engineering proceedings

MDPI

Proceeding Paper

ZigBee Cyberattacks Simulation †

Marieta Haka *, Aydan Haka, Veneta Aleksieva and Hristo Valchanov

Faculty of Computer Sciences and Automation, Technical University of Varna, 9010 Varna, Bulgaria; aydin.mehmed@tu-varna.bg (A.H.); valeksieva@tu-varna.bg (V.A.); hristo@tu-varna.bg (H.V.)

* Correspondence: marieta.yordanova@tu-varna.bg

† Presented at the International Conference on Electronics, Engineering Physics and Earth Science (EEPES 2025), Alexandroupolis, Greece, 18–20 June 2025.

Abstract

ZigBee technology is well-known for wireless network communication and enables low-cost devices operating at low transmission speed and low power consumption in IoT networks. The technology is used for wireless networks through which a large amount of sensitive information passes, which requires ensuring a higher level of security. This creates a need to develop tools to analyze vulnerabilities in such networks. The massive occurrence of cyberattacks requires a more in-depth study to propose adequate and effective approaches for improving security in ZigBee networks. Such research can be performed both in real and simulated environments. In this paper, a new module is proposed for simulating Sniffing, Brute Force, and Dictionary attacks.

Keywords: Internet of Things; cyberattacks; ZigBee; simulation

check for updates

Academic Editor: Grigor Mihaylov

Published: 27 August 2025

Citation: Haka, M.; Haka, A.; Aleksieva, V.; Valchanov, H. ZigBee Cyberattacks Simulation. *Eng. Proc.* **2025**, *104*, 46. https://doi.org/10.3390/engproc2025104046

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The Internet of Things (IoT) represents a technological paradigm that facilitates connectivity among physical devices via networked communication, sensors, and automated analytics and control systems. Its significance is underscored by the increasing demand for intelligent solutions amid the digital transformation of various sectors, including industry, urban infrastructure, and healthcare. Projections indicate that the number of IoT devices will exceed 30 billion by 2030, thereby emphasizing the strategic importance of this technology for future socio-economic advancement [1,2].

Zigbee is recognized as one of the most widely utilized wireless technologies for resource-constrained IoT devices, particularly in applications such as home automation, renewable energy, and manufacturing. It provides reliable and energy-efficient communication. However, given that Zigbee networks transmit substantial amounts of sensitive information, there is a pressing need to ensure a heightened level of security. This necessity has prompted the development of tools aimed at analyzing vulnerabilities within these networks [3].

The prevalence of cyberattacks necessitates comprehensive research to formulate effective strategies for enhancing security in Zigbee networks. Such investigations can be conducted in both real and simulated environments. This paper introduces a novel module designed to simulate Sniffing, Brute Force, and Dictionary attacks.

2. Related Works

There are several simulation products that allow the exploration of ZigBee networks, each offering different features.

NS2 version 35 is a simulator that supports a variety of wireless medium access control protocols, including IEEE 802.11 and IEEE 802.15.4 (ZigBee) [4]. A battery consumption analysis is provided, along with control over the overhead of the physical layer of the ZigBee stack, as well as estimation of the MAC layer's network throughput. The simulator is capable of analyzing performance, network layer routing load, and ZigBee protocol reliability in IoT networks by a statistical model. It supports a range of features, including packet delivery ratios, routing protocols, Ad hoc On-Demand Distance Vector, end-to-end latency measurement, route discovery rate measurement, and route management [5].

The built-in tools of NS3 version 44 facilitate the real-time monitoring of key performance indicators for ZigBee networks [6]. The utilization of a simulator facilitates the emulation of attacks such as denial-of-service and spoofing [7]. To ensure reliable communication, NS3 also includes the capability to evaluate sensor nodes within wide-area low-power networks. Furthermore, it facilitates data transmission between a suitable gateway by tracking metrics such as the number of blocked packets, successfully received packets, and lost packets. This functionality renders it valuable for investigating the robustness and reliability of network layer communication in ZigBee networks [8].

Cooja version 5.0 can be utilized to simulate various routing algorithms and loopholes for hacker attacks, enabling an analysis of their impact [9,10]. The simulator is capable of simulating low-power ZigBee devices and evaluating energy-efficient protocols at the physical layer of the ZigBee stack. Additionally, Cooja is employed to simulate routing strategies at the application layer [9].

CupCarbon version 7.0 is developed for IoT network simulation within the context of smart cities [11]. The system incorporates capabilities for simulating automatic test sequence detection, in addition to the selection of witness nodes in scenarios where an adversary may endeavor to execute replication or cloning attacks on IoT devices. These capabilities are essential for security analysis and are integrated into the network layer of the ZigBee stack [12].

TOSSIM version 2.0 is a simulation environment that works with TinyOS, designed for small wireless sensor networks, enabling the observation of packet traffic [13]. The simulator is also an emulator, able to replicate both software and hardware elements for a specific model [14]. TOSSIM is mainly employed to observe traffic in the network layer of the ZigBee stack in wireless sensor networks. It provides a strong platform for analyzing packet transmission and facilitates the simulation of network bandwidth at the media access control layer [13].

EmStar version 1.0 is a simulation tool that offers a simple modeling environment and network structure for creating, constructing, and implementing diverse sensor network applications. It accommodates multiple popular communication protocols in wireless sensor networks, such as IEEE 802.15.4 and ZigBee. Moreover, it provides services like detection, message sending, and time synchronization in the network layer of the ZigBee stack [15].

Using SensorSim version 1.0, users can simulate IEEE 802.15.4 networks, which are low-power, low-speed wireless sensor networks compatible with protocols like ZigBee. Moreover, the simulator supports energy-efficient wireless sensor network protocols aimed at improving energy usage and prolonging network longevity, such as Low-Energy Adaptive Clustering Hierarchy, Threshold sensitive Energy Efficient sensor Network, and Power-Efficient Gathering in Sensor Information Systems. It additionally supports routing protocols like Ad hoc On-Demand Distance Vector, Destination-Sequenced Distance Vector, and Dynamic Source Routing [16].

OpNet version 18.11.1 facilitates the simulation of bandwidth at the media access control layer, hop count at the network layer, and end-to-end latency at the application

layer in the ZigBee framework. The simulator is suitable for various ZigBee network configurations, including star, tree, and mesh topologies [17].

The reviewed simulators facilitate the examination of various aspects related to the security of ZigBee networks. Those capable of simulating attacks enable the analysis of vulnerabilities within ZigBee networks and the testing of prevention methods. However, the limited number of predefined attack scenarios presents a significant drawback that these simulators must address [18].

Among the investigated simulators, only three allow simulation of cyberattacks. Although they all simulate different types of attacks, none allow simulation of Sniffing, Brute Force, or Dictionary attacks.

3. Cyberattacks on ZigBee Networks

The widespread use of IoT devices increases the risk of security threats within IoT networks. Prior to launching an attack, the perpetrator conducts an analysis of the network to identify vulnerabilities that can be exploited to compromise its security. The most common cyberattacks on IoT networks are [19]:

- Sniffing—malicious traffic interception enables attackers to collect sensitive information. By employing brute force and dictionary attacks, they can decrypt network traffic, leading to various security threats. Additionally, by executing a man-in-the-middle attack, they can manipulate network traffic [20].
- BotNet—network of compromised devices, referred to as bots, that are utilized to perform malicious actions. These devices are controlled by an attacker who employs various methods to infect additional devices, thereby expanding the BotNet. Such attacks can facilitate other cyberattacks due to their large scale and distributed nature [21,22].
- Distributed Denial of Service (DDoS)—DDoS attacks targeting IoT devices involve a large number of compromised devices that generate a substantial volume of traffic, overwhelming the communication infrastructure. Such an attack can disrupt the normal functioning of IoT devices [23].
- Brute Force—refers to the systematic testing of numerous passwords, logins, or encryption keys to gain unauthorized access. This method relies on the attacker attempting a wide array of combinations until the correct access credentials are discovered [24].
- Dictionary—involves attempting to use a set of potential combinations of passwords or keys to discover the actual one. Upon a successful attack, the attacker can gain unauthorized access to the network [25].
- Man-in-the-Middle—the covert capturing of data exchanged between two devices enables an attacker to manipulate the traffic before forwarding it to the intended recipient [26].
- Replay—the interception and retransmission of legitimate data transmissions by an attacker can mislead the recipient into performing unauthorized actions. An attacker executing this type of attack may induce unauthorized changes, such as unlocking smart locks and controlling smart home systems [27].

The most common attacks in ZigBee networks are Brute Force and Dictionary attacks. Brute Force attacks can target either the network or link keys, which are crucial for securing communication between devices. These keys are used to encrypt data exchanged at the network and application layers of the ZigBee stack. If a malicious attacker discloses these keys, it can result in unauthorized access to the ZigBee network. Dictionary attacks can be executed on a ZigBee network by utilizing a pre-prepared set of random 128-bit keys to uncover the actual network key [28].

The widespread occurrence of these attacks necessitates a thorough analysis of vulnerabilities and network behavior during such incidents to develop more effective security strategies for ZigBee networks.

4. Cyberattack Simulation Module

The purpose of this paper is to develop a tool for analyzing the behavior of ZigBee networks in response to some of the most common attacks on these networks, as well as to measure the execution time of these attacks. To achieve this, a new simulation module has been created for a simulator developed by the authors, which enables the simulation of Sniffing, Brute Force, and Dictionary attacks [29].

The developed simulation module makes it possible to visualize several cyberattacks that can be carried out in a real environment in a ZigBee network. The simulation of capturing the communication in the medium presents information about the time of interception of the message (Figure 1(1)), source (Figure 1(2)), destination (Figure 1(3)), communication protocol (Figure 1(4)), additional information (Figure 1(5)), and transmitted data (Figure 1(6)).

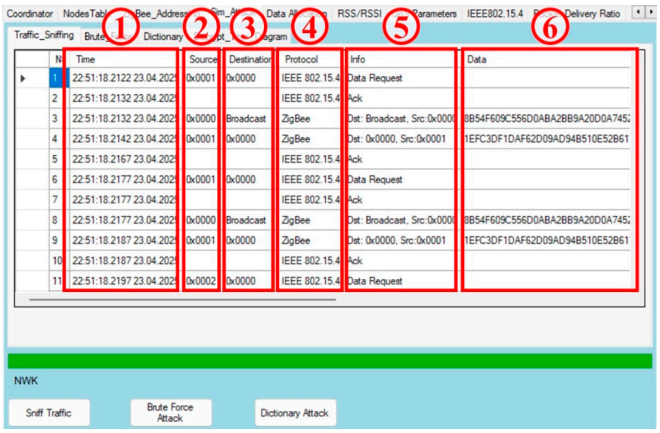


Figure 1. Execution of sniffing attack.

The simulation of Brute Force cyberattacks provides results for the number of cyberattack attempts (Figure 2(1)), the execution time (Figure 2(2)), and information about whether the cyberattack was successful or unsuccessful (Figure 2(3)).

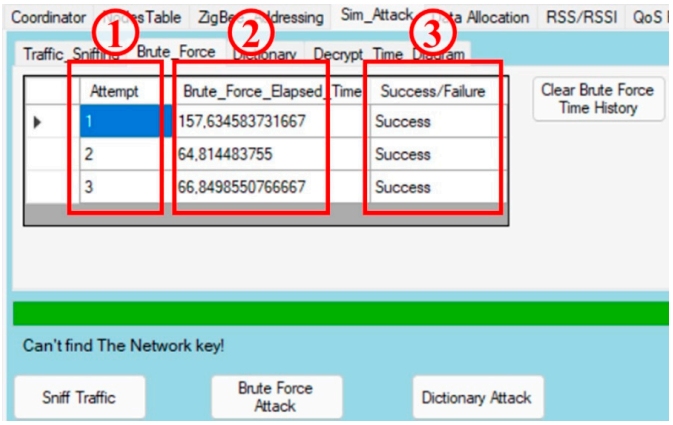


Figure 2. Execution of Brute Force attack.

The simulation of the Dictionary attack makes it possible to create a dictionary of the possible combinations that are searched for (Figure 3(1)), and their number can be defined by the user (Figure 3(2)). It provides information about the number of attempted cyberattacks

(Figure 3(3)), the size of the dictionary (Figure 3(4)), the execution time (Figure 3(5)), and information about whether the cyberattack was successful or unsuccessful (Figure 3(6)).

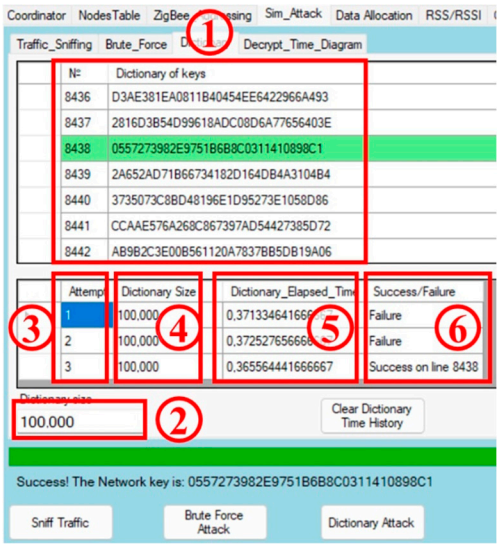


Figure 3. Execution of Dictionary attack.

The results of the cyberattacks performed are presented in a diagram that reflects the decryption time of the respective attempts in minutes (Figure 4).

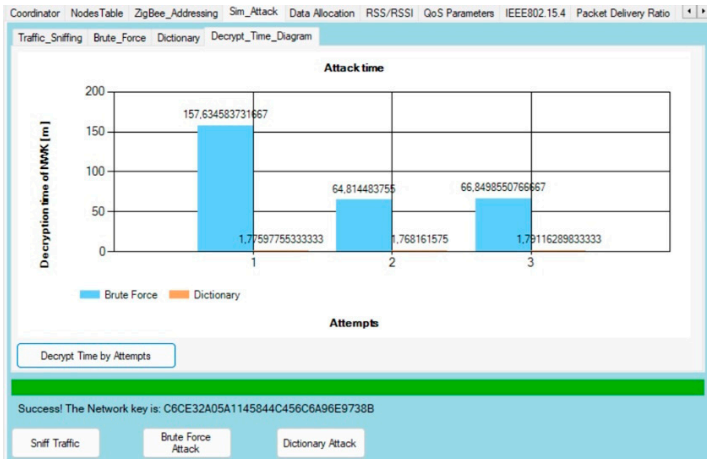


Figure 4. Result of the executed cyberattacks.

The ability to simulate cyberattacks in the ZigBee simulator developed by the authors makes it possible to analyze the time for decryption of communication in the ZigBee network in Brute Force and Dictionary cyberattacks. This makes it possible to define appropriate approaches to improve security in ZigBee networks. It also provides an appropriate environment for a visual presentation of the action of the cyberattacks in question, which is especially important for use in education.

5. Experimental Research and Results

Experimental studies are carried out on an HP ProBook 450 G6 computer system, Intel Core i5-82655U CPU@ 1.60 GHz 1.8 GHz, 8GB, System type 64-bit OS, x64-based processor, Windows 11 Enterprise. A ZigBee network with one coordinator and eight end devices connected in a Star topology is simulated (Figure 5).

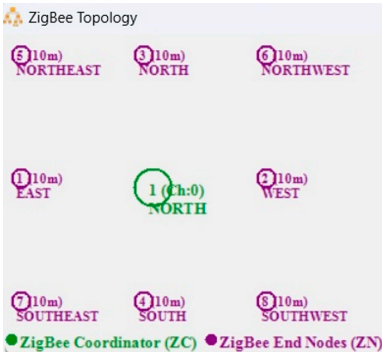


Figure 5. Simulated topology of connected ZigBee devices.

The purpose of the experiment is to present a simulation of network traffic capturing that is transmitted over the wireless channel between end devices and the coordinator, as well as its decryption. Traffic capture simulation occurs after all end devices are connected to the coordinator's network. When devices are authenticated and connected to the network, they receive a key that encrypts communication at the network layer of the ZigBee stack, known as a Network Key (NWK). Encryption of communication on this layer is the mandatory protection defined by the ZigBee standard [30]. The NWK that is used to encrypt communication is generated by the network coordinator and provided to a legitimized device. The size of this key is 128-bit and is represented in hexadecimal form, being used to encrypt communication with AES 128. When starting the Sniffing simulation, the capture of the exchanged messages between the coordinator and end devices is simulated, and the data part transmitted at the network layer of the ZigBee stack is presented in encrypted form (Figure 6). To decrypt this information, it is necessary for the attacker to obtain an NWK. When network layer communication is decrypted, the attacker can monitor what data is transmitted between devices, as well as use the detected NWK to present as a legitimate device on the ZigBee network and send modified messages.

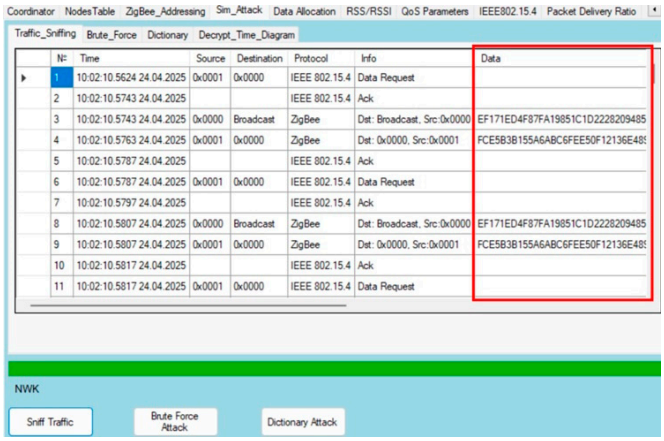


Figure 6. Simulation of captured encrypted traffic.

The simulator presents NWK detection with simulation of Brute Force and Dictionary attacks. As a result of the execution of these attacks, information is recorded about the time in minutes required to detect the NWK (Figures 7 and 8(3)), which decrypts the data part of the intercepted traffic (Figure 9). When performing cyberattacks, three attempts were made to track the difference in decryption time for the two types of attacks and between different attempts for the same attack. In the Brute Force attack, all possible combinations of NWK are traversed to decrypt the traffic, and in the Dictionary cyberattack, the size of the

dictionary is defined (Figure 8(1)), which is filled with various possible NWKs (Figure 8(2)) and then the correct key that will decrypt the traffic is searched.

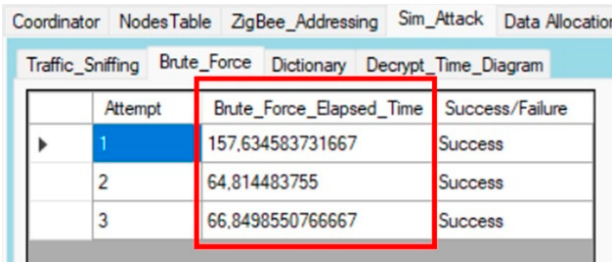


Figure 7. NWK Detection with Brute Force Cyberattack.

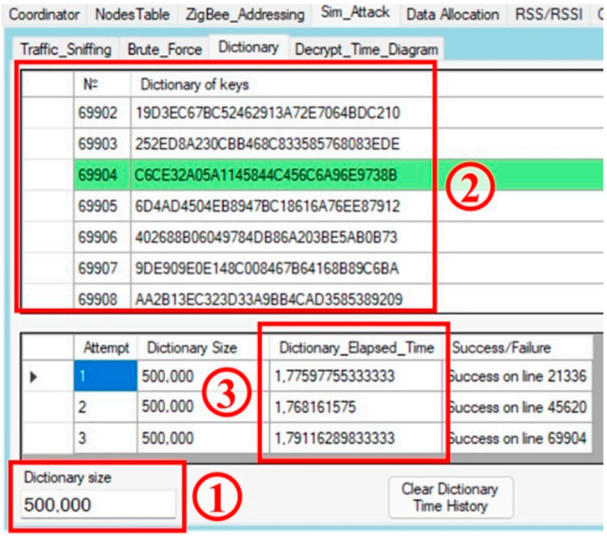


Figure 8. NWK Detection with Dictionary Cyberattack.

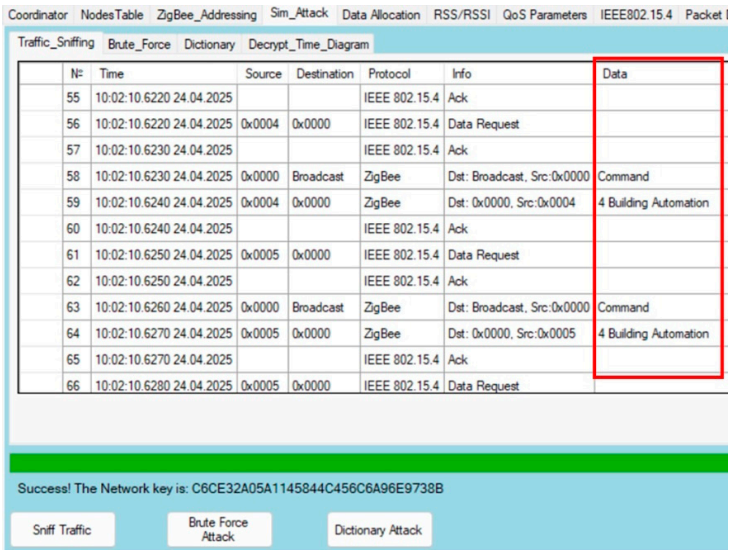


Figure 9. Decrypted data part.

The experimental results obtained (Figure 10) show that the Brute Force cyberattack guarantees that the sought Network Key will be discovered, but this happens slowly, while the Dictionary cyberattack is likely to fail to discover the correct key. The difference in the times of searching for the correct Network Key between the two cyberattacks is large,

with an average of 96.43 min for Brute Force and an average of 1.78 min for Dictionary. Despite the probability of failure, the Dictionary cyberattack is executed much faster than Brute Force and provides an equally high possibility of discovering the key. The presented research gives rise to the claim that new methods and approaches are needed to improve security in ZigBee networks that are resistant to Brute Force and Dictionary cyberattacks.

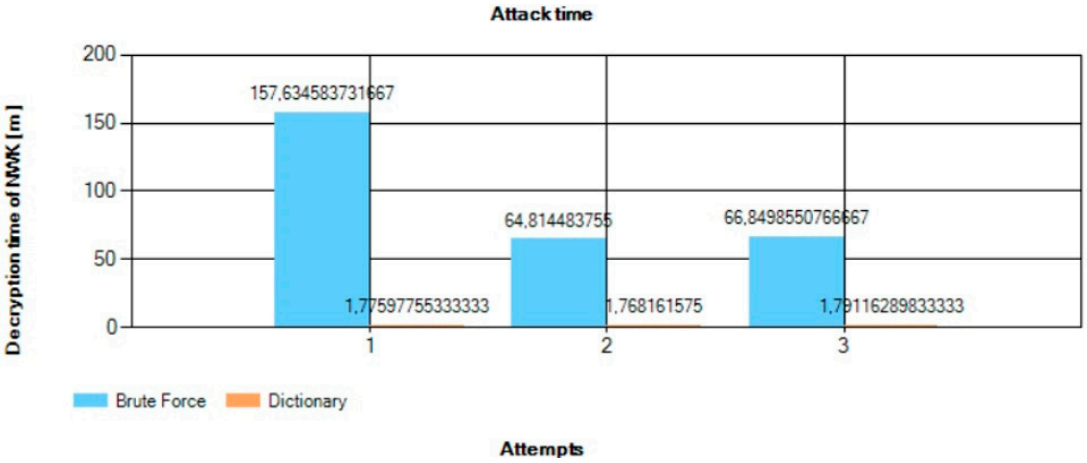


Figure 10. Decryption time of NWK for Brute Force and Dictionary attacks.

6. Conclusions

In this paper a new module is proposed for simulating Sniffing, Brute Force, and Dictionary attacks. The proposed module enables the simulation of attacks, facilitating the analysis of vulnerabilities in ZigBee networks. This capability allows for the development of more robust strategies to enhance security within these networks.

The simulation module allows monitoring of the NWK decryption time. It is found that the key decryption time when a Brute Force attack is executed is longer because it checks all possible combinations. This guarantees greater success of the attack. When a Dictionary attack is executed, the key decryption time is shorter because the possible keys are predefined. However, the attack does not guarantee success because it does not check for all possible combinations. This functionality allows for in-depth research into the vulnerability of ZigBee networks in terms of NWK decryption time. Additionally, the simulation module offers an opportunity to demonstrate the nature and tactics of attacks during education.

This research will be used as a basis for developing new approaches and methods to improve security in future work.

Author Contributions: Conceptualization, M.H., A.H. and V.A.; methodology, M.H., A.H. and V.A.; software, A.H.; validation, A.H. and M.H.; investigation, M.H., A.H., V.A. and H.V.; data curation, M.H., A.H., V.A. and H.V.; writing—original draft preparation, M.H.; writing—review and editing, A.H., V.A. and H.V.; visualization, M.H. and A.H. All authors have read and agreed to the published version of the manuscript.

Funding: The scientific research, the results of which are presented in this paper, was carried out under project NP3 within the framework of the scientific research activity inherent to TU-Varna, funded by the state budget.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are available upon reasonable request to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Auhl, Z.; Moraliyage, H.; Chilamkurti, N.; Alahakoon, D. RACER: A Lightweight Distributed Consensus Algorithm for the IoT with Peer-Assisted Latency-Aware Traffic Optimisation. *Technologies* **2025**, *13*, 151. [CrossRef]
2. Stoyanov, I.S.; Iliev, T.B.; Mihaylov, G.Y.; Evstatiev, B.I.; Sokolov, S.A. Analysis of the Cybersecurity Threats in Smart Grid University of Telecommunications and Post, Sofia, Bulgaria. In Proceedings of the International Symposium for Design and Technology in Electronic Packaging (SIITME), Iasi, Romania, 25–28 October 2018. [CrossRef]
3. Li, J.; Wang, S.; Xu, Z.; Xi, W.; Wang, S.; Gong, W. EchScatter: Enriching Codeword Translation for High-Throughput Ambient ZigBee Backscatter. *ACM Trans. Sens. Netw.* **2025**, *21*, 1–21. [CrossRef]
4. Network Simulator Projects. Network Simulator 2 (NS2). Available online: https://networksimulator2.com (accessed on 25 July 2024).
5. Sandeep; Vasaya, N.; Smera, C.; Kirubanand, V.B.; Balamurugan, E. Simulation model of ZigBee network to analyze routing protocols for the sustainable Healthcare environment. *NeuroQuantology* **2022**, *20*, 1471–1479.
6. Ns3 Projects. Ns 3 Simulations, Zigbee Simulation. Available online: https://ns3simulation.com/zigbee-simulation/ (accessed on 25 July 2024).
7. Fang, X.; Zheng, L.; Fang, X.; Chen, W.; Fang, K.; Yin, L.; Zhu, H. Pioneering advanced security solutions for reinforcement learning-based adaptive key rotation in Zigbee networks. *Sci. Rep.* **2024**, *14*, 13931. [CrossRef]
8. Cheimaras, V.; Peladarinos, N.; Monios, N.; Daousis, S.; Papagiakoumos, S.; Papageorgas, P.; Piromalis, D. Emergency Communication System Based on Wireless LPWAN and SD-WAN Technologies: A Hybrid Approach. *Signals* **2023**, *4*, 315–336. [CrossRef]
9. Zhi, H.; He, Y.; Tian, Z.; Xin, P. Wireless Mesh System Design for Photovoltaic Power Station Based on LoRa. In Proceedings of the 2023 International Conference on Frontiers of Artificial Intelligence and Machine Learning, Beijing, China, 14–16 April 2023; pp. 70–74.
10. Chowdhury, M.; Ray, B.; Chowdhury, S.; Rajasegarar, S. A novel insider attack and machine learning based detection for the internet of things. *ACM Trans. Internet Things* **2021**, *2*, 1–23. [CrossRef]
11. Adday, G.; Subramaniam, S.; Zukarnain, Z.; Samian, N. Investigating and Analyzing Simulation Tools of Wireless Sensor Networks: A Comprehensive Survey. *IEEE Access* **2024**, *12*, 22938–22977. [CrossRef]
12. Mbarek, B.; Soula, M.; Pitner, T.; Meddeb, A. An Effective Replica Node Detection Scheme in Internet of Things Networks. In Proceedings of the 2023 International Wireless Communications and Mobile Computing, Marrakesh, Morocco, 19–23 June 2023; pp. 608–613. [CrossRef]
13. TinyOS. Available online: https://github.com/tinyos (accessed on 4 September 2024).
14. Yigit, Y.; Dagdeviren, O.; Challenger, M. Self-Stabilizing Capacitated Vertex Cover Algorithms for Internet-of-Things-Enabled Wireless Sensor Networks. *Sensors* **2022**, *22*, 3774. [CrossRef] [PubMed]
15. Chen, G.; Dong, W.; Qiu, F.; Guan, G.; Gao, Y.; Zeng, S. Scalable and interactive simulation for IoT applications with TinySim. *IEEE Internet Things J.* **2023**, *10*, 20984–20999. [CrossRef]
16. Pellenz, M.E.; Lachowski, R.; Jamhour, E.; Brante, G.; Moritz, G.L.; Souza, R.D. In-network data aggregation for information-centric WSNs using unsupervised machine learning techniques. In Proceedings of the 2021 IEEE Symposium on Computers and Communications (ISCC), Athens, Greece, 5–8 September 2021; pp. 1–7. [CrossRef]
17. Zhou, T.; Yang, C.; Chen, H.; Han, Y.; Bao, W.; Cheng, Q. Performance research on ZigBee wireless sensor network self-organizing network for 220 kV four-circuit transmission lines on the same tower. *Sustain. Energy Technol. Assess.* **2022**, *53*, 102302. [CrossRef]
18. Almutairi, R.; Bergami, G.; Morgan, G. Advancements and Challenges in IoT Simulators: A Comprehensive Review. *Sensors* **2024**, *24*, 1511. [CrossRef]
19. Kebande, V.R.; Awad, A.I. Industrial internet of things ecosystems security and digital forensics: Achievements, open challenges, and future directions. *ACM Comput. Surv.* **2024**, *56*, 1–37. [CrossRef]
20. Jin, H.; Jeon, G.; Choi, H.W.A.; Jeon, S.; Seo, J.T. A threat modeling framework for IoT-Based botnet attacks. *Heliyon* **2024**, *10*, e39192. [CrossRef]
21. Lefoane, M.; Ghafir, I.; Kabir, S.; Awan, I.U. Internet of Things botnets: A survey on Artificial Intelligence based detection techniques. *J. Netw. Comput. Appl.* **2025**, *236*, 104110. [CrossRef]
22. Kornyo, O.; Asante, M.; Opoku, R.; Owusu-Agyemang, K.; Partey, B.T.; Baah, E.K.; Boadu, N. Botnet attacks classification in AMI networks with recursive feature elimination (RFE) and machine learning algorithms. *Comput. Secur.* **2023**, *135*, 103456. [CrossRef]
23. Kumari, P.; Jain, A.K. A comprehensive study of DDoS attacks over IoT network and their countermeasures. *Comput. Secur.* **2023**, *127*, 103096. [CrossRef]
24. Pourrahmani, H.; Yavarinasab, A.; Monazzah, A.M.H. A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain. *Internet Things* **2023**, *23*, 100888. [CrossRef]
25. Bala, B.; Behal, S. AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges. *Comput. Sci. Rev.* **2024**, *52*, 100631. [CrossRef]

26. Upadhyay, D.; Ghosh, S.; Ohno, H.; Zaman, M.; Sampalli, S. Securing industrial control systems: Developing a SCADA/IoT test bench and evaluating lightweight cipher performance on hardware simulator. *Int. J. Crit. Infrastruct. Prot.* **2024**, *47*, 100705. [CrossRef]
27. Wang, Z.; Sun, C. LICAPA: Lightweight collective attestation for physical attacks detection in highly dynamic networks. *Pervasive Mob. Comput.* **2024**, *99*, 101903. [CrossRef]
28. Neto, E.C.P.; Dadkhah, S.; Ferreira, R.; Zohourian, A.; Lu, R.; Ghorbani, A.A. CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment. *Sensors* **2023**, *23*, 5941. [CrossRef] [PubMed]
29. Yordanova, M.; Haka, A.; Aleksieva, V.; Valchanov, H. Enhanced Simulation Tool for ZigBee Security. In Proceedings of the 2024 5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES), Veliko Tarnovo, Bulgaria, 20–22 November 2024; pp. 1–7. [CrossRef]
30. Connectivity Standards Alliance. Zigbee Specification, Revision 23, 15 March 2023. Available online: https://csa-iot.org/all-solutions/zigbee/ (accessed on 24 April 2025).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.