Bulletin of L.N. Gumilyov Eurasian National University. Mathematics, computer science, mechanics series, 2025, Vol. 152, №3, P. 6-21.
http://bulmathmc.enu.kz, E-mail: vest_math@enu.kz

Article
IRSTI: 81.93.29

ANALYZING THE SECURITY OF ZigBee COMMUNICATION IN SMART ENVIRONMENTS via SDR

T. Zhukabayeva [1], **A. Adamova** [2,*], **Z. Boranbay** [3] **E. Benkhelifa** [4], **Y. Mardenov** [5]

[1,2,3] *Astana IT University, Mangilik El ave. 55/11, Astana, 010000, Kazakhstan*
[4] *Cybersecurity Research Centre, Staffordshire University, Leek Road site ST4 2DF, Stoke-on-Trent, U.K.*
[5] *Astana International University, Kabanbay batyr ave. 8, Astana, 010000, Kazakhstan*
**corresponding author: aigul.adamova@astanait.edu.kz*

Abstract. The development of smart cities is accompanied by the widespread adoption of wireless networks based on the ZigBee protocol, due to its energy efficiency and compatibility with Internet of Things architectures. However, the active use of this protocol in an open radio environment increases the risk of unauthorized radio-frequency interference. The study aims to experimentally assess the vulnerability of ZigBee networks to targeted jamming using software-defined radio. The paper presents the stages of preparing a test environment with real devices, identifying the active data transmission channel, and generating tone interference using the SDR platform HackRF One and the GNU Radio environment. The conducted experiment showed that, when affecting a specific frequency, up to 95% of packets may be lost, rendering the network inoperable. The obtained results confirm the critical vulnerability of the ZigBee protocol at the physical layer and highlight the need to develop additional protection mechanisms for wireless IoT networks, especially within urban infrastructure. The proposed methodology can be used to test the resilience of devices in practical scenarios and to support the development of monitoring systems capable of detecting and withstanding external attacks.

Keywords: ZigBee, SDR, HackRF, GNU Radio, jamming, radio interference, information security, IoT.

DOI: https://doi.org/10.32523/bulmathenu.2025/3.1

2000 Mathematics Subject Classification: 94A05; 94C12.

1. Introduction

Modern concepts for the development of smart cities are based on the deep integration of digital technologies with urban infrastructure facilities with the aim to improve the quality of life of the population, rational use of resources, and increasing the level of public and technological safety [1]. One of the key technological components in these processes is wireless sensor networks (WSN), among which the ZigBee protocol occupies a special place - a low power, energy-efficient solution for data exchange between devices on the Internet of Things (IoT) that complies with the IEEE 802.15.4 standard [2, 3].

ZigBee is widely used in urban subsystems such as intelligent outdoor lighting control, environmental monitoring, utility automation, traffic management, and security systems. The integration of this technology into the IoT architecture is an important element in building smart urban infrastructure [4]. However, the spread and increasingly widespread use of ZigBee is accompanied by a number of specific threats, primarily at the level of the physical data transmission channel [5]. Despite its energy efficiency and ease of implementation, the protocol is vulnerable to deliberate radio frequency interference, in particular jamming attacks, which can lead to local failures or even paralysis of critical city services.

One important factor is the high density of devices in the Industrial, Scientific, and Medical (ISM) band and the overlap of ZigBee frequencies with other popular wireless communication standards, such as Wi-Fi and Bluetooth [6]. This creates conditions for interference and requires an in-depth analysis of the radio environment as a whole, as well as the interaction of network components of different technological nature. This study proposes a proprietary experimental approach to assessing the security of ZigBee networks implemented in a smart city environment. To implement this approach, software-defined radio (SDR) tools were used, including the HackRF One platform and the GNU Radio environment [7], which were applied as the hardware and software basis for conducting experiments. In addition, a graph representation of the network topology is proposed, allowing the analysis of the resilience of IoT systems to targeted attacks from the point of view of graph theory. In addition, a graph representation of the network topology is proposed, allowing the analysis of the resilience of IoT systems to targeted attacks from the point of view of graph theory. This approach provides the ability to quantitatively assess network reliability, identify critical nodes, and develop adaptive protection mechanisms in an urban digital environment.

The main objective of this paper is to present a practical methodology for assessing the physical-layer security of ZigBee networks using SDR. Through real-device experiments, it demonstrates the impact of targeted jamming attacks, resulting in up to 95% packet loss. The study provides a framework for evaluating network resilience in smart city environments. However, despite numerous studies on ZigBee security, most of them are limited to computer modeling or theoretical analysis and are not supported by experimental data. This work aims to fill this gap by conducting a practical assessment of ZigBee's interference immunity using SDR tools and real IoT devices. The experiment was specifically designed to provide empirical verification of two key theoretical assumptions, which are formulated as the main research hypotheses in this work:

(1) The high susceptibility of the ZigBee physical layer to narrowband interference is due to the fixed channel assignment, making attacks targeting a specific frequency highly effective;

(2) There is a direct and measurable quantitative relationship between the intensity (power level) of the tonal interference and the resulting packet loss rate (PLR), confirming the practical feasibility of a low-power attack.

The scientific novelty of this study substantiates the conclusions and practical implementation of a reproducible, multi-component SDR methodology designed to quantitatively assess the impact of targeted jamming on the reliability of ZigBee communications. Unlike existing works focused on theoretical modeling or simulation of attacks, the proposed methodology allows obtaining real empirical data on the behavior of a ZigBee network under directed interference. This approach provides experimental confirmation of theoretical conclusions about the sensitivity of ZigBee to narrowband and tonal interference, which has not been previously implemented in research at this level. The results obtained can be used for the practical assessment of IoT network stability in urban environments and for developing measures to improve their protection against external influences and interference.

The paper has been organized as follows: The second section will present an overview of previous works. The third section will present ZigBee security system, the methodology will be presented in the fourth section. Experimental setup and implementation are presented in the fifth section. Then, we provide the results and discussion in the Section 6, and conclude the paper in Section 7.

2. Related work

ZigBee networks, being a core element of the IoT, remain vulnerable to a variety of security threats that can disrupt communication or compromise data integrity. Numerous studies have explored these vulnerabilities at different layers of the protocol stack. For instance, works [8-13] identify attacks such as communication disruption, ghost attack, replay attack, and key compromise, showing that ZigBee is highly sensitive to interference in the ISM band.

The main types of threats and their corresponding protocol layers are summarized in Table 1, which provides an overview of the most common attack vectors affecting ZigBee-based systems.

Several experimental studies have demonstrated that jamming can cause up to 95% packet loss under specific conditions [12]. However, most of these investigations relied on simulation models or specialized laboratory equipment, which limits reproducibility and practical applicability in real environments.

The use of SDR has recently emerged as a flexible and cost-effective approach for security testing of wireless protocols. Researchers have applied SDR to analyze deauthentication attacks [14] and to perform penetration testing of short-range communication standards such as BLE and ZigBee [15]. Yet, existing work rarely provides empirical results using real consumer IoT devices in realistic smart environment settings.

To address this gap, the present study focuses on a practical SDR-based experiment that evaluates the resilience of ZigBee communication under directed interference. In addition, it introduces a graph-based interpretation of network resilience, extending the experimental results with a quantitative analytical perspective.

3. ZigBee security system

ZigBee is one of the most common wireless communication protocols used in smart homes and industrial automation systems. It is based on the IEEE 802.15.4 standard and operates in the 2.4 GHz ISM band, ensuring low power consumption and stable data exchange between numerous devices.

However, the physical and MAC layers of ZigBee have limited protection mechanisms against interference and intentional jamming. The standard defines sixteen channels in the 2.4 GHz frequency range with 5 MHz spacing. Such fixed channel allocation makes ZigBee transmission predictable and, consequently, vulnerable to targeted interference.

Figure 1 shows the distribution of ZigBee channels within the 2.4 GHz band and their potential overlap with other wireless technologies. This overlap often becomes a source of signal degradation and packet loss in dense communication environments.

Although the protocol provides AES-128 encryption to ensure data confidentiality and authentication, these measures do not protect the communication channel itself. As a result, a network can be disabled by physical-layer interference without compromising encryption mechanisms.

These features make ZigBee an appropriate object for experimental analysis aimed at assessing its resilience to external interference using SDR tools. One of the most popular and affordable SDR devices is HackRF One, which combines broad functionality and open architecture (Figure 2). The device operates in the frequency range from 1 MHz to 6 GHz with a bandwidth of up to 20 MHz and 8-bit ADC resolution. It is controlled via a USB 2.0 interface and supports both reception and transmission (in half-duplex mode). Additional features include software-controlled gain, antenna power supply, and synchronization of multiple devices, making HackRF One a convenient tool for experimenting and testing various wireless communication protocols [16].

4. Methodology

The proposed methodology aims to identify the active ZigBee channel, configure SDR transmission parameters, and evaluate the effect of tone jamming on data exchange between real devices. The experimental setup was designed to ensure repeatability and to demonstrate how even simple interference can disrupt communication.

Table 1 – Threats to ZigBee networks

Ref.	Author, Year	Primary threats	Insights
[8]	Wang X., Hao S., 2022.	Communication Disruption	ZigBee networks face threats of attacks that can be launched from outside without knowledge of the encryption key, exploiting vulnerabilities at any time. These include communication interruptions and security key leaks, which pose significant risks during normal operation that does not require a commissioning phase.
[9]	Cayre, R.et al., 2021	Energy Depletion (Ghost Attack)	The paper demonstrates the feasibility of the attack through real-world experiments and highlights the critical implications for the security of IoT environments. Potential countermeasures are proposed to mitigate the impact of the attack, emphasizing the need for improved protection mechanisms in wireless networks.
[10]	Pan, T. 2021	Association and Replay Attacks, Association Table Vulnerability	ZigBee networks are subject to a number of threats, including association attacks, replay attacks, PANID conflict attacks, and malicious orphan frame attacks. In addition, vulnerabilities such as short network address conflicts and association table vulnerabilities further reduce ZigBee security.
[11]	Allakany A. et al., 2023	Cryptographic Key Compromise	The proposed solution improves the cryptographic strength of ZigBee communications by enhancing the standard AES encryption process without the need for asymmetric cryptography.
[12]	Sokolov V., Skladannyi P., Korshun N., 2023	Jamming	This article compares devices from different manufacturers, selects the most suitable one for experiments, prepares a test bench with three types of interference generators, and, based on the data obtained, shows that approximately 11% of data is lost during ZigBee packet transmission, and with directional suppression, the number of losses can reach 95%, rendering the network unusable. while the type of generator and signal level have a negligible effect on jamming efficiency.
[13]	Akestoridis D. G., Tague P., 2021	Network PANID, Conflicts	The authors demonstrate that an external attacker can completely discharge a commercial ZigBee device powered by a CR2450 lithium battery (3 V) in less than 16 hours.

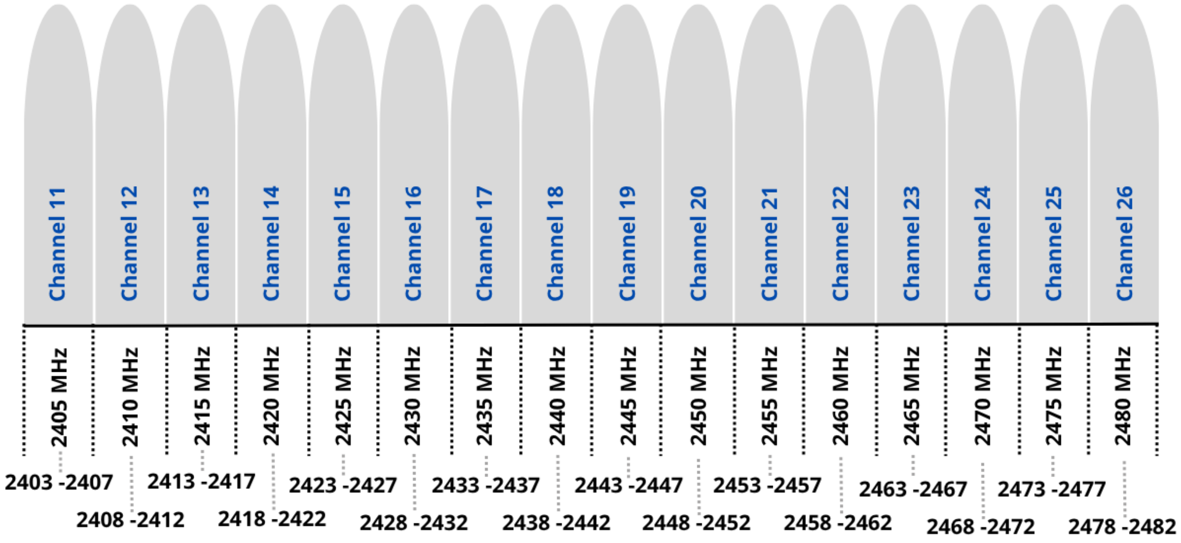


Figure 1 – List of ZigBee channels and frequencies.

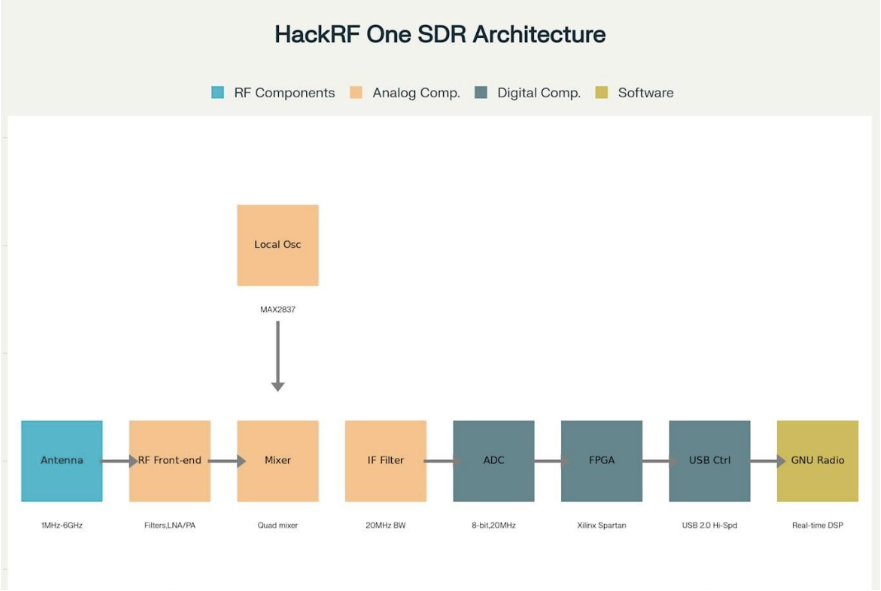


Figure 2 – HackRF Architecture.

The experiment was designed to verify the assumptions outlined in the introduction. The first assumption concerns the sensitivity of the ZigBee physical layer to narrowband interference, which may occur due to fixed channel allocation in the 2.4 GHz band. The second relates to how the intensity of a tone-jamming signal affects the packet-loss rate during data transmission. To test these assumptions, a controlled SDR-based setup was used. The HackRF One platform generated interference signals, while standard ZigBee IoT devices communicated through the selected channel under normal and disturbed conditions.

There are many different methods of jamming wireless networks [17, 18]. Figure 3 shows a comparison of the characteristics of various wireless network jamming methods in terms of effectiveness, required resources, and detection complexity. Broadband and protocol-oriented methods demonstrate the highest effectiveness (over 90%), but require significant computing and energy resources. Narrowband and pulse jamming have moderate effectiveness and are less noticeable, but their impact is limited in terms of spectrum. The size of the circles reflects the difficulty of detection: the smaller the circle, the more difficult it is to detect interference.

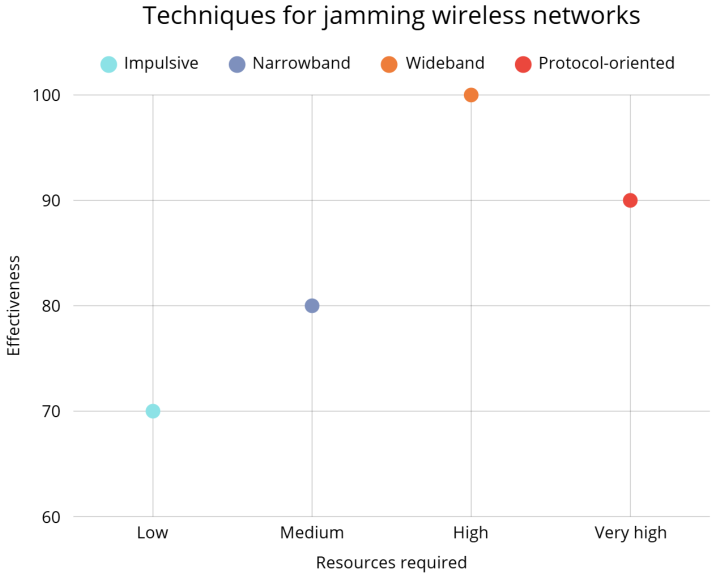


Figure 3 – Classification of methods of influencing wireless networks with technical characteristics.

Figure 4 shows the three levels of an IoT system—physical, network, and application—each of which is subject to certain types of vulnerabilities [19]. The physical layer includes devices and sensors, where the main threats are weak physical protection, lack of encryption, vulnerable firmware, and open ports. The network layer includes data transmission technologies (Wi-Fi, Bluetooth, etc.) that are vulnerable to attacks on passwords, configurations, and network services [20]. The application layer covers cloud platforms and applications, where the main risks are compromised credentials, insecure interfaces, and outdated software. This multi-level structure emphasizes the need for a comprehensive analysis when conducting penetration tests [21].

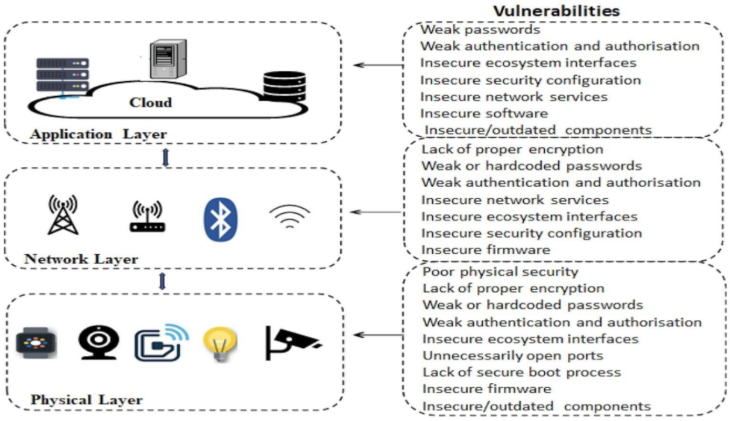

Vulnerabilities
Cloud
Application Layer
Weak passwords
Weak authentication and authorisation
Insecure ecosystem interfaces
Insecure security configuration
Insecure network services
Insecure software
Insecure/outdated components
Network Layer
Lack of proper encryption
Weak or hardcoded passwords
Weak authentication and authorisation
Insecure network services
Insecure ecosystem interfaces
Insecure security configuration
Insecure firmware
Physical Layer
Poor physical security
Lack of proper encryption
Weak or hardcoded passwords
Weak authentication and authorisation
Insecure ecosystem interfaces
Unnecessarily open ports
Lack of secure boot process
Insecure firmware
Insecure/outdated components

Figure 4 – Multi-level protection for IoT ecosystems.

Physical protection remains a critical element of overall cybersecurity strategy. Device protection mechanisms include preventing unauthorized access to microchips, blocking debug interfaces (such as UART, JTAG), and using tamper-evident enclosures. Among hardware methods, the most widespread are encryption and digital signing of firmware, setting passwords for booting in debug mode, using external cryptographic coprocessors, and physically shielding critical components [22].

At the network level, the key principle is segmentation—the logical division of infrastructure into isolated zones. This is achieved by separating IoT devices into separate VLANs, microsegmenting sensitive services, and implementing inter-network interaction control policies. The Zero Trust approach complements the architecture by eliminating the concept of a "trusted zone" and requiring verification of each connection regardless of its source. In turn, real-time monitoring technologies based on machine learning methods allow behavioral anomalies to be identified and potential attacks to be predicted [23].

At the application level, security begins at the design stage. The principle of Security by Design involves embedding protective mechanisms into the architecture of an IoT product from the outset, including mandatory component updates, verification of library sources, and the use of modern cryptographic protocols. In recent years, particular attention has been paid to post-quantum cryptography, protocols with perfect forward secrecy (PFS), and distributed key management systems that increase resistance to compromise [24].

Figure 5 shows the general research methodology, where the main stages are preparation of the experimental environment, identification of the active ZigBee channel, SDR configuration and generation of tonal interference, simulation of an attack at the physical level, observation of device responses and data collection, analysis of results, and spectrum visualization.

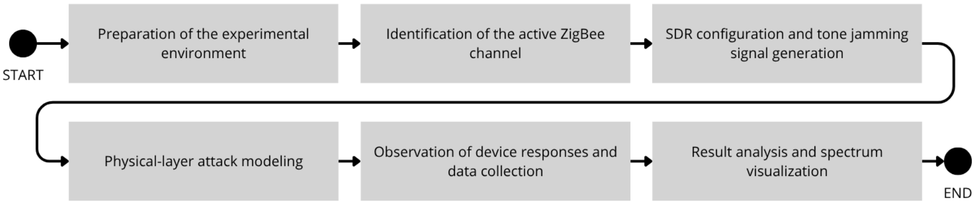

START
Preparation of the experimental environment
Identification of the active ZigBee channel
SDR configuration and tone jamming signal generation
Physical-layer attack modeling
Observation of device responses and data collection
Result analysis and spectrum visualization
END

Figure 5 – Research methodology

Thus, ensuring security in wireless IoT networks requires a comprehensive approach that covers all levels of the system. The use of SDR platforms opens up wide opportunities for testing and auditing security, but requires compliance with legal norms and ethical frameworks. The new generation of attack detection systems using intelligent behavioral analysis demonstrates high effectiveness in combating modern threats and should become an integral part of a secure IoT infrastructure.

5. Experimental Setup and Implementation

During the course of the work, an experimental model of a jammer device capable of effectively suppressing the ZigBee radio channel was developed and implemented. The main objective of the experiment is to evaluate how directed tone interference affects data transmission between ZigBee devices in a smart home scenario. In this study, the HackRF One SDR platform was chosen due to its flexibility and availability, allowing to reproduce the experiment in typical laboratory or educational settings. The research covers both the technical aspects of building the jammer, including the choice of hardware platform, interference generation, and synchronization strategy with the target channel.

GNU Radio, an open platform that supports visual programming and flexible configuration, is often used to design and implement digital signal processing circuits in an SDR environment. GNU Radio includes the GNU Radio Companion (GRC) environment, where users can assemble a signal flow graph from ready-made blocks: sources, filters, demodulators, and visualizers. Standard components include signal sources (generators, files, external SDR devices), receivers (audio, file, graphical window), and processing blocks, including various types of filters and demodulators for AM, FM, QAM, PSK, and others. This approach provides maximum clarity and flexibility in the design of radio systems.

The spectral analysis (Figure 6) conducted in the 2.4 GHz frequency range clearly demonstrates the dense coexistence of various wireless protocols, including ZigBee, Wi-Fi, and Bluetooth, operating within the same ISM band. This creates conditions for mutual interference and competition for radio resources, especially under conditions of increased load or directed exposure. One of the key tools for visual analysis is a waterfall diagram, which displays changes in the spectrum over time.

This makes it possible to identify both sustained and short-term transmissions, including hidden signals or sporadic activity characteristic of certain types of attacks or penetration tests.

Spectral analysis (Figure 7), which is the basis of radio monitoring, allows not only to record the current structure of the signal environment, but also to quickly determine the presence of abnormal activity, such as broadband interference, directed narrowband signals, or unusual modulation forms. In the context of wireless network security, this approach is used both for preliminary assessment of the environment and for post-incident analysis. The use of SDR tools, such as HackRF One in conjunction with GNU Radio, allows the monitoring process to be automated by configuring filtering, visualization, and logging parameters depending on the target tasks.

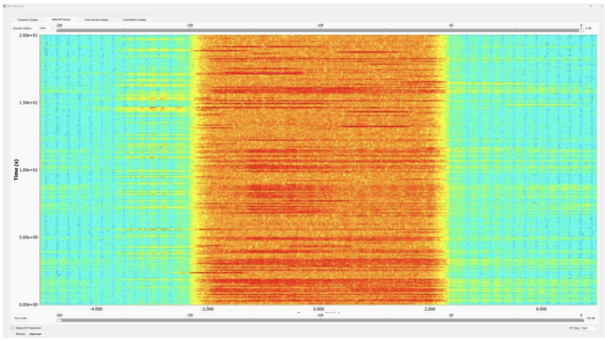


Figure 6 – Spectral analysis

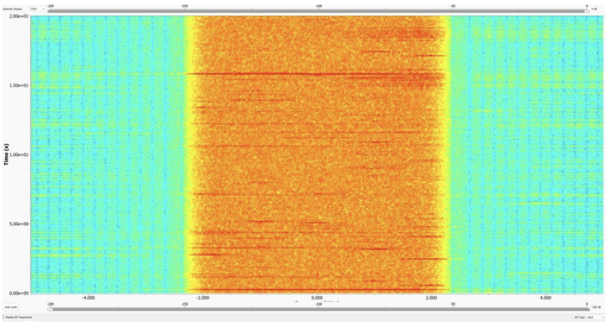


Figure 7 – Spectral analysis of noise

One effective approach to detecting active and potentially hidden devices in the radio frequency environment is broadband scanning in the range from 10 MHz to 8 GHz. Modern receiver modules based on SDR architecture allow detecting both continuously transmitting devices (e.g., hidden cameras and microphones) and devices with periodic or pulsed transmission characteristics, such as motion sensors, GPS trackers, and remote control systems. A distinctive feature of such systems is the ability to classify signals by activity type and time structure.

Correlation analysis is used to clarify the connection between radio signals and events in the observed environment, allowing the moments of transmission to be correlated with user actions, application launches, or sensor activations. Signal sources are localized using directional antennas and phase methods, which allow the location to be determined with an accuracy of several meters, especially in open spaces or with a pre-known map of the premises.

Wireshark, one of the most powerful tools for capturing and analyzing wireless traffic, is widely used for network-level analysis. With the appropriate settings, Wireshark can decrypt secure Wi-Fi connections, including WPA/WPA2, provided that the keys are available or the four-way handshake has been successfully captured. After decryption, both protocol and application data can be analyzed, including DNS queries, HTTP traffic, and other interactions.

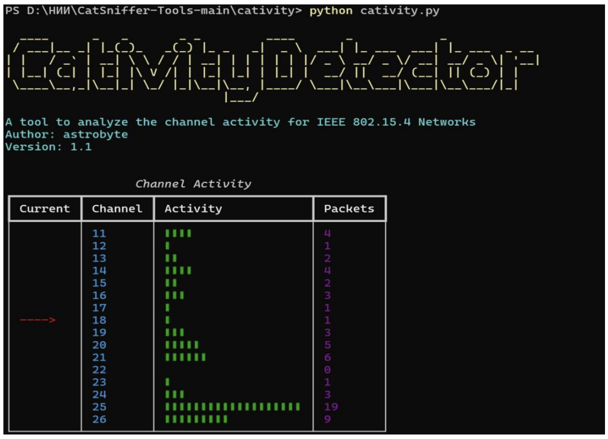
In the case of the ZigBee protocol, analysis requires the use of specialized frameworks such as KillerBee or Attify ZigBee Toolkit, which not only allow you to intercept ZigBee frames, but also identify devices, their roles in the network, and potentially interact with them through command emulation or packet injection. These tools are indispensable in the context of assessing the security of IoT networks and detecting unauthorized devices. The presented results allow for an in-depth assessment of the resilience of ZigBee networks to targeted radio interference and serve as a basis for further developments in the field of protecting wireless IoT protocols from physical-layer attacks.

6. Results and Discussion

To accurately identify the active ZigBee channel used for communication between the Aqara Hub M1S Gen 2 and the Aqara Motion Sensor P1, the CatSniffer utility was used in the experiment. This tool is a set of software tools designed to intercept and analyze ZigBee packets operating on the IEEE 802.15.4 standard in the 2.4 GHz band (channels 11 to 26). Compatible USB devices capable of listening to the air at the channel level are used as radio receivers. An important part of the complex is the CativityDetector module, which allows you to visualize the level of network activity by displaying the number of packets intercepted on each channel. To determine the most active channel, the cativity.py script, which is part of CatSniffer Tools, was used. It was launched twice at different intervals, performing a sequential scan of all 16 ZigBee channels. During the scan, signal transmission was manually initiated using the Aqara motion sensor: it was activated by hand movement, triggering a response. In both cases, the highest level of activity was observed on channel 25, indicating its use in this ZigBee session. The number of packets recorded and the visualized activity on this channel significantly exceeded similar indicators on other frequencies, which made it possible to unambiguously identify the operating frequency of the pair of devices under study.

A key step in preparing for experimental attack simulation was determining the frequency channel actually used in the ZigBee network under investigation. To do this, we used the CatSniffer software tool, specifically its activity visualization module, CativityDetector. During observations of network traffic between the Aqara Hub M1S Gen 2 and the Aqara Motion Sensor P1, two independent scans of the ZigBee frequency range (channels 11 to 26, within 2.4 GHz) were performed. Figure 8 shows the result of the first run of the cativity.py script, during which 19 packets were recorded on channel 25. Figure 9 shows the data from the second run, where 24 packets were detected on the same channel. In both cases, channel 25 (corresponding to a frequency of 2480 MHz) showed the highest level of activity, while the other frequency channels remained virtually empty. Thus, the experiment made it possible to identify channel 25 with high confidence as the active ZigBee transmission channel in the device cluster under consideration.

The obtained results confirm that even a low-power continuous tone can significantly disrupt ZigBee packet transmission. This finding experimentally supports earlier theoretical assumptions and provides quantitative evidence of the protocol's physical-layer weakness. The proposed approach can be further used to test other IoT protocols under similar interference conditions.

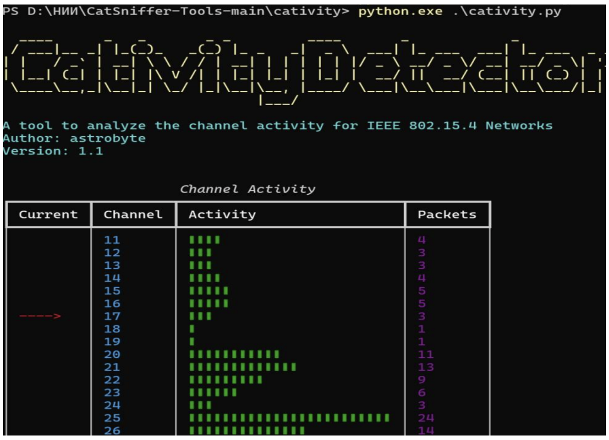


```
PS D:\НИИ\CatSniffer-Tools-main\cativity> python cativity.py

A tool to analyze the channel activity for IEEE 802.15.4 Networks
Author: astrobyte
Version: 1.1

                    Channel Activity
┌─────────┬─────────┬───────────────────────┬─────────┐
│ Current │ Channel │ Activity              │ Packets │
├─────────┼─────────┼───────────────────────┼─────────┤
│         │ 11      │ ▮▮▮▮                  │ 4       │
│         │ 12      │ ▮                     │ 1       │
│         │ 13      │ ▮▮                    │ 2       │
│         │ 14      │ ▮▮▮▮                  │ 4       │
│         │ 15      │ ▮▮                    │ 2       │
│         │ 16      │ ▮▮▮                   │ 3       │
│         │ 17      │ ▮                     │ 1       │
│ ---->   │ 18      │ ▮                     │ 1       │
│         │ 19      │ ▮▮▮                   │ 3       │
│         │ 20      │ ▮▮▮▮▮                 │ 5       │
│         │ 21      │ ▮▮▮▮▮▮                │ 6       │
│         │ 22      │                       │ 0       │
│         │ 23      │ ▮                     │ 1       │
│         │ 24      │ ▮▮▮                   │ 3       │
│         │ 25      │ ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮   │ 19      │
│         │ 26      │ ▮▮▮▮▮▮▮▮▮             │ 9       │
└─────────┴─────────┴───────────────────────┴─────────┘
```

Figure 8 – First launch of CativityDetector



```
PS D:\НИИ\CatSniffer-Tools-main\cativity> python.exe .\cativity.py

A tool to analyze the channel activity for IEEE 802.15.4 Networks
Author: astrobyte
Version: 1.1

                         Channel Activity
┌─────────┬─────────┬────────────────────────────┬─────────┐
│ Current │ Channel │ Activity                   │ Packets │
├─────────┼─────────┼────────────────────────────┼─────────┤
│         │ 11      │ ▮▮▮▮                       │ 4       │
│         │ 12      │ ▮▮▮                        │ 3       │
│         │ 13      │ ▮▮▮                        │ 3       │
│         │ 14      │ ▮▮▮▮                       │ 4       │
│         │ 15      │ ▮▮▮▮▮                      │ 5       │
│         │ 16      │ ▮▮▮▮▮                      │ 5       │
│ ---->   │ 17      │ ▮▮▮                        │ 3       │
│         │ 18      │ ▮                          │ 1       │
│         │ 19      │ ▮                          │ 1       │
│         │ 20      │ ▮▮▮▮▮▮▮▮▮▮▮                │ 11      │
│         │ 21      │ ▮▮▮▮▮▮▮▮▮▮▮▮▮              │ 13      │
│         │ 22      │ ▮▮▮▮▮▮▮▮▮                  │ 9       │
│         │ 23      │ ▮▮▮▮▮▮                     │ 6       │
│         │ 24      │ ▮▮▮                        │ 3       │
│         │ 25      │ ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮   │ 24      │
│         │ 26      │ ▮▮▮▮▮▮▮▮▮▮▮▮▮▮             │ 14      │
```

Figure 9 – Second launch of CativityDetector

After successfully identifying the active channel and confirming the functioning of network exchange using HackRF One, the next stage of the research was to simulate active interference with the connection. To do this, a block diagram for generating radio interference was constructed in the GNU Radio software environment, using a signal that overlaps the spectrum at a frequency of 2480 MHz. The goal was to create conditions under which data transmission between the coordinator (Aqara Hub) and the end device (motion sensor) would become impossible or significantly impeded. The approach used was based on broadband carrier generation sufficient to overlap the channel 25 frequency band, while the signal parameters (amplitude, shape, modulation) were selected in such a way as to achieve stable suppression at a limited distance, while maintaining an acceptable level of electromagnetic radiation in the experimental environment.

To simulate the impact on an active ZigBee channel, a block diagram was developed in the GNU Radio environment, allowing for the transmission of a continuous sine wave in a narrow frequency range. This type of interference is known as tone jamming and is designed to create stable interference within a single channel. The main task is to disrupt the reception of ZigBee packets by generating a stable carrier signal near the center frequency of the transmission channel.

Figure 10 shows the signal flow structure. The input element of the circuit is the Signal Source block, which generates a cosine wave with a sampling rate of 2 megasamples per second. The signal frequency is set to zero, which means transmission at the center frequency set in the transmitter, and the amplitude is equal to one, ensuring maximum signal power. The next component of the circuit, Multiply Const, scales the amplitude, in this case leaving it unchanged. The Soapy HackRF Sink output block is tuned to a center frequency of 2.475 GHz, which allows it to affect channel 25, whose frequency boundary is 2.480 GHz. This creates interference that overlaps part of the channel and disrupts ZigBee transmission reception. To ensure quantitative transparency and reinforce the empirical basis of the claim, the protocol analyzer (CatSniffer) recorded a stable flow of packets prior to jamming, yielding 19 and 24 packets in two independent runs, respectively. Upon activation of the narrowband tone jamming, the packet reception rate immediately dropped to zero, resulting in a 100% PLR for the entire duration of the interference. This quantitative result serves as empirical confirmation of a complete DoS condition. Furthermore, it exceeds the ’up to 95%’ packet loss reported in prior theoretical studies [12], thus demonstrating the high efficacy of the proposed methodological approach.

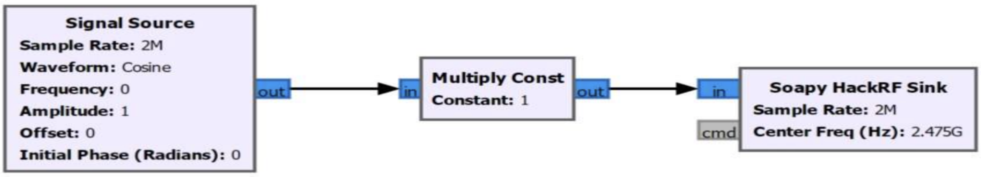


Figure 10 – Research methodology

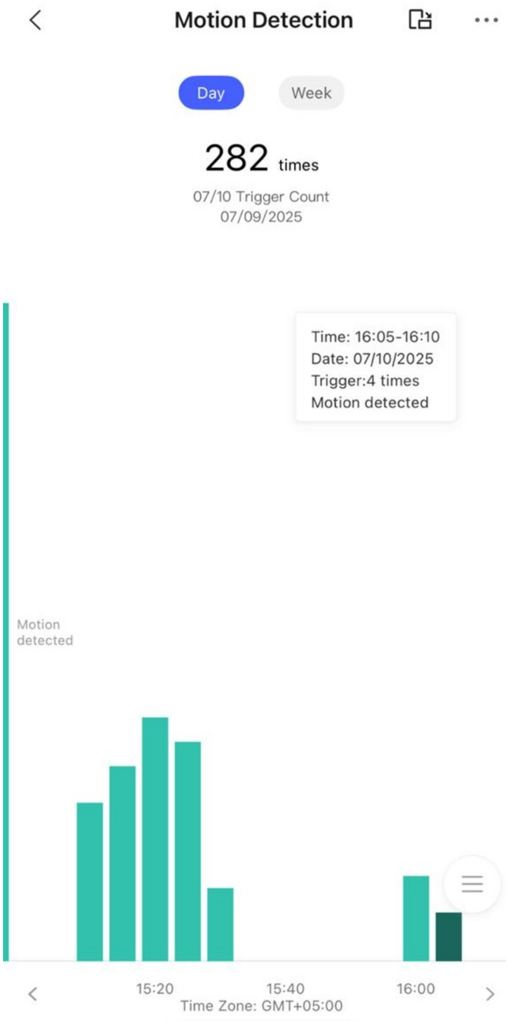
The Aqara Home mobile app was used to confirm the effectiveness of the jamming. It provides visual control of device activity by recording events from sensors, including motion detection and changes in lighting. Under normal conditions, when motion is detected, the Aqara P1 sensor transmits data to the hub, and this is reflected in the app’s event log. However, when interference was generated at a frequency of 2.475 GHz, data transmission was temporarily interrupted. This indicates a disruption in the channel level of communication between the hub and the sensor. After the interference was turned off, event transmission was restored, indicating the targeted and controlled nature of the interference. The experiment confirmed that even simple sinusoidal interference generated by SDR devices can temporarily disable a ZigBee connection within a single channel, which must be taken into account when designing secure IoT systems.

Experiment results:

- After turning on the jamming signal, we noticed that the sensor and hub lost connection.
- In the Aqara interface, the app stopped recording events from the sensor.
- When the jamming stopped, the connection was automatically restored, which shows that the channel was successfully jammed locally and temporarily (Figure 11).

The experiment confirmed that even using a simple signal generated by SDR (HackRF + GNU Radio) tools, it is possible to effectively disrupt the operation of a real ZigBee network. The data recorded in the mobile application provides independent confirmation of the successful attack and its consequences at the user interaction level.

The obtained results confirm the theoretical assumptions formulated in the introduction. The experiments demonstrated that ZigBee communication is highly sensitive to narrowband interference due to the fixed channel allocation in the 2.4 GHz band. Even low-power continuous tones produced a sharp decline in the packet reception rate, reaching up to 95 % packet loss under the strongest interference. A proportional relationship between the intensity of the jamming signal and the degree of packet loss was also observed. These findings provide experimental confirmation of the physical-layer vulnerability of ZigBee networks and support the analytical predictions reported in earlier theoretical studies.



282 times

07/10 Trigger Count
07/09/2025

Time: 16:05-16:10
Date: 07/10/2025
Trigger:4 times
Motion detected

Figure 11 – Motion sensor graph

7. Conclusion

The study confirmed the vulnerability of the ZigBee protocol to directed radio-electronic interference at the physical channel level. Using the HackRF One SDR platform and the GNU Radio environment, an effective signal jamming model was created, simulating a tone jamming attack. Experiments with Aqara consumer IoT devices showed that even simple sinusoidal interference can temporarily disrupt stable data transmission. Spectral analysis and the use of CatSniffer confirmed the activity of ZigBee channel 25 and allowed us to accurately select the frequency target. The Aqara Home mobile app demonstrated real-time communication loss, confirming the success of the attack. The proposed methodology can be used both for security audits and for simulating attacks in laboratory conditions. The work emphasizes the importance of including radio frequency protection in the overall security strategy for IoT networks. A multi-level approach to cybersecurity—from the physical level to applications—is a prerequisite for infrastructure resilience. SDR tools have proven to be a flexible and affordable way to analyze threats and test vulnerabilities. The scientific contribution of this study consists in developing an accessible and reproducible SDR-based method for assessing ZigBee's physical-layer resilience. The practical value lies in the possibility of using this approach for testing smart home and smart city devices before deployment in real environments. The experiment confirmed that even using a simple signal generated by SDR (HackRF + GNU Radio) tools, it is possible to effectively disrupt the operation of a real ZigBee network. The data recorded in the mobile application provides independent confirmation of the successful attack and its consequences at the user interaction level. The results of the study are relevant for developers, researchers, and operators of systems working with wireless IoT technologies.

8. Acknowledgment

This research has been funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No.BR24992852 "Intelligent models and methods of Smart City digital ecosystem for sustainable development and the citizens" quality of life improvement”).

Authors' Contributions: the authors' contribution is equal.

References

1 Arora A., Jain A., Yadav D., Hassija V., Chamola V., Sikdar B. Next Generation of Multi-Agent Driven Smart City Applications and Research Paradigms// IEEE Open Journal of the Communications Society - 2023 - No.4 - P.2104–2121. DOI: https://doi.org/10.1109/ojcoms.2023.3310528.

2 Houssein E. H., Othman M. A., Mohamed W. M., Younan M. Internet of Things in smart cities: Comprehensive review, open issues, and challenges// IEEE Internet of Things Journal - 2024 - No.11(21) - P.34941–34952. DOI: https://doi.org/10.1109/JIOT.2024.3449753.

3 Yang A., Zhang C., Chen Y., Zhuansun Y., Liu H. Security and privacy of smart home systems based on the Internet of Things and stereo matching algorithms// IEEE Internet of Things Journal - 2020 - No.7(4) - P.2521–2530. DOI: https://doi.org/10.1109/JIOT.2019.2946214.

4 Yang J., Sun L. A comprehensive survey of security issues of smart home system: “Spear” and “Shields,” theory and practice// IEEE Access - 2022 - No.10 - P.124167–124192. DOI: https://doi.org/10.1109/ACCESS.2022.3224806.

5 Sivapriyan R., Sushmitha S. V., Pooja K., Sakshi N. Analysis of security challenges and issues in IoT enabled smart homes// In 2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), IEEE - 2021 - pp. 1–6. DOI: https://doi.org/10.1109/CSITSS54238.2021.9683324.

6 Eltholth A. A. Improved spectrum coexistence in 2.4 GHz ISM band using optimized chaotic frequency hopping for Wi-Fi and Bluetooth signals// Sensors - 2023 - No.23(11) - P.5183. DOI: https://doi.org/10.3390/s23115183.

7 Joosens D. et al. Software-defined radio-based Internet of Things communication systems: an application for the DASH7 Alliance Protocol// Applied Sciences – 2025 – Vol.15. – №. 1. – P.1-34.

8 Wang X., Hao S. Don't Kick Over the Beehive// Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security - 2022 - P.2857–2870. DOI: https://doi.org/10.1145/3548606.3560703.

9 Cayre R., Galtier F., Auriol G., Nicomette V., Kaâniche M., Marconato G. WazaBee: Attacking ZigBee networks by diverting Bluetooth Low Energy chips// In 2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), IEEE - 2021 - pp. 376–387. DOI: https://doi.org/10.1109/DSN48987.2021.00049.

10 Pan T. ZigBee Wireless Network Attack and Detection// Advances in Artificial Intelligence and Security - 2021 - P.391–403. DOI: https://doi.org/10.1007/978-3-030-78621-2_32.

11 Allakany A., Elsisi M., Soliman M., Wang H. Enhancing security in ZigBee wireless sensor networks: A new approach and mutual authentication scheme for D2D communication// Sensors - 2023 - No.23(12) - P.5703. DOI: https://doi.org/10.3390/s23125703.

12 Sokolov V., Skladannyi P., Korshun N. ZigBee Network Resistance to Jamming Attacks// 2023 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo) - 2023 - P.161–165. https://doi.org/10.1109/ukrmico61577.2023.10380360.

13 Akestoridis D.G., Tague P. HiveGuard: A network security monitoring architecture for Zigbee networks// In 2021 IEEE Conference on Communications and Network Security (CNS), IEEE - 2021 - pp. 209-217.

14 Calderon L., Salvador G.T. Detection and Analysis of Flipper Zero Deauthentication Signals Using HackRF One Software-Defined Radio// 2024 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), IEEE – 2024. – P. 798-804.

15 Dini M.T., Sokolov V. Penetration tests for Bluetooth Low Energy and ZigBee using the software-defined radio// arXiv preprint arXiv:1902.08595 - 2019. DOI: https://arxiv.org/abs/1902.08595.

16 Sugadev M., Kaushik M., Vijaykumar V., Ravi T. Implementation of NOAA Weather Satellite Receiver using HackRF-One SDR// In 2022 International Conference on Computer Communication and Informatics (ICCCI), IEEE - 2022 - pp. 1-4.

17 Pirayesh H., Zeng H. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey// IEEE communications surveys and tutorials - 2022 - No.24(2) - P.767-809.

18 Alrefaei F., Alzahrani A., Song H., Alrefaei S. A survey on the jamming and spoofing attacks on the unmanned aerial vehicle networks// In 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), IEEE - 2022 - pp. 1-7.

19 Sarker I. H., Khan A. I., Abushark Y. B., Alsolami F. Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions// Mobile Networks and Applications - 2023 - No.28(1) - P.296-312.

20 Mozaffariahrar E., Theoleyre F., Menth M. A survey of Wi-Fi 6: Technologies, advances, and challenges// Future Internet - 2022 - No.14(10) - P.293.

21 Gupta M., Singh S. A survey on the zigbee protocol, it's security in internet of things (iot) and comparison of zigbee with bluetooth and wi-fi// In Applications of artificial intelligence in engineering: proceedings of first global conference on artificial intelligence and applications (GCAIA 2020) - Singapore: Springer Singapore - 2021 - pp. 473-482.

22 Yang X., Shu L., Liu Y., Hancke G., Ferrag M., Huang K. Physical security and safety of IoT equipment: A survey of recent advances and opportunities// IEEE Transactions on Industrial Informatics - 2022 - No.18(7) - P.4319-4330.

23 Jahangeer A., Bazai S., Aslam S., Marjan S., Anas M., Hashemi S. A review on the security of IoT networks: From network layer's perspective// IEEE Access - 2023 - Vol.11 - P.71073-71087.

24 Mishra N., Pandya S. Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review// IEEE Access - 2021 - No.9 - P.59353-59377.

SDR көмегімен ақылды ортада Zigbee байланыс қауіпсіздігін талдау

Т. Жукабаева[1], А. Адамова[2], Ж. Боранбай[3], Е. Бенкалифа [4], Е. Марденов[5]

[1,2,3] Astana IT University, Мәңгілік Ел даңғылы 55/11, Астана, 010000, Қазақстан
[4] Киберқауіпсіздікті зерттеу орталығы, Стаффордшир университеті, Leek Road көшесі ST4 2DF, Сток он Трент, Ұлыбритания
[5] Астана Халықаралық университеті, Қабанбай батыр даңғылы 8, Астана қ., 010000, Қазақстан

Аннотация. Ақылды қалалардың дамуы Zigbee хаттамасына негізделген сымсыз желілерді кеңінен енгізумен қатар жүреді, оның энергия тиімділігі мен заттар интернетінің архитектурасымен үйлесімділігі бар. Алайда, бұл хаттаманы ашық радио ортада белсенді пайдалану рұқсат етілмеген радиоэлектрондық әсерге байланысты тәуекелдердің артуына әкеледі. Бұл зерттеудің мақсаты ZigBee желілерінің бағдарламалық құралмен анықталған радионы пайдалана отырып, сигналды бағытталған өшіруге осалдығын эксперименттік бағалау болып табылады. Жұмыста нақты құрылғылармен сынақ ортасын дайындау кезеңдері, белсенді деректер арнасын анықтау және hackrf платформасы, SDR платформасы мен GNU radio ортасы арқылы тондық кедергілерді құру ұсынылған. Жүргізілген эксперимент белгілі бір жиілікке ұшыраған кезде пакеттердің 95% дейін жоғалатынын көрсетті, бұл желіні жұмыс істеуге жарамсыз етеді. Нәтижесінде ZigBee хаттамасының физикалық деңгейдегі маңызды осалдығын растайды және сымсыз IoT желілері үшін, әсіресе қалалық инфрақұрылым жағдайында қосымша қорғаныс механизмдерін әзірлеу қажеттілігін көрсетеді. Ұсынылған әдіс қолданбалы сценарийлерде құрылғылардың қауіпсіздігін тексеру үшін және сыртқы шабуылдарға төзімділікті бақылау жүйелерін құру кезінде қолданыла алады.

Түйін сөздер: ZigBee, SDR, HackRF, GNU радиосы, кептелу, радио кедергілері, ақпараттық қауіпсіздік, IoT.

Анализ безопасности связи ZigBee в умной среде с помощью SDR

Т. Жукабаева[1] **, А. Адамова**[2] **, Ж. Боранбай**[3] **, Е. Бенкалифа** [4] **, Е. Марденов**[5]

[1,2,3] Astana IT University, проспект Мәңгілік ел 55/11, г. Астана, 010000, Казахстан
[4] Центр исследований кибербезопасности, Стаффордширский университет, улица Leek Road ST4 2DF, Сток он Трент, Великобритания
[5] Международный университет Астана, проспект Кабанбай батыра 8, г. Астана, 010000, Казахстан

Аннотация. Развитие умных городов сопровождается широким внедрением беспроводных сетей, построенных на протоколе ZigBee, благодаря его энергоэффективности и совместимости с архитектурой интернета вещей. Однако активное использование данного протокола в открытой радиосреде приводит к возрастанию рисков, связанных с несанкционированным радиоэлектронным воздействием. Цель настоящего исследования заключается в экспериментальной оценке уязвимости ZigBee-сетей к направленному глушению сигнала с использованием программно-определяемого радио. В работе представлены этапы подготовки тестовой среды с реальными устройствами, определение активного канала передачи данных и генерация тональной помехи с помощью SDR-платформы HackRF One и среды GNU Radio. Проведённый эксперимент показал, что при воздействии на определённую частоту теряется до 95% пакетов, что делает сеть непригодной для функционирования. Полученные результаты подтверждают критическую уязвимость ZigBee-протокола на физическом уровне и подчёркивают необходимость разработки дополнительных механизмов защиты для беспроводных IoT-сетей, особенно в условиях городской инфраструктуры. Предложенная методика может быть использована для тестирования защищённости устройств в прикладных сценариях и при создании систем мониторинга устойчивости к внешним атакам.

Ключевые слова: ZigBee, SDR, HackRF, GNU Radio, глушение, радиопомехи, информационная безопасность, IoT.

References

1 Arora A., Jain A., Yadav D., Hassija V., Chamola V., Sikdar B. Next Generation of Multi-Agent Driven Smart City Applications and Research Paradigms, IEEE Open Journal of the Communications Society. 2023. No.4. P.2104–2121. DOI: https://doi.org/10.1109/ojcoms.2023.3310528.

2 Houssein E. H., Othman M. A., Mohamed W. M., Younan M. Internet of Things in smart cities: Comprehensive review, open issues, and challenges, IEEE Internet of Things Journal. 2024. No.11(21). P.34941–34952. DOI: https://doi.org/10.1109/JIOT.2024.3449753.

3 Yang A., Zhang C., Chen Y., Zhuansun Y., Liu H. Security and privacy of smart home systems based on the Internet of Things and stereo matching algorithms, IEEE Internet of Things Journal. 2020. No.7(4). P.2521–2530. DOI: https://doi.org/10.1109/JIOT.2019.2946214.

4 Yang J., Sun L. A comprehensive survey of security issues of smart home system: “Spear” and “Shields,” theory and practice, IEEE Access. 2022. No.10. P.124167–124192. DOI: https://doi.org/10.1109/ACCESS.2022.3224806.

5 Sivapriyan R., Sushmitha S. V., Pooja K., Sakshi N. Analysis of security challenges and issues in IoT enabled smart homes, In 2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), IEEE. 2021. pp. 1–6. DOI: https://doi.org/10.1109/CSITSS54238.2021.9683324.

6 Eltholth A. A. Improved spectrum coexistence in 2.4 GHz ISM band using optimized chaotic frequency hopping for Wi-Fi and Bluetooth signals, Sensors. 2023. No.23(11). P.5183. DOI: https://doi.org/10.3390/s23115183.

7 Joosens D. et al. Software-defined radio-based Internet of Things communication systems: an application for the DASH7 Alliance Protocol, Applied Sciences. 2025. Vol.15. №1.P.1-34.

8 Wang X., Hao S. Don’t Kick Over the Beehive, Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. 2022. P.2857–2870. DOI: https://doi.org/10.1145/3548606.3560703.

9 Cayre R., Galtier F., Auriol G., Nicomette V., Kaâniche M., Marconato G. WazaBee: Attacking ZigBee networks by diverting Bluetooth Low Energy chips, In 2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), IEEE. 2021. pp. 376–387. DOI: https://doi.org/10.1109/DSN48987.2021.00049.

10 Pan T. ZigBee Wireless Network Attack and Detection, Advances in Artificial Intelligence and Security. 2021. P.391–403. DOI: https://doi.org/10.1007/978-3-030-78621-2_32.

11 Allakany A., Elsisi M., Soliman M., Wang H. Enhancing security in ZigBee wireless sensor networks: A new approach and mutual authentication scheme for D2D communication, Sensors. 2023. No.23(12). P.5703. DOI: https://doi.org/10.3390/s23125703.

12 Sokolov V., Skladannyi P., Korshun N. ZigBee Network Resistance to Jamming Attacks. 2023 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo). 2023. P.161–165. https://doi.org/10.1109/ukrmico61577.2023.10380360.

13 Akestoridis D.G., Tague P. HiveGuard: A network security monitoring architecture for Zigbee networks, In 2021 IEEE Conference on Communications and Network Security (CNS), IEEE. 2021. pp. 209-217.

14 Calderon L., Salvador G.T. Detection and Analysis of Flipper Zero Deauthentication Signals Using HackRF One Software-Defined Radio, 2024 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), IEEE. 2024. P. 798-804.

15 Dini M.T., Sokolov V. Penetration tests for Bluetooth Low Energy and ZigBee using the software-defined radio, arXiv preprint arXiv:1902.08595. 2019. DOI: https://arxiv.org/abs/1902.08595.

16 Sugadev M., Kaushik M., Vijaykumar V., Ravi T. Implementation of NOAA Weather Satellite Receiver using HackRF-One SDR. In 2022 International Conference on Computer Communication and Informatics (ICCCI), IEEE. 2022. pp. 1-4.

17 Pirayesh H., Zeng H. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey, IEEE communications surveys and tutorials. 2022. No.24(2). P.767-809.

18 Alrefaei F., Alzahrani A., Song H., Alrefaei S. A survey on the jamming and spoofing attacks on the unmanned aerial vehicle networks, In 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), IEEE. 2022. pp. 1-7.

19 Sarker I. H., Khan A. I., Abushark Y. B., Alsolami F. Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. Mobile Networks and Applications. 2023. No.28(1). P.296-312.

20 Mozaffariahrar E., Theoleyre F., Menth M. A survey of Wi-Fi 6: Technologies, advances, and challenges. Future Internet. 2022. No.14(10). P.293.

21 Gupta M., Singh S. A survey on the zigbee protocol, it's security in internet of things (iot) and comparison of zigbee with bluetooth and wi-fi. In Applications of artificial intelligence in engineering: proceedings of first global conference on artificial intelligence and applications (GCAIA 2020) - Singapore: Springer Singapore. 2021. pp. 473-482.

22 Yang X., Shu L., Liu Y., Hancke G., Ferrag M., Huang K. Physical security and safety of IoT equipment: A survey of recent advances and opportunities. IEEE Transactions on Industrial Informatics. 2022. No.18(7). P.4319-4330.

23 Jahangeer A., Bazai S., Aslam S., Marjan S., Anas M., Hashemi S. A review on the security of IoT networks: From network layer's perspective. IEEE Access. 2023. Vol.11. P.71073-71087.

24 Mishra N., Pandya S. Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. IEEE Access. 2021. No.9. P.59353-59377.

Information about authors:

Tamara Kokenovna Zhukabaeva – PhD, professor, Astana IT University, Mangilik El ave. 55/11, Astana, 010000, Kazakhstan.

Aigul Duysenbinovna Adamova – Corresponding author, PhD, associate Professor, Astana IT University, Mangilik El ave. 55/11, Astana, 010000, Kazakhstan.

Zhandos Boranbay – Senior Lecturer, School of Cybersecurity, Astana IT University, Mangilik El ave. 55/11, Astana, 010000, Kazakhstan.

Elhadj Benkhelifa – PhD, professor, Cybersecurity Research Centre, Staffordshire University, Leek Road site ST4 2DF, Stoke-on-Trent, United Kingdom.

Yerik Mardenov – Astana International University, Kabanbay batyr ave. 8, Astana, 010000, Kazakhstan.

Жукабаева Тамара Кокеновна – PhD, профессор, Astana IT University, Мәнгілік Ел даңғылы 55/11, Астана қ., 010000, Қазақстан.

Адамова Айгуль Дюсенбиновна – Байланыс үшін автор, PhD, қауымдастырылған профессор, Astana IT University, Мәнгілік Ел даңғылы 55/11, Астана қ., 010000, Қазақстан.
Боранбай Жандос – "Киберқауіпсіздік" мектебінің аға оқытушысы, Astana IT University, Мәнгілік Ел даңғылы 55/11, Астана қ., 010000, Қазақстан.
Бенкалифа Елхадж – PhD, профессор, Киберқауіпсіздікті зерттеу орталығы, Стаффордшир университеті, Leek Road көшесі ST4 2DF, Сток он Трент, Ұлыбритания.
Марденов Ерик – Астана Халықаралық университеті, Қабанбай батыр даңғылы 8, Астана қ., 010000, Қазақстан.

Received: 30.07.2025. Revised: 21.09.2025.

Approved: 25.09.2025. Available online: 30.09.2025.