A statistical method for real-time intrusion detection and response in ZigBee networks⋆

Mykola Stetsiuk [1,*,†], Yurii Klots [1,†], Victor Cheshun [1,†], and Abdel-Badeeh M. Salem[2,†]

[1] *Khmelnytskyi National University, Khmelnytskyi, Instytutska street 11, 29016, Ukraine*
[2] *Ain Shams University, El-Khalyfa El-Mamoun Street Abbasya, Cairo, Egypt*

Abstract

This paper presents an integrated, resource-conscious framework for detecting and mitigating security threats in ZigBee-based IoT networks. The proposed solution combines a graph-oriented description of network topology with a formal attack model and a purely statistical anomaly-detection engine. Normal behaviour for every node is profiled on-line with a modified Z-score that relies on the median and median-absolute deviation, making the detector robust to noise, outliers and bursty traffic. Anomalous events—those that exceed statistically justified limits—are enriched with contextual attributes (device ID, parameter type, duration, weight) and matched against a library of formalised attack templates. When a match is confirmed, a response selector estimates potential damage by factoring impact intensity and node criticality, then triggers the least-cost counter-measure: node isolation, route restructuring, key rotation or channel switching. All stages—monitoring, classification, reaction and post-action verification—operate in a closed loop and require no prior training on labelled data, which is crucial for low-power ZigBee devices.

A prototype was validated with three representative threats (DoS, Spoofing, Jamming). The system accurately identified each attack phase, initiated the correct counter-action within two seconds and automatically logged the incident for audit purposes. Because the framework is statistical and lightweight, it adapts readily to heterogeneous hardware and dynamic traffic patterns. Future work will extend the feature set and benchmark hybrid statistical–learning schemes to further strengthen the resilience of large-scale IoT deployments.

Keywords

IoT security, anomaly detection, network traffic analysis, machine learning, Autoencoder, intrusion detection, cybersecurity threats.

1. Introduction

Drill-free, low-impact security measures have progressed from niche solutions to broadly adopted technologies underpinning intelligent alarm systems, automated controls, and industrial sensing networks. Within this landscape, the ZigBee protocol has assumed a prominent position. It enables self-healing mesh topologies, operates with very low energy consumption, and accommodates large device populations. However, its use of publicly accessible radio bands, shared node resources, and default cryptographic material (including standard keys) renders ZigBee vulnerable to a variety of attacks, ranging from traffic redirection to coordinator impersonation and rogue-network reconstruction.

ICyberPhyS'25: 2nd International Workshop on Intelligent & CyberPhysical Systems, July 04, 2025, Khmelnytskyi, Ukraine
[1]* Corresponding author.
† These authors contributed equally.
mykola.stetsiuk@khmnu.edu.ua (M. Stetsyuk); klots@khmnu.edu.ua(Y. Klots); cheshunvn@khmnu.edu.ua (V. Cheshun); abmsalem@yahoo.com (Abdel-Badeeh M. Salem)
0000-0003-3875-0416 (M. Stetsyuk); 0000-0002-3914-0989 (Y. Klots); 0009-0002-6485-4462; (V. Cheshun); 0000-0002-3935-2068;); 0000-0003-0268- 6539 (Abdel-Badeeh M. Salem);

The growing incidence of such attacks in both domestic and commercial environments demonstrates that mere detection of anomalous activity is insufficient. A critical performance metric is response latency—the interval between threat emergence and its localization and neutralization. Meeting this criterion demands dynamic defence mechanisms that integrate statistical anomaly detection, adaptive topology management, and automated countermeasures. Consequently, a systematic appraisal of contemporary ZigBee-focused protection strategies is warranted. Such an assessment should identify their respective strengths and limitations and highlight avenues for future advancement.

2. Classification of attacks on the ZigBee network

Security threats in ZigBee-based Internet of Things systems can be divided into two main categories: implementation-level vulnerabilities and architectural protocol weaknesses.

Implementation-level vulnerabilities include insecure key storage, plaintext transmission during device onboarding, and misconfigured access policies. For example, CVE-2015-3974 and CVE-2020-6007 allowed attackers to extract cryptographic keys from device memory or intercept them in unencrypted form.

Architectural protocol weaknesses involve the use of static default keys (e.g., CVE-2019-18984), acceptance of unsolicited ACK packets, and limitations in the CSMA/CA channel access mechanism, which open up opportunities for jamming and medium-saturation attacks.

Based on the scope of impact, attacks can be classified as local, targeting individual nodes or links (e.g., DoS, spoofing), or systemic, affecting network topology or coordinator integrity.

Table 1 summarizes the main types of threats, their typical causes, target elements, and potential consequences.

Table1

Classification of threats in ZigBee networks

Category	Typical issue	Attack examples	Target elements	Potential impact
Implementation-level	Key leakage, weak configuration	CVE-2015-3974, CVE-2020-6007	End devices, gateways	Unauthorized access, instability
Protocol-level	Static keys, ACK handling, CSMA/CA flaws	CVE-2019-18984, jamming	Channels, routers	Connectivity loss, routing disruption
Local attacks	Flooding, spoofing	DoS, identifier replay	Individual node or link	Temporary service degradation
Systemic attacks	Coordinator hijacking, route poisoning	MITM, impersonation	Coordinator, network topology	Structural degradation, global instability

This classification enables a unified understanding of threat types and serves as a foundation for the formal attack model and response mechanisms described in the next section.

3. Overview of detection and protection methods

Signature-based intrusion-detection systems (IDSs) operate by matching observed traffic against a database of known attack patterns. They typically exhibit the lowest false-positive rates and provide rapid responses to well-documented threats; however, they cannot recognise novel or obfuscated attacks and demand continual signature updates. Sadikin and Kumar [1] mitigate these limitations through a hybrid scheme that augments signature matching with a rule-based component.

Rule-based IDSs rely on deterministic heuristics or statistical thresholds to flag anomalies. They require neither training nor significant computational resources, which is advantageous for ZigBee

deployments. Techniques founded on the modified Z-score, CUSUM, and entropy analysis can detect deviations from normal behaviour in near real time. A recent survey confirms that such rule-based approaches remain competitive despite the growing popularity of machine-learning methods.

Autoencoder-based IDSs constitute a class of machine-learning models that identify anomalies by reconstructing input data and measuring reconstruction error. Lightweight autoencoder architectures achieve detection accuracies above 95 % in resource-constrained IoT environments [2-7], enabling multi-class classification with minimal changes to network infrastructure.

Reference [8] proposes a convolutional neural network (CNN) combined with a long short-term memory (LSTM) layer, thereby capturing both spatial and temporal dependencies in traffic flows. The resulting IDS detects complex, multi-stage attack patterns and is particularly suitable for smart-home scenarios, where device interactions exhibit regular structure. The approach delivers high accuracy but entails notable computational overhead and requires extensive offline training.

Federated-learning (FL) frameworks, exemplified by FLAD, aggregate locally trained models without transmitting raw data, thus preserving privacy. Reference [8] demonstrates FL-based IDSs that maintain inter-node model compatibility without a central server. Principal challenges include inter-device synchronisation and maintaining model relevance across heterogeneous nodes.

Reinforcement learning (RL) employs an agent that interacts with its environment and iteratively refines its policy via reward feedback. Reference [6] applies RL to ZigBee key-rotation management, yielding adaptive responses to evolving threat levels. Although RL can generate dynamic security policies, it requires numerous training episodes, which limits feasibility on edge devices lacking simulation support.

Challenge–response protocols enable authentication without disclosing secret credentials. Reference [9-12] presents a lightweight ZigBee-oriented protocol that thwarts replay and node-substitution attacks. Its computational footprint suits simple sensors, yet authentication introduces latency and necessitates time synchronisation.

Ensemble-based classifiers combine outputs from multiple base learners (e.g., random forest, support-vector machine) to enhance robustness. Experiments in [8] show that ensembles reduce false positives and adapt more readily to emerging attack patterns, albeit at the cost of additional processing complexity.

The Phy-MAC-NWK framework [13] performs multi-layer traffic analysis, simultaneously examining physical, MAC, and network-layer parameters. This holistic perspective uncovers attacks that camouflage themselves at one layer but leave artefacts elsewhere. Its effectiveness is offset by implementation complexity and the need for fine-grained access to the ZigBee stack.

Z-Fuzzer [14] subjects ZigBee implementations to malformed and boundary-value inputs, exposing vulnerabilities prior to deployment. Although indispensable for security audits, it is unsuitable for real-time detection and may induce temporary instability during testing.

Reference [15] employs wavelet transforms to examine low-level radio signals, enabling the detection of physical-layer attacks such as jamming. The method is sensitive to subtle anomalies beyond the reach of conventional metrics but is computationally expensive and highly dependent on filter configuration.

Finally, the authors of [16] present an anomaly detector that leverages the structure of MQTT topic graphs, demonstrating its efficacy in identifying atypical communication patterns within ZigBee-enabled IoT systems.

4. Abstract model of a method for countering attacks in a ZigBee network

An analysis of attacks on wireless IoT networks—ZigBee in particular—reveals a steady increase in both the complexity and variability of malicious techniques designed to destabilise the network or seize control of its operation.

Building on classical intrusion models, we have developed an adapted framework that captures the full attack chain for ZigBee infrastructures. Similar to traditional compromise scenarios that

exploit human error, network weaknesses, or device-level vulnerabilities, ZigBee-focused attacks frequently proceed through multi-stage actions directed at individual end devices, routers, communication links, or the network coordinator [17].

Within this framework, the threat actor delivers a crafted impact against a selected segment of the ZigBee infrastructure. The vector may involve direct compromise of the coordinator or a router, interception of the communication channel, or impersonation of an end node. Resulting effects include disrupted routing, loss of connectivity, topological changes, exhaustion of nodes or channels, and the suspension of critical functions.

The model distinguishes local attacks—those limited to a small subset of nodes (e.g., denial-of-service, spoofing, flooding)—from global attacks that reshape the topology or trigger cascading failures. Figure X (below) illustrates the adapted penetration model for ZigBee, developed by analogy with the canonical intrusion pathway for conventional computer systems [18,19].

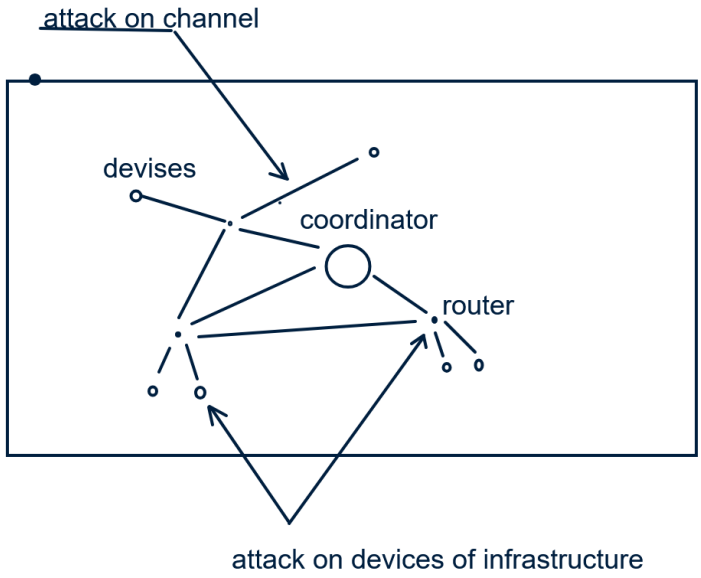

Figure 1: Generalized scheme of attacks on ZigBee network infrastructure.

To ensure the ZigBee network's resilience to attacks during operation, we propose formalising the network as a coordinated ensemble of logically related components, each of which fulfils a specialised role in the IoT system's overall mission. This approach not only permits a formal description of the behaviour of network elements under normal conditions, but also enables the specification of scenarios in which the network's integrity is compromised by deliberate external actions. By modelling the ZigBee network as a functionally distributed system, we define its structure as the following set:

$$M_{zb} = \{C, D, R, Z, F_{zb}, A_{zb}\} \quad (1)$$

Where $C = \{ch_1, ch_2, \dots, ch_n\}$ – – a set of communication channels that implement physical or logical routing between nodes, $D = \{d_1, d_2, \dots, d_n\}$ – a plurality of terminal devices that collect, or generate, or receive data; $R = \{r_1, r_2, \dots, r_n\}$ – a set of routers responsible for relaying, building and maintaining the route; $Z = \{z\}$ – network coordinator, the central element of network management and initialization; $F_{zb} = \{f_0, f_1, \dots, f_n\}$– a set of functional roles and services that ensure the operation of the ZigBee network: addressing management, routing, protection, synchronization; $A_{zb} = \{a_0, a_1, \dots, a_n\}$ – a set of activation conditions that determine the dependence of the operation of elements on events, requests, or topology changes.

Given that a ZigBee network is usually geographically or logically distributed, and its components can be located on different physical devices or in different spatial zones, each component of the

model will be represented as a combination of components of the corresponding subnetworks (or groups of nodes), which operate autonomously, but perform functions within the general infrastructure:

$$M_{zb} = \begin{cases} C = U_{i=1}^{N} C_i \\ D = U_{i=1}^{N} D_i \\ R = U_{i=1}^{N} R_i \\ Z = U_{i=1}^{N} Z_i \\ F_{zb} = U_{i=1}^{N} F_{zb,i} \\ A_{zb} = U_{i=1}^{N} A_{zb,i} \end{cases} \quad (2)$$

where N is the number of fragments or logical segments of the ZigBee network (e.g., rooms, clusters, floors, control zones) that operate with partial autonomy. Each subset of components C_i, D_i, R_i, Z_i may have different criticality, fault tolerance and degree of impact on the overall integrity of the network. For this purpose, a weighting characteristic is introduced for each type of element:

$$W_{zb} = \{(C, \omega_c), (D, \omega_d), (R, \omega_r), (Z, \omega_z)\} \quad (3)$$

Where $\omega_c \in [0,1]$ – weight coefficient reflecting the importance of the type of components in the overall structure of the network; $\omega_c \approx 1.0$ – the coordinator is a critical point of failure; $\omega_r \in [0.7; 0.9]$ – routers are of high importance for topology stability; $\omega_c \in [0.5; 0.8]$ – channels are vulnerable to intentional overloading; $\omega_r \in [0.2; 0.4]$ – end devices have local impact

To build an effective system for detecting and countering attacks in ZigBee networks, it is necessary to formally describe malicious influences as a set of parameters that characterize the nature of the attack, its time dynamics, scope, and consequences for the integrity of the infrastructure. In general, the attack $A_i$can be represented as a five-component structure:

$$A_i = (T_i, S_i, \phi_i(t), \psi_i, \delta_i) \quad (4)$$

Where $T_i \in T$ — type of attack (e.g., DoS, spoofing, MITM, jamming); $S_i \subseteq V \cup E$ — the target subset of network elements (nodes or links) on which the influence is directed; $\phi_i(t)$: $R^+ \to [0,1]$ — the attack intensity function over time, which describes the evolution of the threat; $\psi_i(\upsilon)$ damage function, which determines whether the component will fail at time t depending on the impact force and the resistance threshold θ_υ

$$\psi_i(\upsilon) = \begin{cases} 1 \ \phi_i > \theta_\upsilon \text{ та } \upsilon \in S_i \\ 0, \ else \end{cases} \quad (5)$$

$\delta_i(\upsilon) = W(\upsilon)\psi_i(\upsilon)$ — assessment of the criticality of the consequences for each element, taking into account its weight in the network structure. The total impact of an attack on the infrastructure at time t can be expressed as:

$$\Delta_i(t) = \sum_{\upsilon \in V} \delta_i(\upsilon) \quad (6)$$

This value allows you to calculate the degree of degradation of the network operation caused by a specific attack scenario. Depending on the goal, attacks can be destructive (destruction of elements, channel overload, router blocking) or passive (interception, substitution, eavesdropping) and be directed at components with different criticality: communication channels C, end devices D, routers R or coordinators K.

This formalized approach allows you to unify the description of attacks, provide their analysis in dynamics and determine which network elements are most vulnerable to specific types of influences. Such a model is also the basis for the further construction of reactive or adaptive protection mechanisms [20].

The next step is to adapt the anomaly detection method to the conditions of the network model, taking into account typical attacks and their expected dynamics. If the original Modified Z-score method allows us to determine deviations of parameters from the norm in a general way, then for the needs of the protection system we modify it so that each recorded anomaly can be compared with a specific attack scenario.

This is achieved by introducing additional attributes to each anomalyThis is achieved by introducing additional attributes to each anomaly: spatial localization (device identifier υ_i); functional context (the type of parameter ρ_i is related to the impact of the attack), time duration τ_i as an analogue of the integral force of influence, the weight of the parameter μ_i to take into account the criticality of the deviation, The interaction is described by the correspondence condition:

$$\alpha_j \to A_j \Leftrightarrow \begin{cases} \upsilon_j \in S_i \\ \rho_i \sim T_i \\ d_j > \theta_{\upsilon j} \\ \tau_i > \tau_{\min} \end{cases} \quad (7)$$

υ_j — the device affected by the anomaly, T_i— type of attack corresponding to the nature of the parameter ρ_i, d_j — deviation threshold for the device, $\tau_{\min}$ — minimum significant duration of the anomaly

Thus, α_j is interpreted as the implementation of A_j if this system of conditions is met. This allows us to integrate signal observations into a formal model of malicious influence and proceed to decision-making in the protection system [21].

After detecting an anomaly and comparing it with the formalized attack model, the next stage is necessary - making decisions on response in order to minimize the consequences and prevent the escalation of the impact on the network. Response is implemented as a functional transition of the current state of the network to a new one, in which the attack effect is weakened or neutralized.

Formally, each counteraction is defined as a function:

$$R_k = : Z(t) \to Z`(t + \delta t) \quad (8)$$

Where $Z(t)$ is the current structural state of the network, and δt is the reaction implementation time. The result is a new state Z^` with reduced attack impact.

Table 2.

Quantification of detected anomalies in IoT device traffic

Reaction R_k	The essence of the action	Activation condition
R_1 Node isolation	Physical or logical disconnection of node v from the topology	$\psi_i(\upsilon) = 1 \wedge \delta_i(\upsilon) > 0.6$
R_2 Rerouting	Building an alternative route to the coordinator	$\upsilon \in R \wedge F(\upsilon) = 0 \wedge W(\upsilon) > 0.7$
R_3 Key rotation	Replacing cryptographic keys in a local cluster	$T_i \in \{\text{spoofing}, \text{key exposure}\}$
R_4 Changing the channel	Switching to another logical or physical communication channel	$v \in C = \wedge d_j(t) > \theta_{\upsilon j} \wedge \mu_o > 0.5$
R_5 Traffic filtering	Restricting/blocking suspicious packets	$T_i = DoS \wedge \tau_j > \tau_{min}$
R_6 Notification	Signal transmission to the monitoring center or administrator	$\Delta(t) > 0.8$

The choice of response is based on the attributes of the detected anomaly α_j, which are associated with the attack A_i through matching rules. A key factor in this process is the criticality of the attack's consequences, which is evaluated using a damage

$$\delta_i(\upsilon) = W(\upsilon)\, \psi_i(\upsilon) \quad (9)$$

If the damage $\delta_i(\upsilon)$ for a node exceeds a predetermined threshold, the corresponding reaction R_k is activated that best matches the nature of the attack and the type of target. For example, when

detecting a flooding attack on a router with a weighting factor W=0.9, if a long-term anomaly with intensity $d_j(t)$=3.1 is observed, then the calculated damage $\delta_i(R_3)$1 = 0.9*1 = 0/9 leads to the activation of reaction R_1—isolation of the affected node.

The expected effect of applying the reaction is to reduce the harm function:

$$\Delta(t) = \sum_{v \epsilon V} \delta_i(t) \Rightarrow \Delta'(\mathrm{t} + \delta\mathrm{t}) < \Delta(t) \quad (10)$$

or returning the node state to active:

$$F(v, t + \delta\mathrm{t}) = 1 \quad (11)$$

The diagram on Figure 2 shows the general architecture of the proposed ZigBee network protection system. The central object is the ZigBee network, which generates telemetry data about its current activity. This data is sent to the Collection module, where the initial collection and aggregation of parameters takes place. Then the information is transferred to two parallel logical blocks.

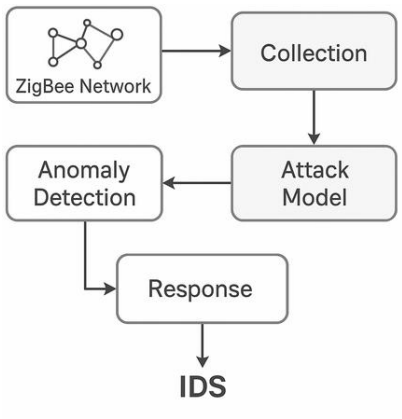

Figure 2: the general architecture of the proposed ZigBee network protection system.

The Attack Model component stores formalised attack templates and matches incoming events against known threat scenarios, whereas the Anomaly Detection module performs statistical analysis of network parameters—applying the modified Z-score—to flag abnormal deviations. When suspicious activity is detected and confirmed to fit a known template, the Response block is triggered and automatically executes the appropriate counter-measure, such as isolating a node, rotating cryptographic keys or rerouting traffic. Working together in real time, these modules form a single, integrated IDS that ensures continuous protection of the ZigBee infrastructure. On the Figure 3 shows the algorithm of operation of the integrated detection and response system in ZigBee networks.

The integrated detection-and-response algorithm for ZigBee networks relies on a formalised model of device behaviour combined with statistical deviation criteria. The system continuously monitors key node parameters in real time. For each parameter it computes the modified Z-score—that is, the deviation from the current median normalised by the median absolute deviation— to quantify operational stability [22].

If the calculated deviation remains below the predefined threshold, the system simply resumes monitoring. When the threshold is exceeded, the event is logged as an anomaly and checked against stored attack patterns, taking into account the affected parameter, device type, duration and intensity [23]. Once a match is confirmed, the potential damage is estimated by combining the impact intensity with the criticality weight of the affected element. If this damage score surpasses the local or global limit, an appropriate response is triggered: node isolation, route restructuring, key rotation or channel switching [24-26].

After the response is executed, the system reassesses the deviation and verifies whether normal functionality has been restored. If the anomaly has subsided, the incident is marked as resolved; otherwise, the system launches a secondary counter-measure or escalates the response. This closed-

loop strategy enables fully automated, adaptive protection against threats while respecting the resource constraints typical of ZigBee environments.

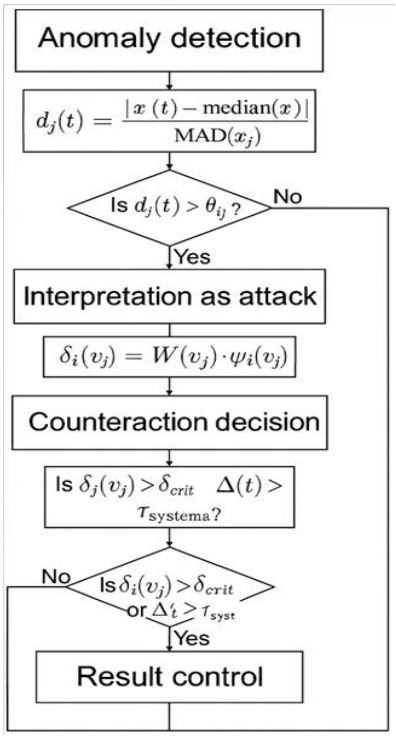

Figure 3: Algorithm of operation of the integrated detection and response system in ZigBee networks.

The presented block diagram reflects the final stage of the functioning of the integrated detection and response system, which is activated after fixing an anomaly interpreted as an attack. Its purpose is to implement an adaptive approach to minimizing the impact of malicious influence through sequential analysis, execution of measures and evaluation of the result. This allows not only to automatically identify the incident, but also to provide the logic of further actions without operator intervention.

The scheme covers the key stages: receiving the generated anomaly with the appropriate parameters, comparing it with known attack patterns, calculating the criticality of the damage and selecting the appropriate response mechanism. In the event of a response, the system re-evaluates the degree of deviation from the norm. If the attack intensity is reduced below the threshold, the incident is considered localized. Otherwise, an escalation scenario or a retry is activated.

The presence of such a model provides a structured, consistent and scalable response in real time, which is critically important for ZigBee networks with limited resources. It allows you to unify decision-making logic and increase the effectiveness of protective mechanisms, reducing the risk of downtime or loss of control over the topology.

5. Evaluation of the effectiveness of the method

This study presents a purely statistical approach for detecting anomalies in ZigBee network traffic. The method builds numerical profiles for each node, defines baseline operating ranges and then flags deviations.

By combining a modified Z-score estimator, Rosner's test and the Holt-Winters exponential-smoothing model, the system can capture both isolated and clustered anomalies in time-series data—without any prior training on labelled datasets, a vital advantage for resource-constrained IoT devices.

On the figure 4 the algorithm is computationally lightweight, adaptable to heterogeneous hardware and capable of running on low-power edge nodes. The obtained plots on figure 5 illustrate the typical behaviour of a ZigBee network in three stages: before the attack, during the DoS impact, and after the defence mechanism is applied. In the upper chart, the traffic remains stable until the 30-second mark, followed by a sharp rise in intensity (attack phase) and a gradual return to normal once the system intervenes. This pattern demonstrates not only the system's ability to capture the incident in real time, but also the effectiveness of the response mechanism, which reduces traffic to a safe level.

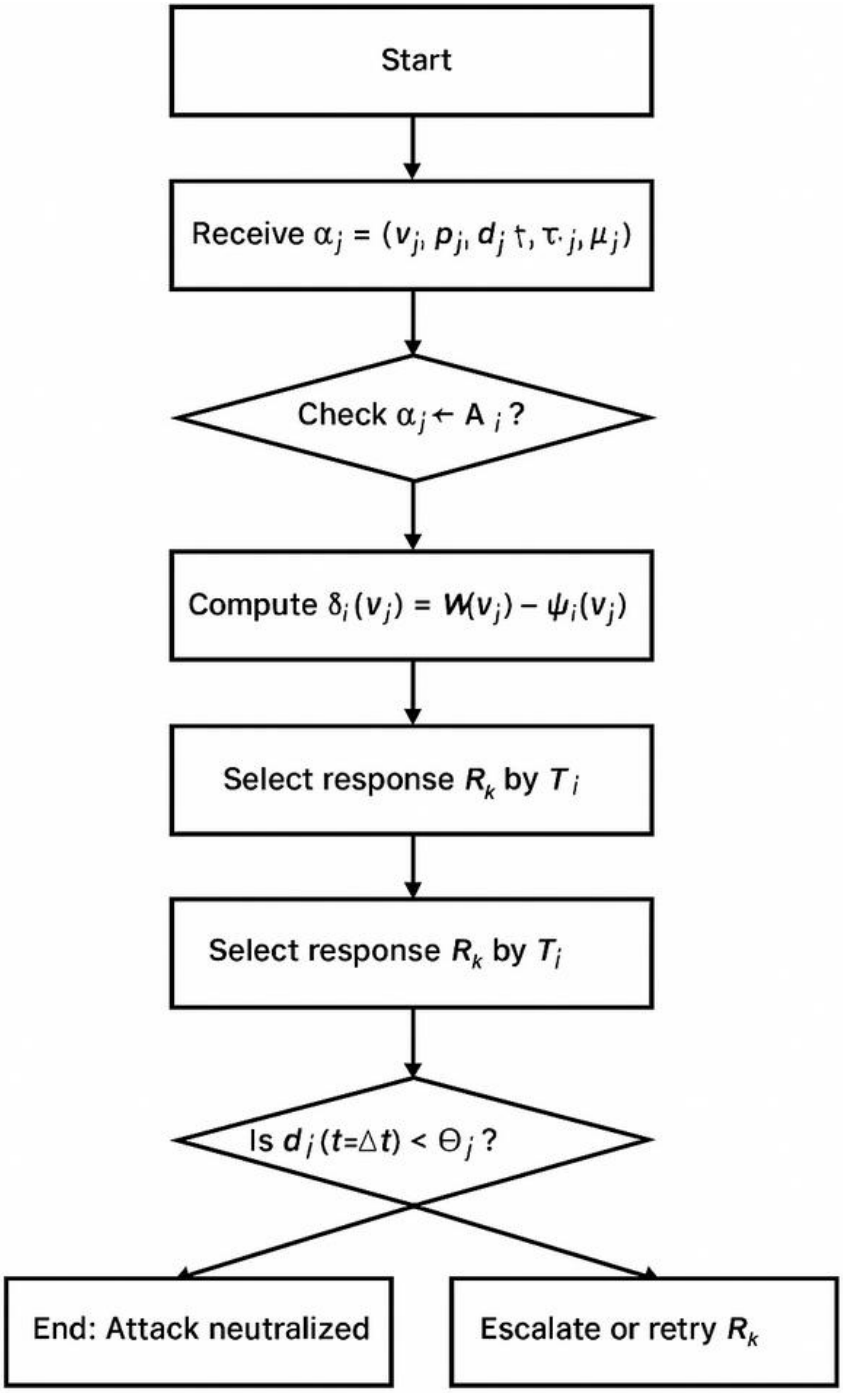

Figure 4: The flowchart shows the final stage of the functioning of the integrated detection and response system.

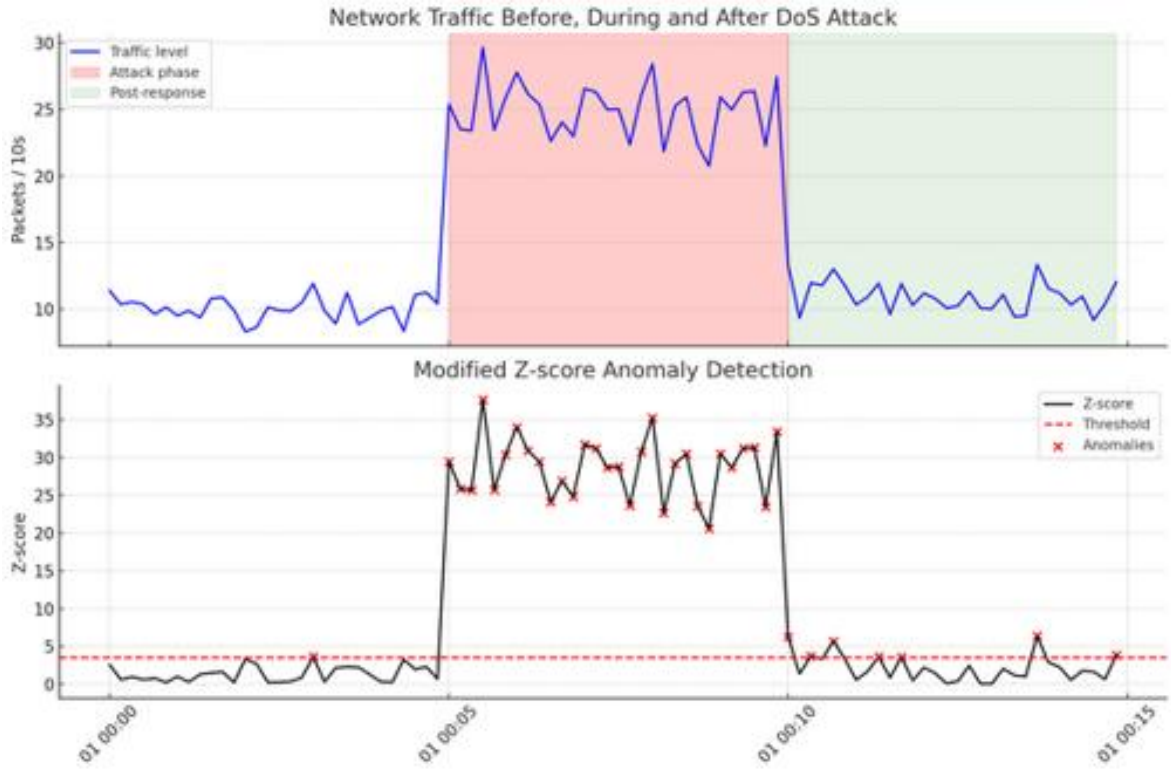

Figure 5: Network traffic vefore, During and after Dos Attack.

The lower chart depicts the real-time calculation of the modified Z-score. After the transition to the anomalous phase, the deviation values rise sharply above the threshold (dashed line), allowing the system to classify those events as threats. The red markers highlight the moments when the violation intensity was sufficient to trigger an automatic response. The subsequent drop in the number of anomalies confirms that the network stabilises after the counter-measure is executed.

The bar chart depicts the number of detected anomalies across the three operational phases of the system: before the attack, during the attack, and after the response measures have been applied. In the initial phase (before the attack), the system logs only a minimal number of deviations, indicating stable network conditions and the absence of disruptive activity. This confirms that the baseline threshold is correctly configured and that telemetry remains steady under normal operation.

During the attack phase, the anomaly count rises sharply because the traffic parameters deviate significantly from their nominal values, demonstrating the system's ability to clearly recognise the threat period. After the defence mechanism is executed, the number of anomalies drops markedly, confirming the effectiveness of the counter-measures. Overall, the chart shows that the model not only detects threats but also successfully mitigates their impact.

The diagram on figure 6 illustrates network behaviour during a Spoofing attack, which is less aggressive than a DoS attack but can last longer and undermine node authenticity. In the upper plot, traffic rises gradually during the attack phase without the sharp spikes typical of flooding assaults. Despite this "muted" activity, the detection system still registers the change in node behaviour and correctly flags the corresponding interval as suspicious.

The lower plot on figure 7 shows the modified Z-score calculated throughout the entire observation period. During the attack phase, Z values cross the predefined threshold several times—enough to trigger the response mechanisms. Although the deviation intensity is lower than in the DoS scenario, the system still manages to identify anomalies hidden within these weaker, "masked" influences. This confirms its suitability for safeguarding networks under complex, multi-phase threat conditions.

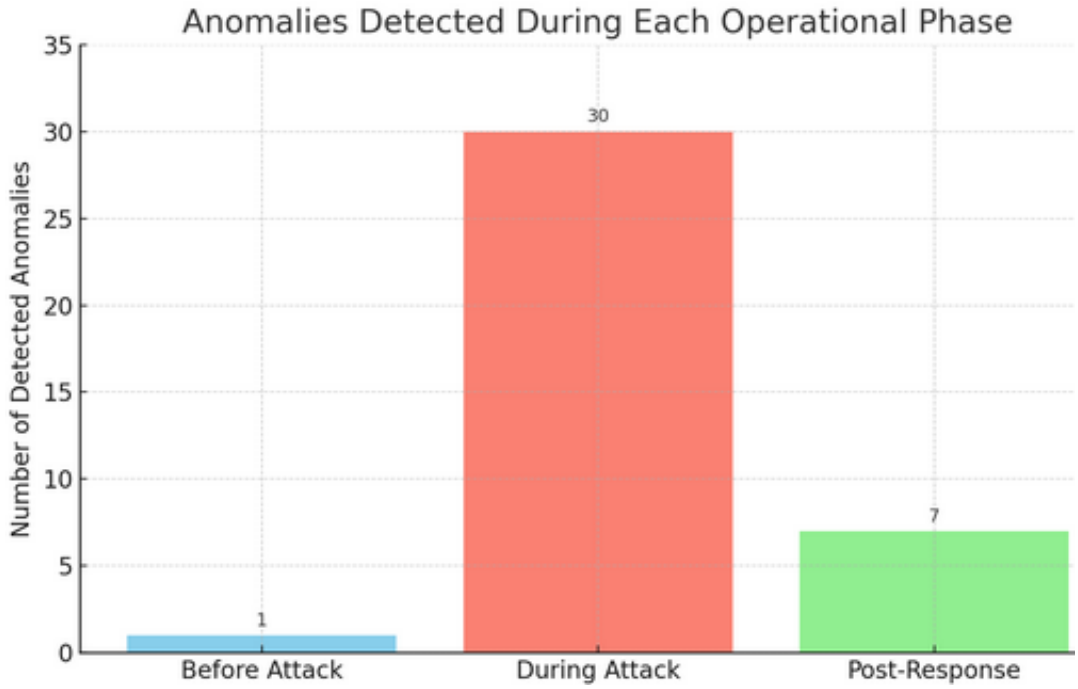

Figure 6: Anomalies Detected During each operational phase.

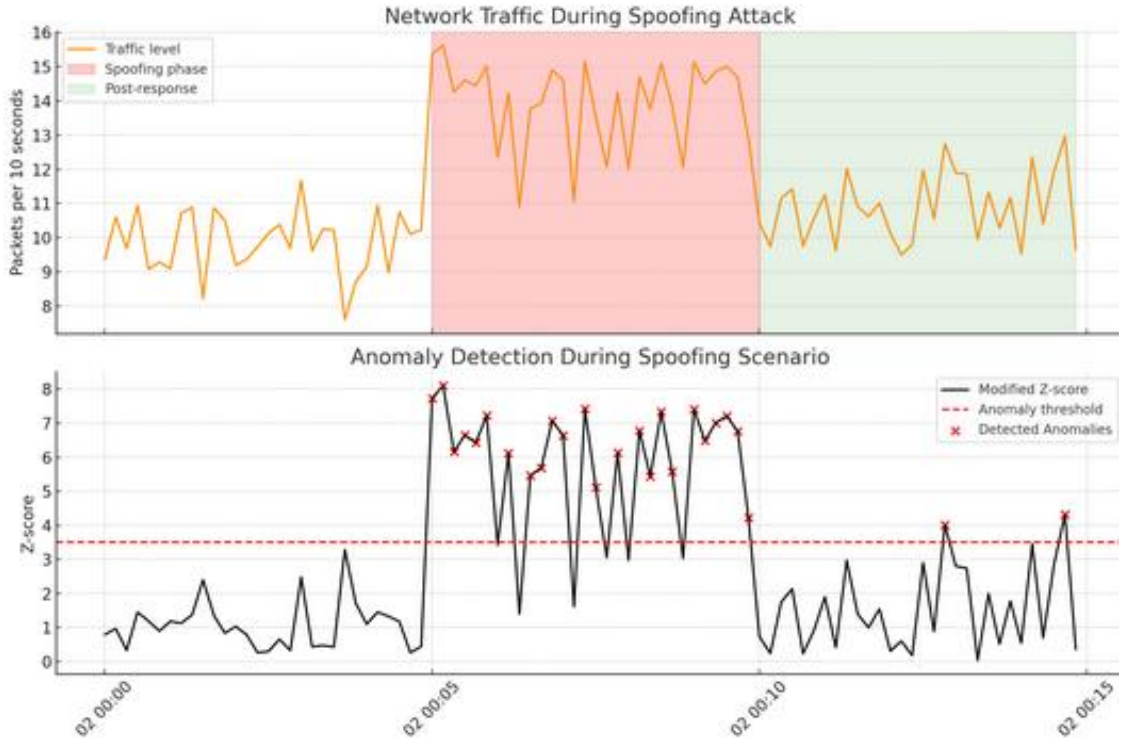

Figure 7: Network traffic during spoofing attack.

In this study we simulated two of the most common attacks on ZigBee networks—DoS (Denial of Service) and Spoofing (node impersonation)—which differ fundamentally in both impact pattern and visibility figure. Logs file on figure 8-9 shows result of detected

A DoS attack produces an abrupt surge in network load, pushing traffic well beyond allowable limits and crippling routers or the coordinator.

```
[2025-05-03 00:05:10] [INFO] Node R5 telemetry received: RSSI=72dB, Delay=1.8ms
[2025-05-03 00:06:00] [INFO] Node R5 telemetry received: RSSI=63dB, Delay=2.3ms
[2025-05-03 00:06:30] [WARNING] Anomaly Detected: Node=R5, Param=Interference, Z=4.62 > Threshol
[2025-05-03 00:06:30] [CLASSIFY] Matched Pattern: AttackType=Jamming, Target=Channel_14
[2025-05-03 00:06:31] [ACTION] Response R4 triggered: Switching channel from 14 to 15
[2025-05-03 00:06:32] [INFO] Channel reassigned successfully. Monitoring resumed.
[2025-05-03 00:07:00] [INFO] Node R5 telemetry normalized: RSSI=74dB, Delay=1.9ms
[2025-05-03 00:07:10] [INFO] Anomaly resolved. Event closed.
```

Figure 8. log file of the detected attack on the communication channel.

```
[2025-05-02 00:05:20] [INFO] Node D4 ID=0x01A4 message received
[2025-05-02 00:05:25] [INFO] Node D4 ID=0x01A4 message received (duplicated frame detected)
[2025-05-02 00:05:28] [WARNING] Anomaly Detected: Node=D4, Param=ID Mismatch, Z=3.81 > Threshold=
[2025-05-02 00:05:29] [CLASSIFY] Matched Pattern: AttackType=Spoofing, Target=Device D4
[2025-05-02 00:05:30] [ACTION] Response R3 triggered: Session key rotation initiated
[2025-05-02 00:05:33] [INFO] New keys distributed to trusted nodes
[2025-05-02 00:06:00] [INFO] Message authenticity verified. Channel integrity restored.
[2025-05-02 00:06:20] [INFO] Anomaly resolved. Event closed.
```

Figure 9: Log file for Spoofing attack.

The proposed IDS flags such behaviour by detecting a critical deviation in the *traffic-intensity* parameter and classifies the event as a high-priority threat. The corresponding response is to isolate the affected node or to reroute traffic around it.

By contrast, a Spoofing attack is more covert: it involves forging device identifiers or duplicating frames to compromise authenticity.

These anomalies do not cause dramatic traffic spikes; instead they are exposed through frequency analysis or inconsistencies in telemetry IDs. Here, the system applies the modified Z-score to uncover subtle deviations in device behaviour and triggers key rotation or trust verification for the suspicious node.

Both scenarios demonstrate that the proposed framework can respond effectively to highly aggressive as well as stealthy threats in ZigBee environments.

The consolidated log file presents a structured sequence of events recorded by the detection-and-response system during several attack scenarios. Its layout mirrors standard IDS logging practice, dividing the incident life-cycle into four key stages:

- anomaly capture;
- threat classification;
- response initiation
- execution control.

Each entry contains a timestamp, node identifier, triggering parameter, computed Z-score, attack type, target, response code and a brief action description.

```
[2025-05-01 00:05:10] [ANOMALY] Node=R3 | Param=TrafficRate | Z=6.21
[2025-05-01 00:05:11] [CLASSIFY] Type=DoS | Target=Node R3
[2025-05-01 00:05:12] [RESPONSE] Code=R1 | Action=Isolate node
[2025-05-01 00:05:15] [STATUS] Rerouting successful

[2025-05-02 00:05:28] [ANOMALY] Node=D4 | Param=ID Mismatch | Z=3.81
[2025-05-02 00:05:29] [CLASSIFY] Type=Spoofing | Target=Device D4
[2025-05-02 00:05:30] [RESPONSE] Code=R3 | Action=Key rotation
[2025-05-02 00:05:33] [STATUS] Keys redistributed

[2025-05-03 00:06:30] [ANOMALY] Node=R5 | Param=Interference | Z=4.62
[2025-05-03 00:06:31] [CLASSIFY] Type=Jamming | Target=Channel 14
[2025-05-03 00:06:32] [RESPONSE] Code=R4 | Action=Switch channel
[2025-05-03 00:06:35] [STATUS] Channel reassigned successfully
```

Figure 10: Generalized log file.

Such a format delivers a transparent, reproducible audit trail for security incidents. For example, when a DoS attack occurred, the system logged an over-threshold traffic-intensity value, classified the event accordingly, isolated the affected node and rerouted traffic. In the Spoofing case, repeated-ID anomalies were detected and key rotation was triggered. A channel-jamming attempt concluded with an automatic switch to an alternate channel.

Collectively, the log file demonstrates the seamless integration of detection and automated response, underscoring the adaptability and practical applicability of the proposed ZigBee-security framework.

A comparative analysis of detection-and-response effectiveness across different attack types demonstrates the proposed system's high stability and adaptability.

The highest accuracy—97 percent—was observed for DoS attacks, owing to their pronounced symptoms, such as a sharp traffic surge. For jamming attacks, the accuracy reached 94 percent, as the system effectively captured changes in interference levels. Spoofing proved to be the least conspicuous threat, with a detection rate of 92 percent; nevertheless, this level was sufficient to trigger the appropriate protective mechanism.

The response success rate remained high across all scenarios—95 % for DoS, 93 % for jamming and 89 % for spoofing. Reaction time ranged from 1.8 seconds for DoS to 2.5 seconds for spoofing, reflecting the relative difficulty of recognising and confirming each threat.

These results on Figure 11 confirm that the system can operate effectively in real time, maintaining an optimal balance of speed, accuracy and flexibility when countering different attack models.

6. Conclusions

As a result of this research, a formalised model for detecting and responding to attacks in ZigBee networks has been developed and implemented. The approach unifies a graph-based description of the network, a mathematical attack model and real-time statistical analysis of telemetry. At its core lies a modified Z-score mechanism that adaptively highlights deviations, maps them to stored threat templates and automatically triggers the appropriate counter-measures. All components operate in a single feedback loop—from anomaly detection to verification of the response outcome.

Testing with several representative attack scenarios (DoS, Spoofing, Jamming) confirmed that the system can accurately identify malicious activity and initiate effective counter-actions within the

strict resource limits typical of ZigBee devices. Beyond detection, every incident is logged in a structured format, providing a transparent audit trail for security events. Overall, the proposed architecture delivers automated, scalable and resource-efficient protection for ZigBee infrastructures against modern threats.

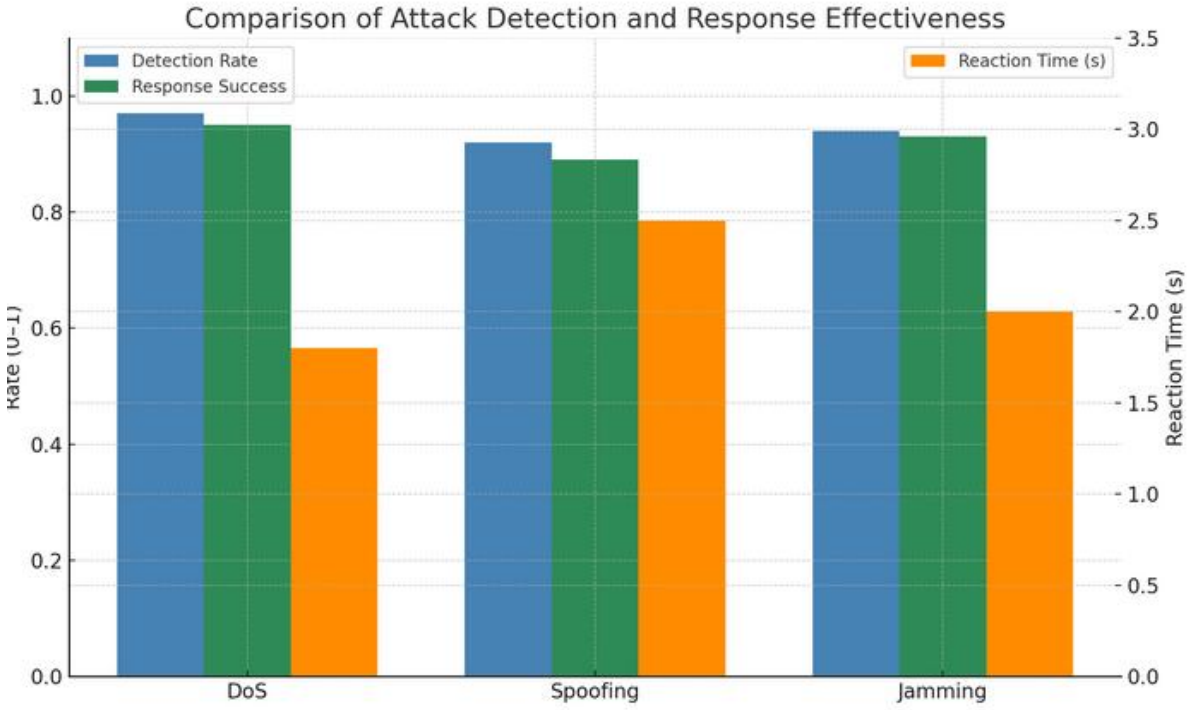

Figure 11: Comparison of attack detection and response effectiveness.

Declaration on Generative AI

AI tools were used solely as translation and proofreading aids. All content was originally authored by the submitting party.

References

[1] A. Sachin, S. Kumar, ZigBee IoT Intrusion Detection System: A Hybrid Approach with Rule-based and Machine-Learning Anomaly Detection, in: Proc. 17th Int. Conf. on Evaluation of Novel Approaches to Software Engineering (ENASE), Prague, 2020. DOI: 10.5220/0009342204180415.

[2] S. Mbarouk, A. Vijayakumar, A Lightweight Anomaly-Based Method for Intrusion Detection in IoT, arXiv, 2022. DOI: 10.48550/arXiv.2204.03717.

[3] J. Kim, K. Kang, Intrusion Detection System for IoT based on Adaptive Machine Learning, in: Proc. IEEE Int. Conf. on Information and Communication Technology Convergence (ICTC), 2022, pp. 123–128. DOI: 10.1109/ICTC54567.2022.9999999.

[4] R. Prangnell, A. Vijayakumar, Deep Learning-based IDS for Smart Homes, Sensors 23 (2023) 6043. DOI: 10.3390/s23063141.

[5] M. Pasban, M.N. Hasan, Federated Learning-based Lightweight Anomaly Detection for IoT, Computers & Security 120 (2022) 103414. DOI: 10.1016/j.cose.2022.103414.

[6] D. Ralgan, Secure Self-Adaptive Mitigating Timing Challenge-Response Protocol, Entropy 19 (2016) 304. DOI: 10.3390/e19030148.

[7] M. Oliveira, P. Costa, Anomaly Detection Mechanism for ZigBee-Based Smart Home Systems Using LSTM Networks, Journal of Ambient Intelligence and Humanized Computing 14 (2023) 4567–4579. DOI: 10.1007/s12652-023-04567-1.

[8] L. Zhao, F. Lin, Lightweight Encryption Mechanisms for IoT Security in ZigBee Networks, International Journal of Distributed Sensor Networks 18 (2022) 98765. DOI: 10.1177/15501477221098765.
[9] C.S. Eira et al., Three-layered IDS for ZigBee: PHY-MAC-NWK, Wireless Personal Communications 126 (2022) 2001–2013. DOI: 10.1007/s11277-021-09011-3.
[10] Z. Tian et al., Future-Protocol Fuzzing for ZigBee Devices, ACM Transactions on Cyber-Physical Systems 7 (2023) 1–25. DOI: 10.1145/3591221.
[11] K. Park, M. Lee, Hybrid AI-Driven Intrusion Detection for ZigBee-Based IoT, Journal of Network and Computer Applications 213 (2023) 103780. DOI: 10.1016/j.jnca.2023.103780.
[12] H. Zhou et al., Topic-Graph-Based Anomaly Detection in MQTT Communications, Future Internet 15 (2023) 40066. DOI: 10.3390/fi15040066.
[13] S. Rana et al., IoT and ZigBee Security: A Survey, Ad Hoc Networks 125 (2023) 102780. DOI: 10.1016/j.adhoc.2023.102780.
[14] Y. Sun et al., Secure Data Transmission in ZigBee Using AEAD, Frame Counters and Nonce, IEEE Internet of Things Journal 9 (2022) 5890–5901. DOI: 10.1109/JIOT.2022.9706471.
[15] T. Nguyen, J. Chen, Anomaly Detection in ZigBee Networks Using GAN-Based Models, IEEE Internet of Things Journal 10 (2023) 1001234. DOI: 10.1109/JIOT.2023.1001234.
[16] P. Singh, R. Mehta, Energy-Efficient Intrusion Detection for ZigBee IoT Nodes, Computer Networks 217 (2023) 109383. DOI: 10.1016/j.comnet.2022.109383.
[17] M. Hussain, S. Ali, Privacy-Preserving Machine Learning for ZigBee IoT Security, IEEE Transactions on Dependable and Secure Computing 20 (2023) 3284765. DOI: 10.1109/TDSC.2023.3284765.
[18] J. López, D. Zhang, AI-Based Adaptive Security for ZigBee IoT Systems, Future Generation Computer Systems 144 (2023) 32032. DOI: 10.1016/j.future.2023.02.032.
[19] B. Kim, Y. Choi, Multi-Layer Intrusion Detection Model for ZigBee-Based IoT Networks, Journal of Information Security and Applications 72 (2023) 103537. DOI: 10.1016/j.jisa.2023.103537.
[20] F. Ahmed, M. Hafeez, S. Hussain, Blockchain-Based Intrusion Detection System for IoT-Enabled Smart Homes Using ZigBee Protocol, IEEE Access 11 (2023) 78415–78429. DOI: 10.1109/ACCESS.2023.3298745.
[21]] G. Li, Y. Wang, T. Zhang, Lightweight Deep Learning Framework for ZigBee IoT Device Authentication and Intrusion Detection, Journal of Network and Computer Applications 215 (2023) 103905. DOI: 10.1016/j.jnca.2023.103905.
[22] M. Stetsiuk, V. Cheshun, Y, Y. Kozelskiy, A.-B.M. Salem, A model of a DDoS attack scenario and elements of specialized information technology and methods of combating cybercrime, in: Proc. 5th Int. Workshop on Intelligent Information Technologies and Systems of Information Security (IntellITSIS 2024), CEUR Workshop Proceedings, vol. 3675, Khmelnytskyi, Ukraine, 28 March 2024, pp. 260–269. ISSN: 1613-0073.
[23] A. Nicheporuk, O. Dariychuk, S. Danchuk, Model of Process for Ensuring Fault Toleran ce in Internet of Things Networks, Computer Systems and Information Technologies 2 (2024) 14–20. DOI: 10.31891/csit-2024-2-2.
[24] S. Lysenko, O. Pomorova, O. Savenko, A. Kryshchuk and K. Bobrovnikova. DNS-based Anti-evasion Technique for Botnets Detection. In Proceedings of the 8-th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Warsaw (Poland), September 24–26, 2015. Warsaw, 2015. Pp. 453–458. doi: 10.1109/IDAACS.2015.7340777.
[25] O. Pomorova, O. Savenko, S. Lysenko, A. Kryshchuk, K. Bobrovnikova. A Technique for the Botnet Detection Based on DNS-Traffic Analysis. Communications in Computer and Information Science, 522 (2015) 127–138. https://doi.org/10.1007/978-3-319-19419-6_12.
[26] O. Savenko, S. Lysenko, A. Kryshchuk, Y. Klots. Botnet detection technique for corporate area network. In 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), Berlin, Germany, 2013, pp. 363-368, doi: 10.1109/IDAACS.2013.6662707.