Resistance to Replay Attacks of Remote Control Protocols using the 433 MHz Radio Channel

Olha Mykhaylova[1], Artem Stefankiv[1], Taras Nakonechny[1], Taras Fedynyshyn[1], and Volodymyr Sokolov[2]

[1] *Lviv Polytechnic National University, 12 Stepan Bandera str., Lviv, 79000, Ukraine*
[2] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*

Abstract

This study focuses on the analysis of replay attacks, which pose a significant risk to remote control systems using the 433 MHz radio frequency band. A replay attack occurs when an attacker intercepts communications between two legitimate parties and resends the intercepted data to activate a remotely controlled system or commit identity theft. Special attention is paid to the study of the EV1527 protocol and its structure, as well as potential vulnerabilities that can be exploited by attackers. The study includes a detailed analysis of the design documentation on modules using the EV1527 protocol, as well as an assessment of the characteristics of the corresponding antennas and the features of working with hardware and software. The work also includes a comparative analysis of the technical means that can be used to carry out the attack and a demonstration of a practical attack using the HackRF One software-controlled transceiver in a laboratory setting. The main goal of the work is to demonstrate the mechanisms for implementing a replay attack on remote control systems with static code and to develop recommendations for improving the security of these systems. The results of the study are aimed at increasing the understanding of potential risks and vulnerabilities, as well as at determining the feasibility of using such protocols in modern physical security and access control systems.

Keywords

Radio channel, interception, replay, physical security, PT2262, HackRF One, EV1527, NanoVNA V2.2.

1. Introduction

Remote control systems are an important part of modern security solutions, providing convenience and efficiency in managing physical perimeters—from barriers and automatic gates to alarm systems. However, radio communications, which are often the backbone of these systems, can become vulnerable, opening the door to potential attacks [1, 2]. Particular attention in this context is paid to the vulnerability of remote-control protocols, particularly EV1527, which can be used to implement signal replay attacks [3–5].

In this work, we focus on analyzing these vulnerabilities, using both theoretical and practical methods to demonstrate possible attacks in a laboratory setting. The importance of such research lies in the increasing reliance on wireless technologies in security systems, making them a potential target for attackers and reflecting the need to develop more robust security protocols [6–8].

The motivation for this research was the numerous cases of replay attacks highlighting the vulnerability of existing systems. Our goal is not only to identify and demonstrate vulnerabilities but also to develop recommendations for improving the security

CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2024, Kyiv, Ukraine
EMAIL olha.o.mykhailova@lpnu.ua (O. Mykhaylova); artem.stefankiv.kb.2020@lpnu.ua (A. Stefankiv); t@online.ua (T. Nakonechny); fedynyshyn.taras@gmail.com (T. Fedynyshyn); v.sokolov@kubg.edu.ua (V. Sokolov)
ORCID: 0000-0002-3086-3160 (O. Mykhaylova); 0009-0006-8851-8358 (A. Stefankiv); 0009-0003-4487-9424 (T. Nakonechny); 0009-0006-8233-8057 (T. Fedynyshyn); 0000-0002-9349-7946 (V. Sokolov)

of using remote control systems. To do this, we conducted a detailed analysis of the documentation of the EV1527 and PT2262 protocols and studied the principles of their operation, message structure, and data modulation. A comparative analysis of equipment capable of carrying out such attacks was also carried out, including the software-controlled HackRF One transceiver and the NanoVNA V2.2 vector network analyzer [8–10].

It is important to note that the development of remote-control technology has deep roots in history. From early host and wireless systems developed in the late 19th century to meet the control needs of autonomous vehicles, including torpedoes, to modern wireless devices that are an integral part of our daily lives. For example, in the late 1930s, Philco pioneered a wireless remote controller for consumer electronic devices, known as Mystery Control, which used low-frequency radio transmission. This was a significant breakthrough in remote control technology. Another good example could be a set of modern wearable [12] Bluetooth-connected devices, which are also used as a part of a Smart-home setup and may execute remote control functions.

Also, a significant step forward in the development of remote-control technology was the creation of the first television remote control by Zenith Radio Corporation in 1950. It was originally connected to the TV using a wire, but in 1955 the “Flashmatic” wireless remote was developed, which controlled the TV using directional flashes of light [13, 14].

The structure of the work includes a literature review, methodology, analysis results, comparative study, and discussion of the results. We hope that this work will not only highlight current challenges in remote control security but also contribute to the development of safer solutions in this area.

2. Analysis of Recent Research and Publications

Current research in the field of security of remote control and keyless entry protocols emphasizes the use of dynamic codes, especially focusing on the HCS301 protocol. This protocol is used in keyless entry systems for vehicles, including car alarms and car starting systems. One of the key features of the HCS301 is the use of a patented KeeLoq block cipher based on a nonlinear feedback shift register, which provides a high level of security.

One of the important studies conducted by Tobias van Capelleven from Radboud University Nijmegen is devoted to a comparative analysis of the security of car alarm systems based on the EV1527 protocol. In his work, van Capelleven highlights the vulnerability of EV1527 to replay attacks, which calls into question its reliability in a security context.

In addition, other sources, such as articles on the Yaoertai website, go into detail about the mechanisms and features of the HCS301 Rolling Code Technology. These articles provide information on the operation of the HCS301, its benefits, and applications in various fields including automotive and home security systems. Particular attention is paid to how HCS301 technology protects against various types of attacks, including protection against replay attacks.

This analysis of current research and publications highlights the importance of understanding the various security protocols and vulnerabilities that exist in modern remote control and keyless entry systems. They provide valuable information that can be used to improve the security of these systems [11].

3. Setting Objectives

The main goal of this study is an in-depth analysis of the EV1527 protocol, including its design, principles of operation, and potential vulnerabilities. The study involves a thorough review of the design documentation of the modules that use this protocol, as well as an analysis of the main characteristics of the antennas and the features of working with hardware and software.

The main tasks of the research include:

1. Analysis of the Design of the EV1527 Protocol: Studying the technical structure and main components of the protocol, as well as understanding its functionality and data transmission mechanisms.
2. Vulnerability Detection: Identifying potential weaknesses in the EV1527

protocol, including its susceptibility to replay attacks and other threats.

3. Comparative Analysis of Equipment: Evaluation and comparison of different types of equipment that can be used to carry out attacks on systems using the EV1527 protocol.
4. Practical Verification: Performing experiments and tests in laboratory conditions to verify theoretical conclusions and identify real system vulnerabilities.
5. Evaluation of Feasibility of Using the Protocol: Based on the received data and analysis, conclude the practicality and safety of using the EV1527 protocol in remote control systems.

The results of this study will provide valuable information on the reliability and security of the EV1527 protocol, which is critical for its application in security and remote-control systems. This research is expected to help developers and engineers in choosing the most secure and efficient solutions for their systems.

4. Analysis of EV1527 Protocol Documentation

EV1527 is a message encoder chip that uses the protocol of the same name and was developed by Silvan Chip Electronics Tech. Co. Ltd (PRC) [4]. This protocol and the microcircuit of the same name and its clones are used in systems for remote control of mechanisms, automation systems, control panels for "smart home" systems, self-made devices, etc. This widespread use is due to the relative cheapness of the microcircuit, the presence of a collision prevention mechanism, and the simplicity of the implementation of the receiver and transmitter. There are ready-made solutions based on this standard that can be easily integrated into the existing structure, including access control devices such as barriers, automatic gates, automatic shutters, etc.

The EV1527 chip is manufactured in DIP-8 and TSOP-8 packages and has four data inputs, one clock input, power inputs, and one code output that can be transmitted via radio. The main frequencies for communication are 433 MHz for European countries and 315 MHz for the USA and Canada. The available documentation shows a typical circuit for turning on a microcircuit with a radio transmitter [4, p. 3] (Fig.1).

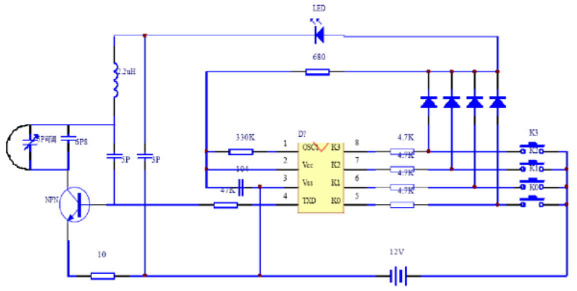
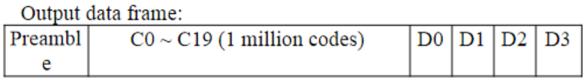


Figure 1: Typical wiring diagram of the EV1527 encoder chip

The protocol used by this chip is more resistant to overrun and collision attacks. The protocol provides for one type of message with a fixed structure. The message consists of a preamble and a main part (Fig. 2).


Output data frame:

Preambl e	C0 ~ C19 (1 million codes)	D0	D1	D2	D3

Figure 2: Structure of the EV1527 protocol message

The preamble is 32 bits long and is used to synchronize the transmitter and receiver. The structure of the preamble is as follows: one period of the dominant state and 31 periods of the recessive state at the output of the chip [4, p. 2] (Fig. 3).

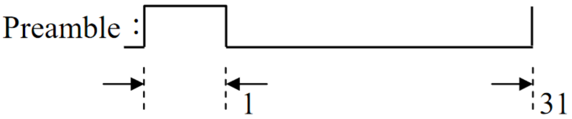


Figure 3: Structure of the message preamble

The main part of the message consists of a key code and four data bits. The main part of the message is coded using the sequences "3–1" (three periods in the dominant state and one period in the recessive state at the output of the microcircuit) to transmit a logical one and the inverted sequence "1–3" to transmit a logical zero [4, p. 2] (Fig. 4). Analogous coding is used in the microcircuit PT2262 [5, p. 7].

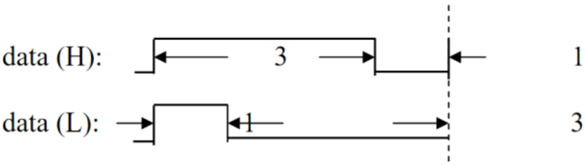


Figure 4: Coding at the output of the chip

The key code is specified in twenty bits, which allows for the existence of 1048576 unique keys and greatly complicates the execution of a traversal attack since it is necessary to go through not only the above number of key codes but also the 16 button codes used in the attacked system. The total number of combinations for a complete search is 16777216 messages.

However, this protocol uses static code and does not use cryptographic means to increase the level of security. The message does not change after each generation, so a replay attack is possible [3].

5. Comparative Analysis of EV1527 and PT2262 Protocols

This section provides a comparative analysis of two popular remote control protocols: EV1527 and PT2262. Both protocols are often used in remote control systems, but they have some key differences.

EV1527 is a chip developed by Silvan Chip Electronics Tech. Co. Ltd (PRC), which uses a fixed message format and does not have cryptographic protection. The protocol provides one type of message with a fixed structure, including a 32-bit preamble and a main part with a key code and four data bits. EV1527 uses a collision avoidance mechanism and is easy to implement.

PT2262, on the other hand, can have different message configurations from 6 to 12 bits of key code and 0 to 6 bits of button code. The protocol provides a synchronization sequence at the end of the message, which is a change from EV1527. PT2262 does not have built-in collision mitigation mechanisms and uses static addressing.

One key difference is that if a transmitter is lost, PT2262-based systems require a code change on the receiver and other transmitters to revoke the lost transmitter's access. The system based on EV1527 does not have this drawback, where you can revoke access by deleting the record of the lost transmitter from the receiver's memory.

In general, although both protocols lack cryptographic security and are vulnerable to replay attacks, EV1527 proves to be more flexible to use and adapt to different user needs. This makes it a more attractive choice for modern remote-control systems, despite existing vulnerabilities.

6. Principle of Replay Attack

A replay attack is a form of cyber-attack where an attacker intercepts communications between two legitimate parties and resends the intercepted data. This method is used to gain unauthorized access to a system or initiate unwanted actions on behalf of a legitimate user. Unlike a man-in-the-middle attack, where the attacker actively interferes with communication, a replay attack is passive.

The attack scenario can be described as follows (Fig. 5):

1. An attacker, whom we'll call Eve, listens to the radio frequency range in which the signal's receiver and transmitter operate and record the signal.
2. Alice sends a signal to Bob to activate a certain mechanism, such as opening an automatic gate.
3. Bob receives and decodes the signal, and if it matches the stored code, acts.
4. Eve replays the intercepted signal, and the system, vulnerable to a replay attack, perceives this as a signal from Alice and performs a response action.

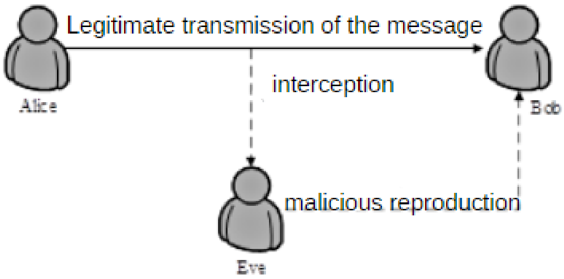


Figure 5: Replay attack scheme

At the same time, the attacker must have opportunities for passive interception and reproduction.

The importance of implementing stronger security mechanisms in these systems is becoming apparent to reduce the risks of unauthorized access or control.

To protect against replay attacks, remote control systems must incorporate additional layers of security, such as cryptographic encoding or the use of dynamic codes that change with each transmission. For example, the use of technologies similar to the HCS301 Rolling Code discussed earlier can significantly improve the security of remote-control systems.

A replay attack is particularly dangerous because it does not require the attacker to have deep technical knowledge or sophisticated equipment. The ease of implementation of such attacks makes them a threat to a wide range of wireless systems, from home automation systems to more sophisticated access control systems.

Understanding these risks and vulnerabilities is critical for security developers and hardware manufacturers. This research highlights the need to continuously update cybersecurity knowledge and develop more resilient and robust solutions to prevent similar attacks in the future.

7. Comparative Analysis of the Main Characteristics of Antennas for Signal Interception

Conducting a comparative analysis of the main characteristics of the antennas allows you to determine the suitability of each of the available antennas for signal interception and re-play and to identify their shortcomings and/or defects.

The existing receiver and transmitters use the LPD433 band (433.050 MHz—434.79 MHz), which is within the 70 cm radio amateur band (430 MHz—440 MHz).

The range of the LPD433 is divided into 69 channels with a step of 25 kHz, this range is used for low-power, short-range transmitters. Short-range transmitters include remote control systems, home automation systems, car keyless access systems, low-power portable walkie-talkies, etc. In Ukraine, the use of this range is regulated by DSTU ETSI EN 300 220-1:2018 and DSTU ETSI EN 300 220-2:2017, which is a harmonization of the standard ETSI EN 300 220-1 V3.2.1 [15] and ETSI EN 300 220-2 V3 .1.1 [16]. The limits of the range are determined by the recommendation document authored by CEPT/ERC Rec 70-03 [9]. In the USA, this range is not used for unlicensed broadcasting, so the Federal Communications Commission (FCC) allocated the 315 MHz range for short-term operation of short-range devices with a limit on the output electric field strength of 300 μV/m with a transmission duration of up to 3 minutes [11, with. 20].

The main requirement for antennas is the compliance of their operating frequency range with a given band with a minimum value of SWR.

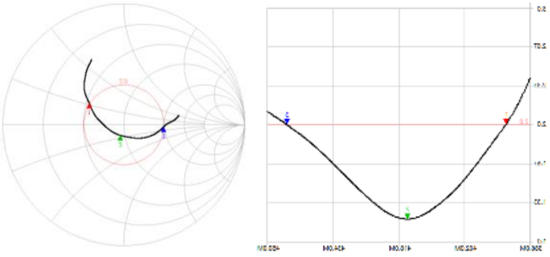
The portable electrical circuit analyzer NanoVNA [17] and the NanoVNA-Saver software [18] were used for the comparative analysis. Four types of antennas were compared according to the parameters of the standing wave coefficient and the operating frequency range. The limit value of SWR for determining the range of operating frequencies is 2.000.

The antennas were measured in vertical polarization and averaged over five consecutive measurements.

7.1. Antenna 1

Telescopic antenna with SMA connector, with a minimum length of 17 cm and a maximum length of 102 cm. The measurement was carried out in two antenna length configurations—minimum and maximum.

Below are the results of measuring the parameters of antenna 1 at the minimum length (Fig. 6, Table 1) and the maximum length (Fig. 7, Table 2).

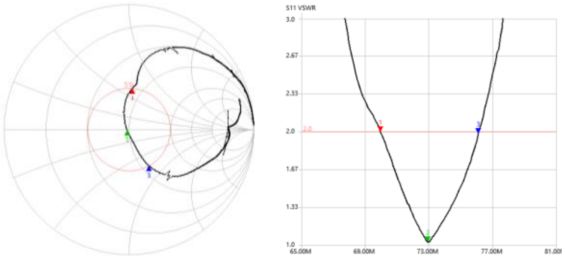


a) b)

Figure 6: Parameters of antenna 1 at the minimum length: (a) Smith chart and (b) frequency dependence graph

Table 1
Values of antenna 1 parameter at the minimum length in marks 1–3

	Mark 1	Mark 2	Mark 3
Frequency, MHz	391.966	415.851	445.286
SWR by voltage	2.000	1.191	2.000
Return losses. dB	−9.543	−1.213	−9.545
Impedance, Ohm	26.6–j10.8	46.9+j7.9	99.8+j3.3



a) b)

Figure 7: Parameters of antenna 1 at the maximum length: (a) Smith chart and (b) graph of dependence of SWR on frequency

Table 2
Values of antenna 1 parameter at maximum length in Mark 1–3

	Mark 1	Mark 2	Mark 3
Frequency, MHz	69.9772	72.9504	76.1219
SWR by voltage	1.996	1.021	1.977
Return losses, dB	–9.566	–39.615	–9.676
Impedance, Ohm	42.2–j31.	49.0+j0.1	57.1+j36.5

The obtained results indicate the suitability of antenna 1 at the minimum length for working with the target signal.

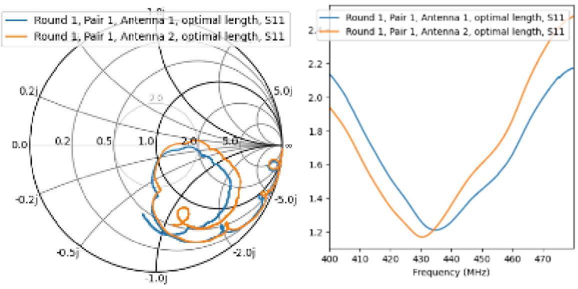
7.2. Antenna 2

Telescopic antenna with SMA connector, minimum length 11.5 cm and maximum length 47.5 cm. Four copies of this antenna are available. For each of the specimens, measurements were made in a length configuration that corresponds to a quarter of the wavelength of the target range (17.5 cm). Using the method of pairwise comparison, the specimen with the best characteristics was selected (Figs. 10–12). The minimum value of the standing wave coefficient in terms of voltage, the frequency at which the minimum value of CSC was reached, and the input resistance of the antenna at the frequency with the minimum CSC were chosen as the criteria for comparison. The comparison took place in two rounds, in the first two pairs of specimens (No. 1 and No. 2 and No. 3 and No. 4, respectively), were compared in the second round, and specimens with better characteristics from the previous rounds were compared.

Graphs were constructed using the sci-kit-of library for the Python programming language [10]. This library supports the creation and import of Touchstone save files, which are used in most circuit analyzers in the NanoVNA-Saver program.

Round 1.

A pair of copies No. 1 and No. 2 is compared. The results of the comparison are shown in Fig.8.



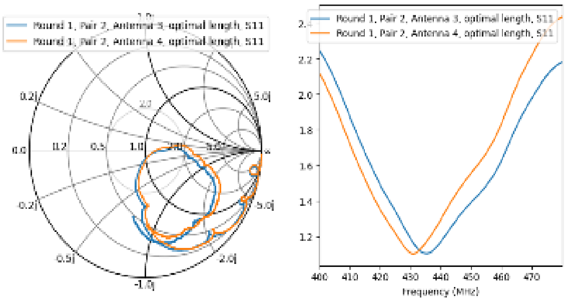
a) b)

Figure 8: Parameters of specimens No. 1 and No. 2 of antenna 2 at the optimal length: (a) Smith diagram and (b) graph of dependence of SWR on frequency.

In Fig. 8, we can see that the values of the wave resistance for both specimens on the SWR 1.0 line are quite close. Still, specimen No. 2 shows an additional resonance at a frequency of 882 MHz, uncharacteristic of specimen No. 1. Also, Fig. 8 demonstrates the superiority of instance #1 over instance #2 in the 430–440 MHz range. The minimum value of SWR of instance #2 is at the beginning of the range and reaches a value of 1.357 at the end of this range. Specimen No. 1 shows a slightly larger value of SWR of 1.208 at a frequency of 435.058 MHz.

From the conducted data analysis, it can be concluded that instance 2 shows the best indicators in this range.

A comparison of pair 2 (specimens #3 and #4) is shown in Fig. 9.



a) b)

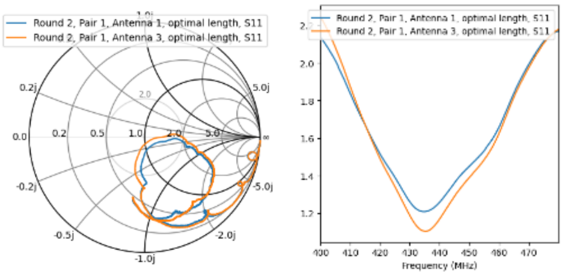
Figure 9: Parameters of instances 3 and 4 of antenna 2 at the optimal length: (a) Smith diagram and (b) graph of the dependence of CSC on frequency

In Fig. 10 we can observe that the values of the reactive component of the support for both instances on the SWR 1.0 line are quite close. Still, instance 2 demonstrates an additional resonance at a frequency of 882 MHz, which is uncharacteristic of instance 1.

Fig. 11 shows the advantage of Instance 1 over Instance 2 in the 430–440 MHz range. Instance 2's minimum SWR value is at the beginning of the range and reaches a value of 1.357 at the end of the range. Instance 1 exhibits a slightly higher SWR of 1.208 at 435.058 MHz.

From the data analysis, we can conclude that specimen 2 demonstrates the best performance in this range.

A comparison of Pair 2 (Instances №3 and №4) is shown in Figs. 12–13.



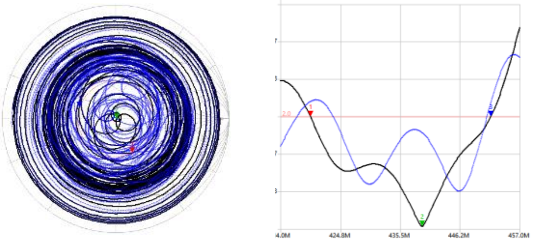
a) b)

Figure 10: Parameters of instances 1 and 3 of antenna 2 at optimal length: (a) Smith chart and (b) graph of SWR versus frequency

Considering the above similarity between the frequencies of the minimum SWR value and the corresponding values shown in Fig. 15, we can conclude that among the available ones, the best performance is demonstrated by specimen No. 3, and it is suitable for working with the target signal.

7.3. Antenna 3

The quad-band car antenna with PL-259 connector is part of the QYT KT-7900D car radio kit, which is designed to operate in the 136–174 MHz, 220–270 MHz, 350–390 MHz and 400-4 bands. The antenna is equipped with a magnetic stand with a SO-239 input connector and a 7-meter long SYWV 50-3 cable with a PL-259 connector. Below are the results of measuring the parameters of antenna 3 in the signal frequency range (Fig. 13, Table 3). Blue color indicates the measurement of parameters when connecting the antenna through the supplied magnetic stand, and black—is when connecting the antenna with a 5-meter-long RG-58U70 cable through an SMA-SO-239 adapter to the antenna.



a) b)

Figure 11: Antenna 3 parameters: (a) Smith chart and (b) graph of SWR versus frequency

From Fig. 11, it can be observed that the magnetic stand hurts the antenna performance. There is no SWR peak in the 440 MHz range declared by the manufacturer when using a magnetic stand.

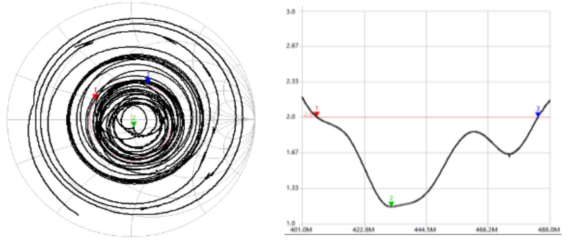
Table 3
Parameter values for antenna 3 without stand-in marks 1–3

	Mark 1	**Mark 2**	**Mark 3**
Frequency, MHz	419.373	439.469	451.821
SWR by voltage	1.998	1.022	1.999
Return losses, dB	−9.552	−39.356	−9.551
Impedance, Ohm	54.9–j36.7	51.0–j0.3	25.5+j5.7

The results indicate that this antenna can handle the target signal, but its performance will be less optimal than that of Antenna 2.

7.4. Antenna 4

A "Ground plane" antenna with a BNC connector and a complete BNC-SMA cable of RG-174 type, 3 meters long, the range declared by the manufacturer is 65–375 MHz. The antenna consists of a printed circuit board on which BNC connectors are fixed for the output and input of the central element and holes for four grounding elements, made in the form of telescopic antennas with a length of 20 to 95 cm. Experimentally, it was possible to tune this antenna to the target range (length of the central element—47.5 cm, length of grounding elements—51.5 cm). The antenna was mounted on a homemade mast at a height of approximately 175 cm from the floor level. Below are measurements of this antenna in the above optimal configuration (Fig. 12, Tab.4).



a) b)

Figure 12: Parameters of antenna 4 at optimal length: (a) Smith chart and (b) graph of SWR versus frequency

Table 4
Values of the parameters of antenna 4 at the optimal length in marks 1–3

	Mark 1	Mark 2	Mark 3
Frequency, MHz	406.237	432.313	483.779
SWR by voltage	2.000	1.157	1.996
Return losses, dB	−9.545	−22.766	−9.566
Impedance, Ohm	26.4+j10.3	51.8–j7.2	53.6+j36.3

From the data obtained, we can conclude that this antenna is suitable for working with the target signal in this configuration, but stability of the parameters cannot be achieved due to the operation of the antenna outside the characteristics declared by the manufacturer and the calculated values of the length of the elements (for the range of 430–440 MHz, the length of the central element should be approximately 16.5 cm, and the length of the grounding elements is 18.3 cm) [11].

Therefore, for working with the target signal in laboratory conditions, the best performance is demonstrated by specimen No. 3 of antenna No. 2. To determine the stability of the indicators over time, a series of consecutive measurements were taken over 16 hours. Measurements were made at intervals of 2–2.5 hours.

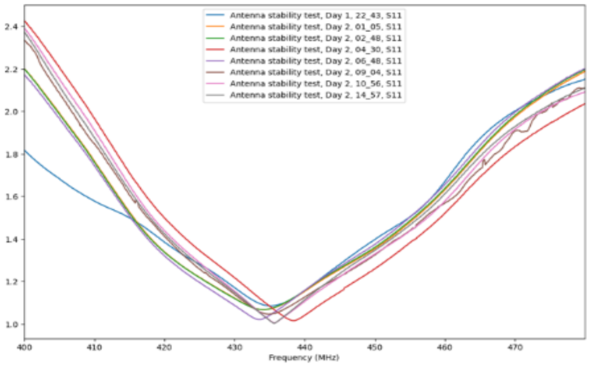


Figure 13: Testing the stability of performance over time

The measurement results are in the same range and do not go beyond the established range, limited by the SWR value of 2.000.

8. The process of performing a replay attack demonstration

In this chapter, we will focus on the detailed study and practical application of signal interception and replay techniques in wireless communication systems. Our goal is to explore and demonstrate how an attacker can use specialized hardware and software to intercept and imitate signals to illegally access or control systems. This process, known as a replay attack, is a key element in studying wireless security and developing effective countermeasures [3–5, 9, 15, 16].

Equipment:

- Signal transmitters.
- Signal receiver with actuator.
- Transceiver with software control HackRF One.
- USB 2.0 A—USB 2.0 Micro-B cable.
- Antenna and connecting cables with adapters.
- Computer running Kali Linux.
- Radiofrequency spectrum analyzer gqrx [9].
- Universal Radio Hacker software package for reverse engineering of wireless protocols [19].

Description of equipment:

1. Signal transmitters: transmitter A is a miniature control transmitter with two buttons labeled A and B and an LED, black with silver accents, powered by a 23A cell; transmitter B is a miniature control transmitter with four buttons marked A, B, C, D, and LED, silver color with protective cover, powered by a 23A element.
2. Signal receiver with actuator—developed by JoyDeal, a compact receiver and command decoder of EV1527 and PT2262 standards with a memory for 15 buttons and a standard helical antenna. The supply voltage ranges from 3.6 to 24 V; an LED with a limiting resistor is used as an actuator.
3. HackRF One software-controlled transceiver—portable transceiver with software control HackRF One in the PortaPack H1 version with the ability to operate autonomously. The transceiver has connectors for connecting an antenna, a built-in oscillator output, and a synchronization input, as well as a USB

Micro-B power/data connector and a 3.5 mm TRS connector for connecting headphones and outputting a demodulated audio signal.

4. USB 2.0 A to USB 2.0 Micro-B cable—data cable with USB 2.0 A and USB 2.0 Micro-B connectors, 1 meter long.
5. Antenna and connecting cables with adapters—instance 3 of antenna 2 was selected as the working antenna; the comparative analysis process is described in paragraph 7. Adapters and connecting cables are not used.
6. Computer running Kali Linux—Asus Vivo book 15 X509FJ laptop with Kali Linux 2024.1 special purpose operating system installed. A description of the procedure for preparing a computer to perform an attack is given below.

Attack Sequence:

- The attacker starts intercepting the signal using Universal Radio Hacker and waits for the legitimate user (victim) to send a signal.
- A legitimate user sends a signal.
- The receiver performs the specified action.
- An attacker, using Universal Radio Hacker, sends a signal imitating a legitimate user of the system (victim).
- The receiver performs the specified action because it cannot distinguish an attacker from a legitimate user.

Performing an attack:

1. System preparation. To prepare the system to work with HackRF One, you need to install the hackrf, hackrf-doc, hackrf-firmware, libhackrf-dev, libhackrf0 packages from the operating system's package manager repositories.

2. Receiver programming. Programming the receiver occurs by pressing the programming button a certain number of times to switch to the required switching mode (instant, switching, latching, timer) and pressing the desired button on the transmitter. As previously noted, the receiver memory has 15 cells. The following positions have been programmed:

2.1. Button A of transmitter A to instantaneous mode.

2.2. Button B of the transmitter to switch mode.

2.3. Button A of transmitter B to timer mode with a delay of 5 seconds.

3. Assessing the radio frequency range and checking signal reception.

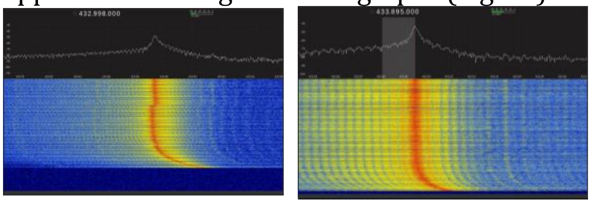
The radio frequency spectrum is estimated using gqrx [20].

Gqrx is a program for real-time radio frequency spectrum analysis, distributed under the open GPL license [9].

Execution order:

- Connect an antenna to HackRF One and connect it to a computer.
- Switch HackRF One to computer mode.
- Launch gqrx on your computer.
- Select HackRF One from the list of devices and establish a connection.
- Set the receiving frequency to 433.92 MHz.
- Enable monitoring.

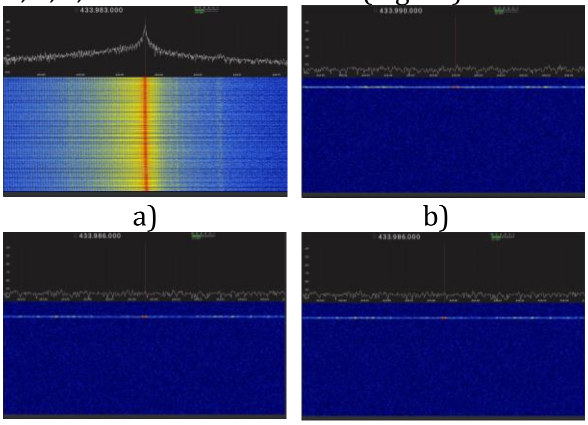
A waterfall graph and a line graph of the signal will appear on the screen. When you press the buttons on transmitter A, we observe the appearance of a signal on the graphs (Fig. 14).



a) b)

Figure 24: Waterfall graphs of transmitter A button signals a) button A; b) button B

We will carry out a similar procedure for buttons A, B, C, and D of transmitter B (Fig. 15):



a) b)

c) d)

Figure 35: Waterfall graphs of transmitter B button signals: (a) button A; (b) button B; (c) button C and (d) button D

From the data obtained, we can conclude that the connection and configuration of the transceiver and computer are correct, and assume that transmitter B is partially operational or does not have the declared functions. Signals from buttons that do not transmit a signal (buttons B, C, and D of transmitter B) are not considered further.

4. Signal interception and analysis.

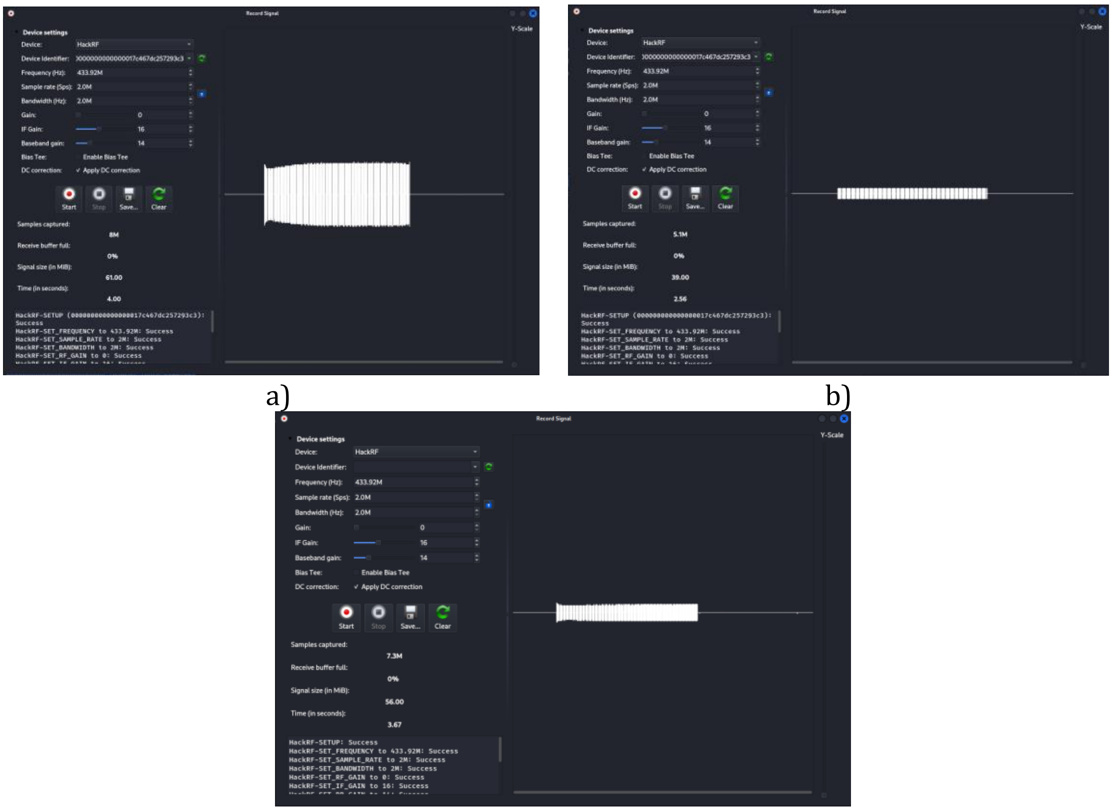
To intercept and analyze the signal, the Universal Radio Hacker software package is used [19]. This software package has the capabilities to record signals, analyze them, reverse engineer wireless protocols, play back recorded signals, and create new signals based on arbitrary data. This software package is written in Python and is distributed under the free license GPLv3. Installation is done using the pipx package manager.

Execution order:

- Connect an antenna to HackRF One and connect it to a computer.
- Switch HackRF One to computer mode.
- In the File menu, select Record signal.
- Select HackRF One from the list of available devices.
- Click the update button, which is located opposite the "Device Identifier" field, and wait for the serial number to appear in the field.
- Set the interception frequency to 433.92 MHz.
- Press the "Start" button.
- Wait for the signal to arrive.
- After recording the signal, press the "Stop" button.
- Save the signal to a file using the Save button.
- Close the recording window, the saved signal will automatically open in the main program window.

Signals from transmitters A and B, recognized by the JoyDeal receiver (buttons A and B of transmitter A and button A of transmitter B) were intercepted (Fig. 16) and interpreted (Fig. 17).

The signal was intercepted with a configured transceiver bandwidth of 2.0 MHz and a scanning frequency of 2 million samples per second.



Device settings
Device: HackRF
Device Identifier: 000000000000000017c467dc257293c3
Frequency (Hz): 433.92M
Sample rate (Sps): 2.0M
Bandwidth (Hz): 2.0M
Gain: 0
IF Gain: 16
Baseband gain: 14
Bias Tee: Enable Bias Tee
DC correction: ✓ Apply DC correction
Samples captured: 8M
Receive buffer full: 0%
Signal size (in MiB): 61.00
Time (in seconds): 4.00

```
HackRF-SETUP (000000000000000017c467dc257293c3):
Success
HackRF-SET_FREQUENCY to 433.92M: Success
HackRF-SET_SAMPLE_RATE to 2M: Success
HackRF-SET_BANDWIDTH to 2M: Success
HackRF-SET_RF_GAIN to 0: Success
```

a)

Device settings
Device: HackRF
Device Identifier: 000000000000000017c467dc257293c3
Frequency (Hz): 433.92M
Sample rate (Sps): 2.0M
Bandwidth (Hz): 2.0M
Gain: 0
IF Gain: 16
Baseband gain: 14
Bias Tee: Enable Bias Tee
DC correction: ✓ Apply DC correction
Samples captured: 5.1M
Receive buffer full: 0%
Signal size (in MiB): 39.00
Time (in seconds): 2.56

```
HackRF-SETUP (000000000000000017c467dc257293c3):
Success
HackRF-SET_FREQUENCY to 433.92M: Success
HackRF-SET_SAMPLE_RATE to 2M: Success
HackRF-SET_BANDWIDTH to 2M: Success
HackRF-SET_RF_GAIN to 0: Success
```

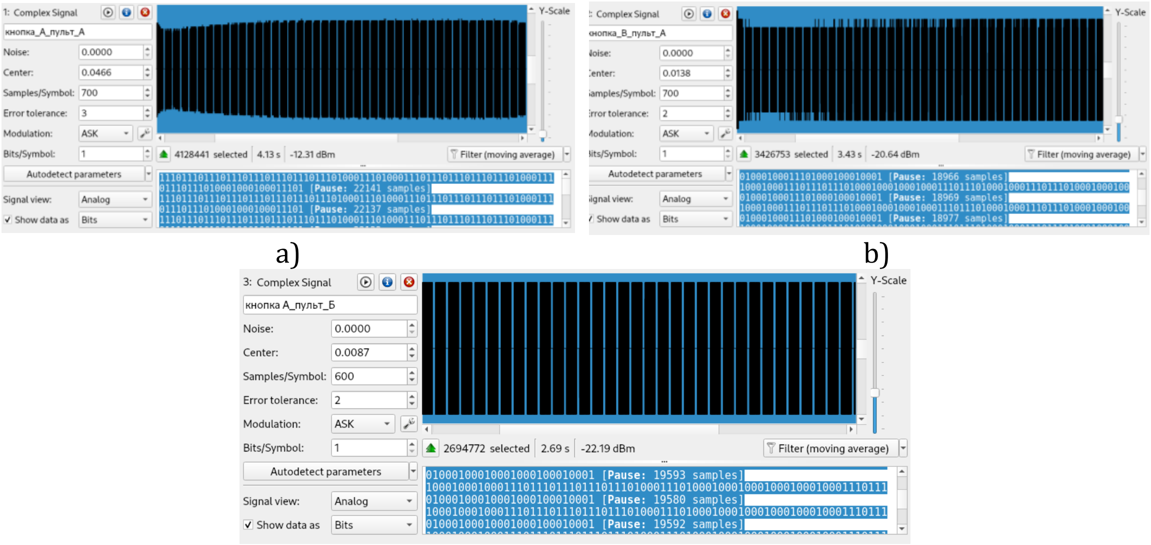
b)

Device settings
Device: HackRF
Device Identifier:
Frequency (Hz): 433.92M
Sample rate (Sps): 2.0M
Bandwidth (Hz): 2.0M
Gain: 0
IF Gain: 16
Baseband gain: 14
Bias Tee: Enable Bias Tee
DC correction: ✓ Apply DC correction
Samples captured: 7.3M
Receive buffer full: 0%
Signal size (in MiB): 56.00
Time (in seconds): 3.67

```
HackRF-SETUP: Success
HackRF-SET_FREQUENCY to 433.92M: Success
HackRF-SET_SAMPLE_RATE to 2M: Success
HackRF-SET_BANDWIDTH to 2M: Success
HackRF-SET_RF_GAIN to 0: Success
HackRF-SET_IF_GAIN to 16: Success
```

c)

Figure 46: Signal capture from transmitters: (a) button A of transmitter A; (b) button B of transmitter A and (c) button A of transmitter B



кнопка_А_пульт_А

Noise: 0.0000
Center: 0.0466
Samples/Symbol: 700
Error tolerance: 3
Modulation: ASK
Bits/Symbol: 1
Signal view: Analog
☑ Show data as Bits

4128441 selected | 4.13 s | -12.31 dBm

```
1110111011101110111011101110111010001110100011101110111011101110100011
0111011101000100010001110 1 [Pause: 22141 samples]
1110111011101110111011101110111010001110100011101110111011101110100011
0111011101000100010001110 1 [Pause: 22137 samples]
1110111011101110111011101110111010001110100011101110111011101110100011
```

a)

кнопка_B_пульт_A

Noise: 0.0000
Center: 0.0138
Samples/Symbol: 700
Error tolerance: 2
Modulation: ASK
Bits/Symbol: 1
Signal view: Analog
☑ Show data as Bits

3426753 selected | 3.43 s | -20.64 dBm

```
010001000111010001000100 01 [Pause: 18966 samples]
1000100011101110111010001000100010001110111010001000111011101000100010 0
010001000111010001000100 01 [Pause: 18969 samples]
1000100011101110111010001000100010001110111010001000111011101000100010 0
010001000111010001000100 01 [Pause: 18977 samples]
```

b)

кнопка А_пульт_Б

Noise: 0.0000
Center: 0.0087
Samples/Symbol: 600
Error tolerance: 2
Modulation: ASK
Bits/Symbol: 1
Signal view: Analog
☑ Show data as Bits

2694772 selected | 2.69 s | -22.19 dBm

```
0100010001000100010001 0001 [Pause: 19593 samples]
1000100010001110111011101110111010001110100010001000100010001000111011 1
0100010001000100010001 0001 [Pause: 19580 samples]
1000100010001110111011101110111010001110100010001000100010001000111011 1
0100010001000100010001 0001 [Pause: 19592 samples]
```

c)

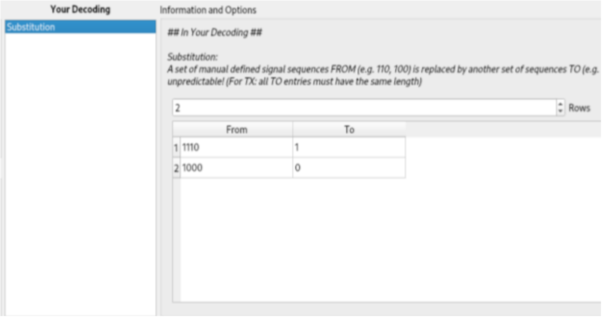
Figure 57: Interpretation of the transmitter signal: (a) button A of transmitter A; (b) button B of transmitter A and (c) button A of transmitter B

The intercepted signals use amplitude shift keying and are recorded at a resolution of 700 samples per symbol.

The PT2262 and EV1527 standards use the same bit encoding—"3–1" to encode a logic one and "1–3" to encode a logic zero. At a resolution of 700 samples per symbol, these would be the sequences "1110" and "1000", respectively.

When adding these parameters to the Universal Radio Hacker analysis template (Fig. 18), we receive the following messages (Fig. 19):

- Button A of transmitter A—0xFF5F7 1 (11111111010111110111 0001) (Fig. 19, message 1).
- Button B of transmitter A—0x38860 8 (00111000100001100000 1000) (Fig. 19, message 47).
- Transmitter B Button A—0x1F40C 0 (00011111010000001100 0000) (Fig. 19, message 91).



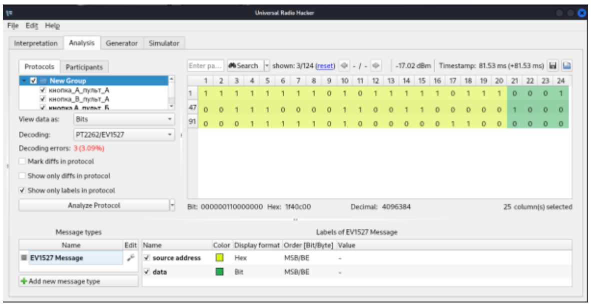
## In Your Decoding ##

Substitution:
A set of manual defined signal sequences FROM (e.g. 110, 100) is replaced by another set of sequences TO (e.g.
unpredictable! (For TX: all TO entries must have the same length)

2 Rows

	From	To
1	1110	1
2	1000	0

Figure 68: Signal encoding parameters



☑ New Group
☑ кнопка_А_пульт_А
☑ кнопка_B_пульт_A
☑ кнопка А пульт Б

View data as: Bits
Decoding: PT2262/EV1527
Decoding errors: 3 (3.09%)
□ Mark diffs in protocol
□ Show only diffs in protocol
☑ Show only labels in protocol

shown: 3/124 (reset) -17.02 dBm Timestamp: 81.53 ms (+81.53 ms)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	1	1	1	1	1	1	1	1	0	1	0	1	1	1	1	1	0	1	1	1	0	0	0	1
47	0	0	1	1	1	0	0	0	0	1	1	0	0	1	1	0	0	0	0	0	1	0	0	0
91	0	0	0	1	1	1	1	1	0	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0

Bit: 000000110000000 Hex: 1f40c00 Decimal: 4096384 25 column(s) selected

Name	Edit
EV1527 Message	

Labels of EV1527 Message

Name	Color	Display format	Order [Bit/Byte]	Value
☑ source address	🟨	Hex	MSB/BE	-
☑ data	🟩	Bit	MSB/BE	-

Figure 79: Received messages (repeated messages hidden)

Additional storage is stored on 24 bits, indicating the use of the EV1527 protocol. The protocol consists of 20-bit transmission addresses and 4-bit mail, which is confirmed by the documentation [4, p. 2].

5. Signal opening.

To open a closed signal, a Universal Radio Hacker is also used, the procedure is below:

- Connect to HackRF One and recognize it from your computer.
- HackRF One in computer mode.
- Open the file with the useful signal.
- For interpretation tabs, click the open button.
- Change the view of the HackRF One seller and find out other connections of the seller (similarly to points 3–4 of the previous preparations).
- Repeat the selection of the number of transmission repetitions by half.
- Click the "Start" button.

As a result of the signal transmission, a signal programmed for the day was received.

9. Conclusions

In the modern world, where digital technologies penetrate all areas of our lives, the issue of security becomes very important. Remote control systems that use static codes are open to several potential threats, of which the replay attack is one of the simplest and most effective. This publication analyzes in detail the vulnerability of the EV1527 protocol, widely used in simple remote-control systems, to this type of attack. The laboratory study demonstrates how a replay attack can be carried out using specialized equipment, thereby confirming the critical vulnerability of the protocol.

The importance of this research cannot be overstated, as it highlights fundamental security flaws in static code-based systems. The conclusions we have reached provide a strong argument in favor of moving from using outdated technologies to more modern and secure solutions. Systems using dynamic codes, such as HCS301, provide a significantly higher level of security by using cryptographic data protection techniques that make such attacks difficult or even impossible.

However, the transition to safer technologies must be deliberate and systematic. It is necessary to consider not only the security of protocols but also the specifics of their application, the convenience of end users, and the cost of implementation. In some cases, the use of general-purpose or specialized protocols that include complex security mechanisms may be more appropriate. It is especially applicable to objects of critical infrastructure, which undoubtedly need to be well-protected and resilient from a cybersecurity perspective [21].

Considering the research conducted, it can be concluded that the security of remote-control systems is a critical aspect that requires immediate attention. The choice of equipment and technologies should be based not only on their effectiveness and ease of use but also on ensuring an adequate level of safety. The use of dynamic codes and cryptographic protocols is a key step towards increasing the security of remotely controlled systems from unauthorized access.

References

[1] M. TajDini, V. Sokolov, P. Skladannyi, Performing Sniffing and Spoofing Attack Against ADS-B and Mode S using Software Define Radio, in: IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (2021) 7–11. doi: 10.1109/UkrMiCo52950.2021.9716665.

[2] M. TajDini, V. Sokolov, V. Buriachok, Men-in-the-Middle Attack Simulation on Low Energy Wireless Devices using Software Define Radio, in: 8th International Conference on "Mathematics. Information Technologies. Education": Modern Machine Learning Technologies and Data Science, vol. 2386 (2019) 287–296.

[3] R. Banakh, A. Piskozub, Attackers' Wi-Fi Devices Metadata Interception for Their Location Identification, IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems 8525538 (2018)112–116. doi: 10.1109/IDAACS-SWS.2018.8525538.

[4] Building a Poor Man's Quarter-Wave 433MHz Antenna: Antenna's Construction, Element14. URL: https://community.element14.com/challenges-projects/project14/rf/b/blog /posts/building-a-poor-man-s-quarter-wave-433mhz-antenna-antenna-s-construction

[5] Small Range Radio Equipment Operating in the Frequency Range from 25 MHz to 1000 MHz, Part 1. Technical Characteristics and Test Methods, DSTU ETSI EN 300 220-1:2018 (2018).

[6] V. Sokolov, P. Skladannyi, N. Korshun, ZigBee Network Resistance to Jamming Attacks, in: IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics (2023) 161–165. doi: 10.1109/UkrMiCo61577.2023.10380360.

[7] V. Sokolov, P. Skladannyi, A. Platonenko, Jump-Stay Jamming Attack on Wi-Fi Systems, in: IEEE 18th International Conference on Computer Science and

Information Technologies (2023) 1–5. doi: 10.1109/CSIT61576.2023.10324031.

[8] V. Sokolov, P. Skladannyi, V. Astapenya, Bluetooth Low-Energy Beacon Resistance to Jamming Attack, in: IEEE 13th International Conference on Electronics and Information Technologies (2023) 270–274. doi: 10.1109/ELIT61488.2023.10310815.

[9] Gqrx SDR—Open source software defined radio by Alexandru Csete OZ9AEC. URL: https://www.gqrx.dk/

[10] GitHub—jopohl/urh: Universal Radio Hacker: Investigate Wireless Protocols Like a Boss, GitHub. URL: https://github.com/jopohl/urh

[11] History of Remote Control, Wikipedia. URL: https://en.wikipedia.org/wiki/Remote_control#History

[12] I. Opirskyy, et al., Security Research of Bluetooth Devices Based on Smart Watches, Ukrainian Sci. J. Inf. Secur. 29(1) (2023). doi: 10.18372/2225-5036.29.17548.

[13] What is the History of the Remote Control? HowStuffWorks. URL: https://science.howstuffworks.com/innovation/everyday-innovations/remote-control-history.htm

[14] S. Yevseiev, et al., Method of Assessment of Frequency Resolution for Aircraft, Eastern-European J. Enterprise Technol. 2, no. 9(122) (2023) 34–45. doi: 10.15587/1729-4061.2023.277898.

[15] Small Range Radio Equipment Operating in the Frequency Range from 25 MHz to 1000 MHz, Part 2. General Technical Requirements, DSTU ETSI EN 300 220-2:2017 (2019).

[16] GitHub—NanoVNA-Saver/nanovna-saver: A tool for reading, displaying and saving data from the NanoVNA, GitHub. URL: https://github.com/NanoVNA-Saver/nanovna-saver

[17] NanoVNA|Very tiny handheld Vector Network Analyzer. URL: https://nanovna.com/

[18] Open Source RF Engineering. GitHub—scikit-rf/scikit-rf: RF and Microwave Engineering Scikit. GitHub. URL: https://github.com/scikit-rf/scikit-rf

[19] Rec 70-03, Relating to the Use of Short-Range Devices (SRD), Montreaux: CEPT (1997).

[20] Princeton Technology Corp, PT2262 remote control encoder, LCSC. URL: https://datasheet.lcsc.com/lcsc/1809291408_PTC-Princeton-Tech-PT2262-S_C42793.pdf

[21] S. Yevseiev, et al., Modeling of Security Systems for Critical Infrastructure Facilities (2022). doi: 10.15587/978-617-7319-57-2.