uses, is also introduced. Using our test settings, the data of normal behavior might be collected.

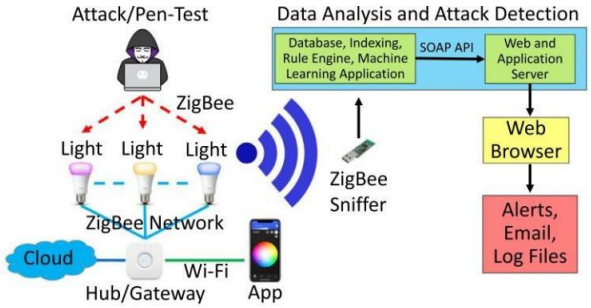

Figure 1. ZigBee IoT lighting system architecture and IDS prototype

The test configurations also enable us to carry out a variety of attacks to gather data sets with anomalies. The discussion of various attack detection strategies employing rule-based and machine learning techniques concludes this section.

A. Proof of Concept

To build a realistic simulation of the IoT system, the researchers employed a commercially available ZigBee IoT lighting system as an experimental testbed. On this testbed, authorized users can manage lights on the network via a mobile app. This includes changing the light's color, dimming it, turning it on and off, and adding a new light bulb to the network. One gate and three light bulbs make up the testbed.

By examining all ZigBee traffic, a realistic data set was gathered and stored in the rules engine for later analysis. The researchers transmitted all legal orders from the application and used a sniffer to gather ZigBee communication in order to observe authorized users' realistically typical behavior. In this instance, the app was utilized to repeatedly manipulate the lights and act normally. On the testbed, a number of attacks were then launched. This makes it possible to gather a realistic assortment of harmful data sets, which is helpful for precise attack detection and categorization.

After gathering large enough data sets, data analysis was done to categorize typical and abnormal behavior. Our

ZigBee IoT IDS prototype and lighting testbed architecture are shown in Figure 1. The rules engine in the prototype used machine learning and rule-based detection techniques.

After implementing rule-based detection and machine learning techniques in the rules engine, the testbed was run again with normal behavior and attack scenarios were recreated in order to evaluate the IDS implementation. This is accomplished by using the App to operate the lighting system and then resuming all testbed attacks. In this scenario, if the IDS prototype notices an attack or unusual behavior, it will trigger an alarm.

B. Anomaly Detection

A crucial step in locating attackers in IoT systems is anticipating and recognizing upcoming attacks. This can be achieved by developing an anomaly detection model utilizing a rule-based approach. IDS can classify anomalies when a new package or command is introduced that deviates from the norm by using a model from the usual data set.

1) RSSI Pattern

Rules for acceptable behavior can be established using a variety of techniques. Modeling the typical device RSSI pattern is one of them. In a typical office setting, the researchers set up an experiment using data on routine activity collected by a sniffer from four nearby nodes in a connected ZigBee lighting system. Figure 2 displays the distribution of the average RSSI level for each approved device. In this graph, the RSSI level for each device varies according to the number of people present and how they move around the office, particularly during business hours. Due to the comparatively low attendance on weekends in this instance, the RSSI rate pattern is largely steady. Figure 2 also demonstrates that, on weekdays, the RSSI is generally steady between the hours when most people leave the office in the evening and the hours when most people return to work the following morning.

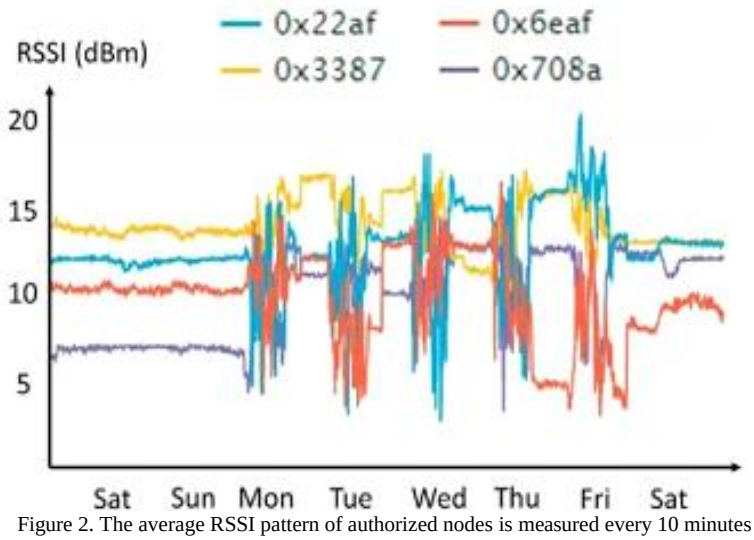

Figure 2. The average RSSI pattern of authorized nodes is measured every 10 minutes

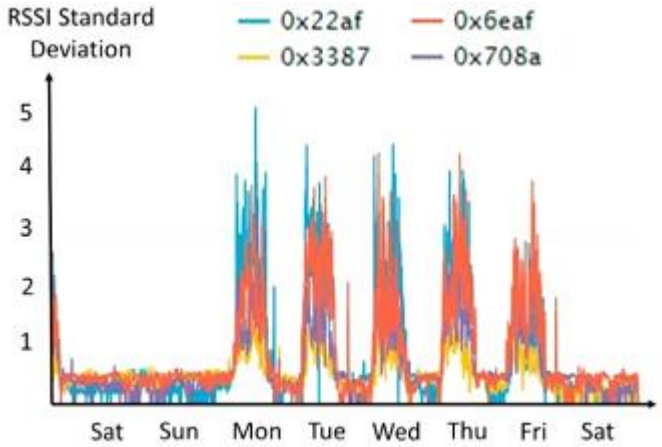

Figure 3. The standard deviation of the RSSI pattern is measured every 10 minutes

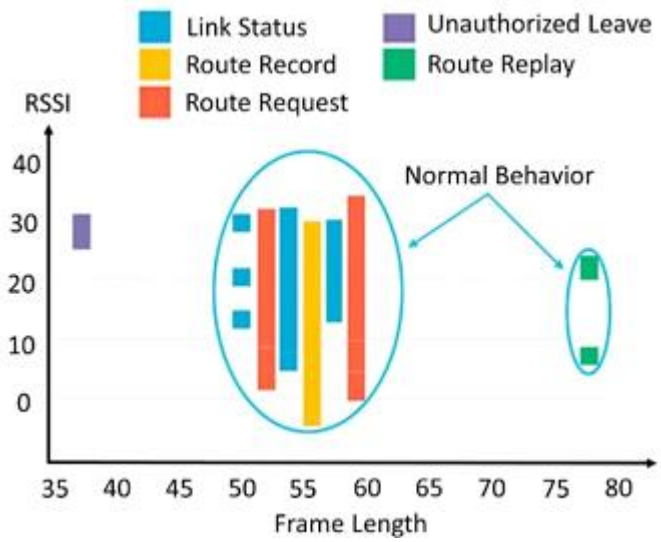

Figure 4. Anomaly detection using packet frame format

The standard deviation of the RSSI level is also calculated as a more accurate detection method to build the model. The standard deviation of the RSSI level for each device is shown in Figure 3. If the current RSSI level deviates from established norms based on past trends for various hours and days of the week, anomaly detection can locate the presence of malicious devices and faked packets. This enables the detection of well-known assaults including replay attacks, flooding attacks, spoofing, packet injection, and any other forms of unknown hostile behavior. This is due to the fact that all malicious activities (e.g., known and unknown attacks) would not conform to established patterns of normal behavior.

2) Package Frame Format

Observing packet frame format patterns is a method to modeling normal behavior. There are several approaches to doing this, one of which is combining features such as frame length, command identifier, and RSSI. A model of a ZigBee lighting system's typical behavior in an office setting is depicted in Figure 4. Figure 4 further demonstrates the adversary's abnormal directives that go outside the parameters of the conventional paradigm.

The size of the packet, the location of the source device indicated by the RSSI number, and the kind of orders sent during normal operation can all be used to build models. Using this paradigm, the following instances of normative behavior guidelines can be defined:

- The packet size (e.g., packet length) must be exactly 77 bytes, or between 50 and 59 bytes.
- The signal strength (e.g., RSSI) should be between -4 and 33 dBm.
- The Route Request, Link Status, Recorded Route, or Route Replay will be valid commands sent during normal operation.

Any package or command in general that does not comply with the normal behavior rules will be classified as an anomaly. For instance, a packet length of 37 bytes for the Leave instruction, which is a sign of a hijacking attack, is categorized as an anomaly.

The rule-based approach is efficient and offers a highly accurate and dependable detection mechanism. It has been demonstrated that rules may be used to identify prospective new attacks as well as known attacks that have already been discovered. However, the process of constructing models for accurate detection using human-made rules is difficult and time-consuming. Furthermore, since detection rules are developed and put into action by people, they are prone to inaccuracy.

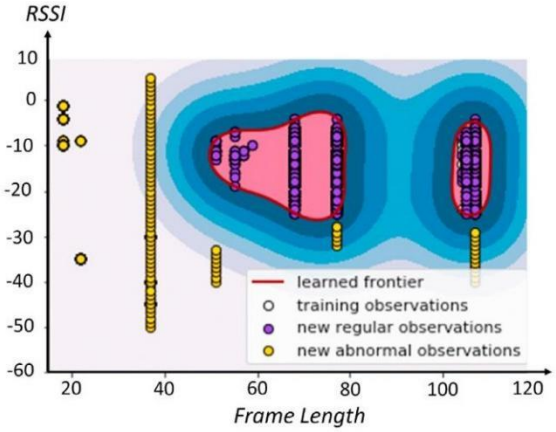

Figure 5. Set of training and test data using One-class-SVM

C. Machine Tilt Anomaly Detection

The process of building a model for anomaly detection is labor-intensive and error-prone. The researchers employed a machine learning technique to build complicated models that included a variety of ZigBee frame format features, such as RSSI, frame length, time, frame counter, and packet interval, to address this problem. To model normal behavior, a data set of testbeds for normal behavior is used. The models were specifically given datasets using One-class-SVM with a non-linear kernel (RBF). Scikit-Learn's OneClassSVM is used to implement the training/test model (sklearn.svm.OneClassSVM). The results of testing the anomaly detection model are shown in Figure 5.

By re-running the testbed to gather fresh normal observations (marked in purple) and testing the model by simulating some of the attacks (marked in yellow), the accuracy of the detection model was confirmed. Here is the attack scenario:

- *Leave* request flooding attack: To carry out this experiment, a 37-byte *Leave* command was generated and used to send flooding packets to network coordinators of various ranges. In this scenario, all flooded commands were propagated with different RSSI ranging from -53 to 7 dBm. However, the *Leave* command sent by the adversary exceeded the learned threshold, causing it classified as an anomaly. Additionally, a 22-bytes *Association_Request* command was created and used to flood the network coordinator. Flooding was carried out from two different locations: inside and outside the room where the testbed was installed. In this case, the command plots were divided into two different RSSI areas (indoors and outdoors). However, the command was classified as an anomaly because the packet length was not within the normal behavior range. Additionally, the attempted flooding attack was repeated by generating a *Data_Request* command with a length of 18 bytes. In the same result, the *Data_Request* flood was plotted outside the normal range, which was also classified as an anomaly.
- Finally, a replay attack employing previously obtained packets from a reliable device was used to evaluate the anomaly detection model. In this case, the test employed packets with lengths of 51, 77, and 105 bytes. However, because the assault was launched from a different place than where a legitimate device was installed, all commands were categorized as anomalous (i.e., outside of the expected range). The repeated assault in this instance took place outside the room. Adversaries may be able to launch repeated attacks from inside, hence the frame counter feature that was utilized to build the model must be capable of spotting these assaults.

A normalized model that may be used to identify potential network attacks can be created by combining a number of variables to identify outlier behavior in ZigBee networks. It is more effective and time-effective to simulate typical behavior using machine learning. However, non-linear kernels (RBF) have limitations in which some parts of the kernel (i.e., learned boundaries) reach the normal behavior data set. This issue creates new observations of normal behavior classifiable as anomalous, especially when they exceed the learned threshold. Therefore, the One-class-SVM model will introduce false positives in the real implementation of IDS where some legitimate messages transmitted by authorized devices will exceed the threshold of normal behavior. This implies that certain legitimate instructions and packages will be labeled as anomalous. As a result, to maintain the correctness of the normal behavior model, ongoing learning must be applied in a complimentary manner.

TABLE I
EXAMPLE OF NETWORK DIAGNOSIS AND DEFINITION

Identifying Diagnostics	Information
MacRxBcast	Every time the MAC layer receives a broadcast, a counter is increased
MacRxBcast	Every time the MAC layer transmits a broadcast, a counter is increased.
MacTxUcast	Every time the MAC layer transmits a unicast, a counter is increased
MacTxUcast	Every time the MAC layer receives a unicast, a counter is increased

D. Reliable and Efficient Data Collection

For intrusion detection to be successfully implemented in a multi-device IoT system, a safe and effective means of data collecting (such as logging) is crucial. Data gathering must be carried out effectively without materially compromising the functionality of the IoT system. Data collecting in IoT systems requires a lot less processing power and bandwidth than it does in conventional intrusion detection systems. Such effective data collecting must also adhere to established security standards, including maintaining the accuracy of the recording process. Therefore, a reliable technique of log verification is required to ensure data integrity and boost attack detection accuracy.

1) Efficient Data Collection

Diagnostic cluster is an optional feature defined by the ZigBee specification. Access to details regarding the ZigBee stack's performance over time is made possible by the diagnostic cluster. Installers and network administrators who research how specific devices function on a network will find this knowledge useful. Implementations of ZigBee diagnostic cluster nodes can report their network data to gateways and to the network management system, where performance and potential network faults may occur, via internet/cloud connectivity.

Counters on ZigBee nodes are used to implement ZigBee diagnostics. When a specific circumstance takes place, these counters are increased. For instance, when a ZigBee node receives a unicast message at the MAC layer, macRxUcast is increased. At predetermined intervals, the value of this counter is reported to a central node (such a gateway) and transmitted to the network management system. The gathered diagnostics can then be utilized to deduce network issues and find solutions. Examples of counters defined in a diagnostic cluster are shown in Table 1.

ZigBee diagnostic cluster served as an effective logging method for the researchers. The reporting mechanism that all devices utilize to routinely submit their observations to a centralized management system at the gateway or in the cloud is shown in Figure 6. Additionally, reports and data for all forms of attacks, including the identification of well-known attacks and systems for anomaly detection, were gathered using the diagnostic reporting system. The researchers used numerous new, non-standard diagnostic criteria that are helpful for detecting intrusions to give comprehensive attack detection. Table 2 provides a list of several possible diagnostic examples.

2) Trusted Data Collection

To debug ZigBee network operation and identify assaults on ZigBee systems, diagnostic data is employed. Some counter values could not have the intended values if an enemy tampers with the ZigBee system. Since it is believed that there are roughly the same numbers of unicast messages transmitted and received in a ZigBee network (with minor variations due to retransmissions and channel failures), it is reasonable to predict that the aggregated values of macRxUcast and macTxUcast will be proportionally linked. An sign that an adversary is injecting messages is when the number of unicast messages received suddenly exceeds the number of unicast messages transmitted, setting off the alarm.

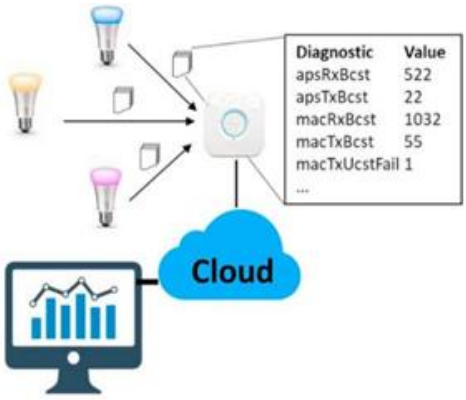

Figure 6. Diagnostic reporting system

TABLE 2
EXAMPLE OF PROPOSED DIAGNOSTIC FOR IDS

Proposed Diagnostics	Information	Utility
RxInterPANUcast	A counter that is incremented each time an InterPAN unicast message is received	To detect attacks relying on InterPAN messages, such as Touchlink Commissioning Attacks
RxInterPANBcast	A counter that is incremented each time an InterPAN broadcast message is received	To detect attacks relying on InterPAN messages, such as Touchlink Commissioning Attacks
RxTransportKey	A counter that is incremented each time a transport lock message is received	To detect fake key messages that can cause ZigBee devices to update their network keys (or other keys)

ZigBee diagnostic readings are not secure, which enables an opponent to mask his activities by falsifying the diagnostic values or altering those that the original node reported. In order to use diagnostic values for intrusion detection in a secure manner, this section suggests ways to ensure their integrity.

To address potential integrity issues in the reported diagnostic data, an intrusion monitor was included as a new IDS component. In order to identify inconsistent diagnostic data that point to network intrusion, the intrusion monitor modifies traffic to (suspected malicious) nodes. An alarm is raised in the event of an intrusion, and the security administrator can respond to it.

By taking part in the diagnostic reporting method, an adversary impersonating a legal node can avoid detection. Through the absence of diagnostic signals from that node, compromised nodes that do not participate in ZigBee diagnostic reporting can easily be identified. This technique addresses malicious nodes that engage in diagnostic reporting but behave differently from native nodes in the manner in which they report diagnostics. It is more likely to report an accurate value if it bases it on historical data or how it perceives the network.

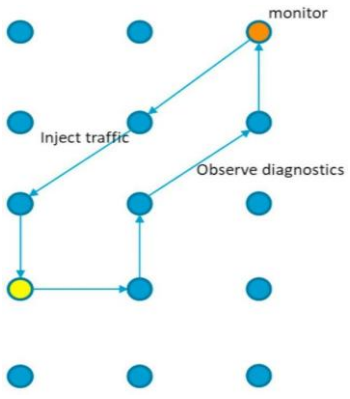

Figure 7. Overview of the Traffic Injection Mechanism

a) Traffic Adaptation

One method of collecting trusted data is to adapt traffic on networks with suspected malicious nodes and to monitor whether or not those nodes report diagnostic values in accordance with the traffic. There are three main ways to do this as follows.

- Observe whether counter updates are activated and reported back by nodes by injecting extra traffic into suspect nodes. The value of the NWKDe cryptionFailure counter, for instance, should rise if a message with a bad message integrity code (MIC) is injected. Nodes that do not increase this counter tend to not report diagnostics truthfully.
- Add more traffic to other nodes or network users but not to suspicious nodes. Other network users' diagnostic values ought to reflect this extra traffic, but not the diagnostics of any suspected malicious nodes.
- Reduce traffic to suspicious nodes and may instruct other nodes to do the same. The diagnostic data given by the alleged malicious nodes ought to reflect the decreased traffic.

The monitor verifies the diagnostic values reported by suspicious nodes and verifies whether or not the values are as expected. If there is a discrepancy, a warning is given. A high-level overview of the traffic injection technique is shown in Figure 7. In general, this traffic adaption technique can identify adversarial malicious reporting and validate the accuracy of diagnostic data supplied by authorized nodes.

b) Safe Diagnostics on Demand

Improving IDS security is recommended by providing an option to request diagnostics that are signed on demand. The monitor can ask nodes that have previously sent hazardous diagnostic readings for signed diagnostics, and subsequent values can be compared. If it receives conflicting diagnostic values, it may ask for signed diagnostics. As an additional step in the verification process, the monitor may also regularly request signed diagnostics. The device along (one of the paths) has modified the diagnostic value, and a warning is raised if the received signed value differs from the unsigned value.

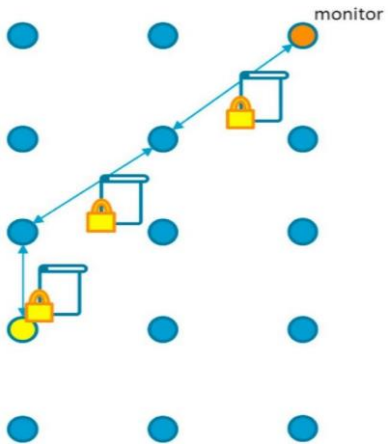

Figure 8. On-demand signed diagnostics

A high-level description of on-demand safe diagnostic techniques is shown in Figure 8. To guarantee the recency of the received signatures, the protocol adheres to a challenge response protocol. It is possible to symmetrically verify message integrity using a shared secret across monitors and nodes (like link keys in ZigBee) or asymmetrically using a signature scheme.

IV. CONCLUSION

This article has illustrated a number of approaches for spotting potential novel threats in ZigBee IoT systems. This article offers a hybrid approach to intrusion detection that combines machine learning-based anomaly detection with human-made rule-based detection.

The integrity and effectiveness of IDS data logging procedures are severely hampered by the widespread deployment of IoT equipment. This article discusses the use of data reporting mechanisms to increase the effectiveness of data gathering given the limitations of IoT devices as a solution to this problem. The researchers have suggested further strategies to strengthen the reporting mechanism's security. As a result, it can stop attacker nodes from altering data and fabricating reports that interfere with IDS's normal operation.

ACKNOWLEDGMENTS

The authors would like to thank all parties involved for the successful completion of this study. In particular, the authors would like to thank PJJ Informatics Engineering, University of Amikom 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*.