Cybersecurity, Infocommunication Systems and Networks

Modeling of the UAV Control Communication System Based on FPGA

Dinara M. Kalmanova[1], Karakat Bolatzhan[1], Aibek M. Moldamurat[2], Botakoz A. Mamyt[1], and Anel N. Meiramova[1]

[1] *Space Engineering and Technology, L.N Gumilyov Eurasian National University, Astana, Kazakhstan*
[2] *Limited liability company "Kazmedia ortalygy", Astana, Kazakhstan*

Abstract

The article considers the modeling of the organization of the communication system based on the FPGA control of the UAV. The UAV communication channels and devices related to communication are considered. In the process of work, the principle of UAV operation was studied and an algorithm for working in the Quartus II program was developed. A Blis-based control system can offer security features, low power consumption, reliability and a high level of integration within a single device. Security, low power consumption, high reliability and system integration are provided.

Keywords

Unmanned aerial vehicle, communication channels, Quartus II, UAV device, modeling, algorithm, telemetric information, programming

1. Introduction

The range of applications of unmanned aerial vehicles (hereinafter referred to as UAVs) is very wide. The UAV is relatively inexpensive, quick to assemble and very wide in scope. The scope of application of UAVs - mining industry, various facilities, oil and gas pipelines, military industry, agricultural industry, exploration of various landfills, telemedia provide great opportunities to provide live broadcasts of various shows.

The UAV control system based on a programmable integrated logic circuit is very efficient and its programming is simple.

Based on the review of scientific articles studied by UAVs, there is a large amount of information about the controlled UAV system. But there are not so many uses of the basis of an integrated logic circuit programmed by the UAV control system. Therefore, given the UAV architecture, due to its lightness and compactness, linking internal external devices is quite acceptable for implementation and programming through a system of PLD.

2. The principle of operation of a PLD

A PLD is a microcircuit consisting of the same transistors in which triggers, registers, multiplexers and other logic elements are assembled for the simplest circuits.

Since the configuration memory is built using Static RAM technology, firstly, when the PLD is powered on, it is necessary to configure the chip, and secondly, the chip can be reconfigured an unlimited number of times. The principles of operation are taken from the article of the list of references [1].

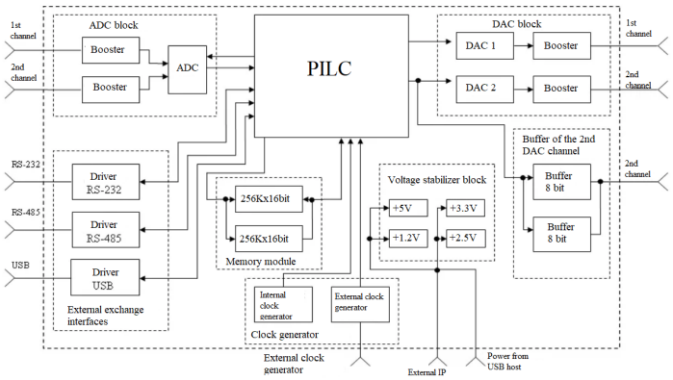

Figure 1: General block diagram of the PLD

Programmable logic blocks (PLBs) are located in the switching matrix that defines the input and output connections of the PLBs (Figure 2).

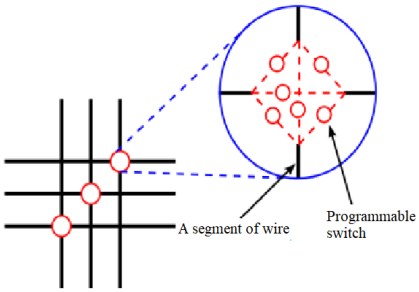

Figure 2: Circuit of the switching matrix

Each conductor intersection has six switching keys controlled by configuration memory cells. By opening one and closing the others, it is possible to switch various signals between PLBs (Figure 3).

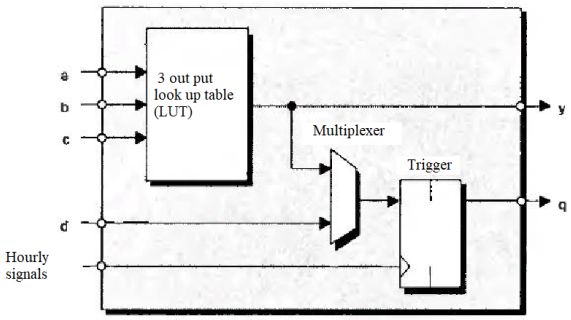

Figure 3: Look up table (LUT)

The PLB (program logic blocks) consists of several arguments defining a logical function (it is called a correspondence table — Look Up Table, LUT) and a trigger (flip-flop, FF). A modern FPGA LUT has six inputs, but for simplicity, the figure shows three (Figure 4). The LUT output is transmitted to the CLB output asynchronously (directly) or synchronously (via the FF trigger operating at the system clock frequency).

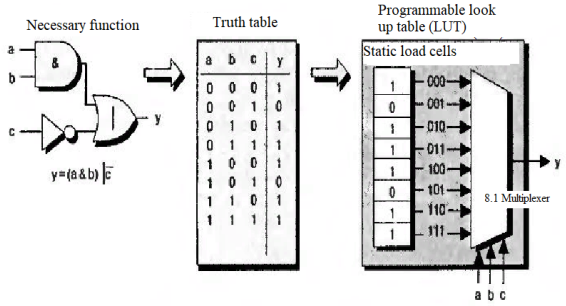

Figure 4: The principle of LUT's implementation

The value of each cell is passed to the input of the output multiplexer LUT, and the input arguments of the logical function are used to select a specific value of the function. PLBs are an important hardware resource of the PLD.

3. Determination of requirements for the UAV automatic control system

At least two communication systems are placed on board the UAV: duplex / half-duplex equipment for transmitting command and telemetry information and a simplex system for transmitting payload information. The equipment for transmitting command and telemetry information is designed for low-speed transmission of command information with a ground control complex (GCC) on board the UAV and low-speed telemetry information from the UAV to the ground control complex. The payload information transmission equipment is designed for one-way high-speed transmission of payload information from the UAV to the ground control complex. In the article of the list of references, the requirements of the management system were obtained [3].

Despite the many options for implementing systems for transmitting command and telemetry information and payload information, the type of communication in which data is transmitted directly between the UAV and the GCC is optimal and is often used. In this case, it is possible to implement the possibility of transmitting information at a high speed, inaccessible to satellite communication systems and at the same time independent of stationary civil communication systems. One of the limiting factors is the distance of radio vision between the UAV and the GCC.

Table 1
Comparative table on the height of the radio-carrying distances between the UAV and the GCC

UAV flight altitude, m	Visibility range (distance to the radio horizon), km			
	At the lifting height of the antenna of the GCC, m			
	1	10	20	30
100	39	47	52	55
250	60	68	72	76
500	83	91	96	99
750	101	109	114	117
1000	117	124	129	132
1500	142	150	154	158
2000	163	171	176	179
3000	199	207	212	215
4000	229	237	242	245
5000	256	264	268	272
6000	280	288	293	296
7000	302	310	315	318
8000	323	331	335	339
9000	342	350	355	358
10000	361	368	373	377

It is possible to organize direct communication between the UAV and the GCC at a distance of up to 200-300 km without taking into account refraction in the atmosphere and the absence of obstacles to the propagation of radio waves. To increase the range of operation of the communication system, it is necessary to use mast structures to increase the altitude of the aircraft and the antenna of the GCC (Figure 5).

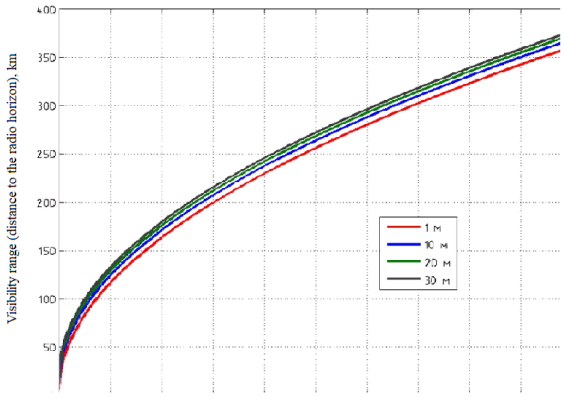

Figure 5: The line-of-sight range of the UAV depending on the flight altitude and the height of the antenna lift of the GCC

The large distance between the UAV and the GCC leads to a large signal disconnection on the road (Figure 6) must be compensated by using antenna systems with an increased gain and an increase in the output power of the transmitters. In the article of the list of references, the distances of the GCC were taken [8].

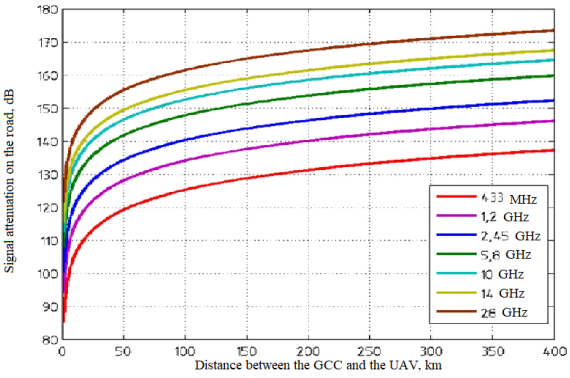

Figure 6: Signal attenuation on the road for different wavelength ranges and at different distances between the UAV and the GCC

The annular antenna array (Figure 7) can be used to build an antenna system in which the maximum direction of the radiation pattern is controlled. Due to the annular symmetry of the antenna array, oriented diagrams can be obtained, which change little when scanned in the plane of the array within 360°.

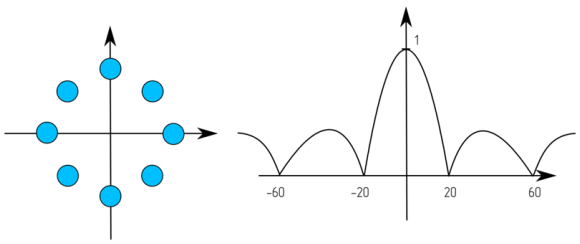

Figure 7: Annular antenna array

If there are several antennas on board the aircraft, it becomes necessary to choose an antenna aimed at the GCC, signal switching is required. There are several options for implementing such a system:

1. Switching the output of the transmitter power amplifier between antennas (one transmitter, one power amplifier, multiple antennas);
2. Replacement of the transmitter output between power amplifiers and antennas (one transmitter, several built-in power amplifiers and antennas);
3. Switching the digital signal between transmitters (the number of transmitters and amplifiers is equal to the number of antennas).

In the simplest case, the output signal of the amplifier is switched between several antennas (Figure 8).

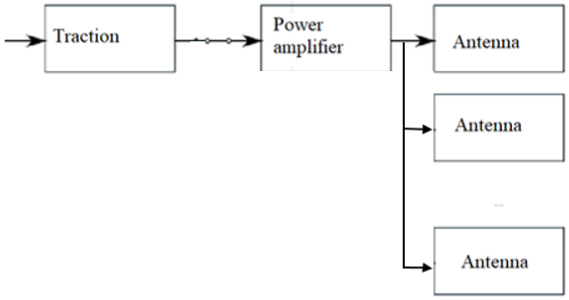

Figure 8: Switching the output of the transmitter power amplifier between antennas (one transmitter, one power amplifier, multiple antennas)

The advantage of this option is the use of a single transfer module and a power amplifier for operation on multiple antenna devices. Disadvantages: losses in the switching device; the presence of restrictions on the power level for semiconductor switches. In the article of the list of references, it is taken about the antenna array [9].

High-speed semiconductor switches have high losses (0.3...2 dB) and low permissible power: the compression point of decibels is mainly +30...Up to 40 dBm. Electromechanical switches are designed for high power and have a lower cost (Figure 9).

Figure 9: DowKey 581-420802A electromechanical switch

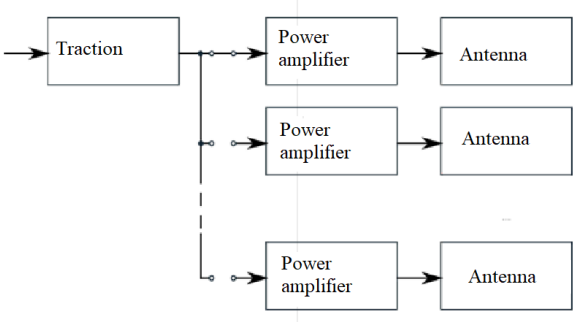

Figure 10: Switching the transmitter output between power amplifiers and antennas

You can place the transmitter power amplifier behind the switch to remove the limitations of the microwave signal switch. At the same time, the number of power amplifiers is equal to the number of antennas (Figure 10).

Disadvantages of this approach: the presence of several power amplifiers that need to be controlled (on/ off when changing antennas); high-power microwave amplifiers (more than 1 Watt) take up a lot of space and have a large mass. For this option, it is necessary to create a single multi-channel power amplifier unit with total power and a cooling system.

Refusal to use microwave signal connectors for each antenna of its transmitter and amplifier (Figure 11). In this case, the signal switch is performed at the level of digital logic (inside the PLD).

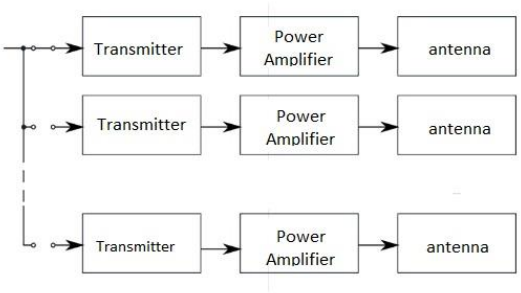

Figure 11: Switching digital signal between transmitters

The advantages of this approach include the high reliability of the system: even if one of the information transmission channels fails, the rest remain operational, providing communication in the remaining azimuth sectors. Mounting the antenna on the pan/tilt head allows a single directional antenna to continuously track the direction of the GCC without interrupting communications. When installing the antenna on a rotary device, the main task is to create a rotary transition that can be placed in different places (Figure 12):

1. Microwave rotary switch is located before the antenna and after the power amplifier;
2. The rotary switch is located after the transmitter and before the power amplifier and antenna;
3. Transmitting device, power amplifier and antenna are placed in the rotary device, digital signals and power supply are transmitted by multi-channel rotary switch.

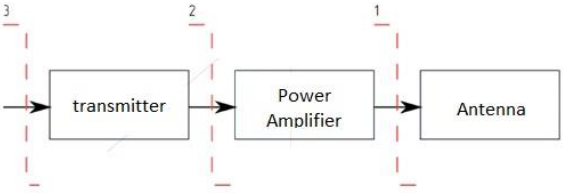

Figure 12: Options for placing the rotary switch

The USB II Platform Cable provides high performance, reliable and convenient Xilinx PLD setup and Xilinx PROM and CPLD programming. The USB II platform cable optimizes direct programming of third-party SPI flash devices and indirect programming of SPI or parallel NOR flash devices via the PLD port. In addition, the Platform Cable USB II is an effective tool for customizing software and firmware using Xilinx applications such as the Embedded Development Kit and ChipScope™ (Figure 13).

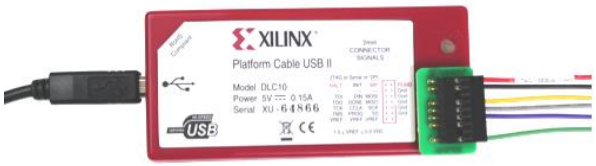

Figure 13: USB II cable

SmartLynq is a high-performance JTAG cable for high-speed PLD and flash memory programming, hardware and software debugging, performance analysis, and event monitoring (Figure 14).

This cable provides:

- bandwidth up to 40 Mbit/s;
- enable host Ethernet for remote access;
- Connect host USB 2.0;
- quick software repair;
- Linux debugging support and hypervisor support.

Figure 14: SmartLynq data cable

The main control device is considered to be a remote control.Unlike conventional digital chips, the logic of PLD operation is not determined in production, it is determined by programming. For programming, programmers and programming environments are used, which allow you to implement the necessary structure of a digital device in the form of an electrical circuit or in the form of a program in special languages that describe Verilog, VHDL, AHDL and other equipment.

4. Implementation of the algorithm in the Quartus II program

Altera®'s Quartus ® II software package is a complete, multi-platform design environment that can be easily adapted to specific project requirements. It is a complex environment for developing systems on a programmable crystal (SOPC). The Quartus II package includes all the utilities needed to work with PLD and CPLD chips.

There are only two processes in the module, which are parallel to each other, synchronized with the clock signal clk. In the first process, we create a counter that counts the equal time segments that switch from one LED to another. In the second process, we execute a function that turns on the LEDs alternately after a certain time set by the counter from the first process.

First of all, we open the Quartus II window (Figure 15). All the buttons used in Window are located in this window; we create a new project using the New Project Wizard (menu File) command.

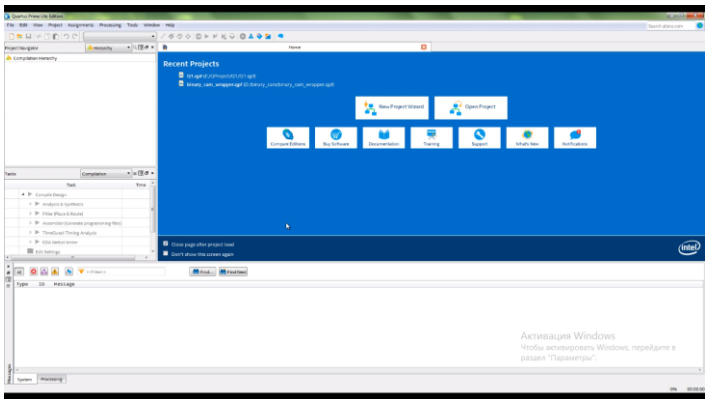

Figure 15: Window of the Quartus II program

Creation of the source file of the project using a text editor (Text Editor) in Verilog HDL, VHDL or Altera Hardware Description Language (AHDL) languages. In addition, you can create a project diagram in a graphic editor (block editor) using symbols representing other source files or logical elements of the project (Figure 16).

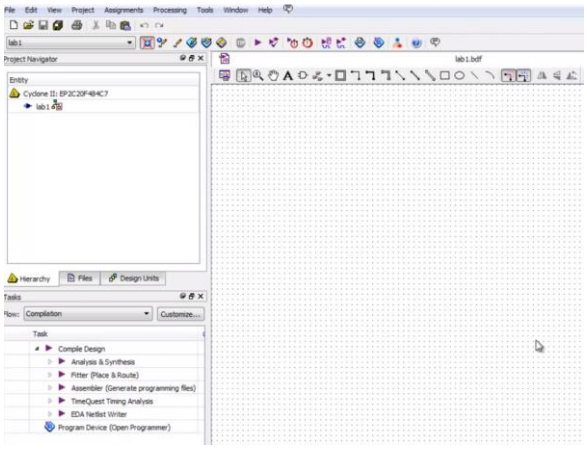

Figure 16: Working panel of the Quartus II version

Here is the last page. Click Finish. The project has been created. (Figure 17).

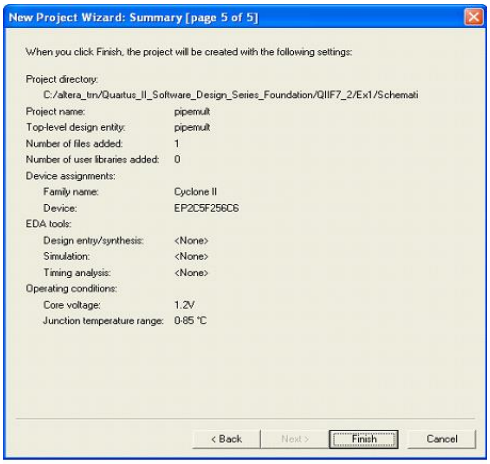

Figure 17: Completion of work

By pressing the right mouse button, we call the library of tools. We draw up our scheme through the library (Figure 18). If you want to continue learning, you do not need to leave the Quartus II environment. A closed project can always be opened using the File -> Open Project command.

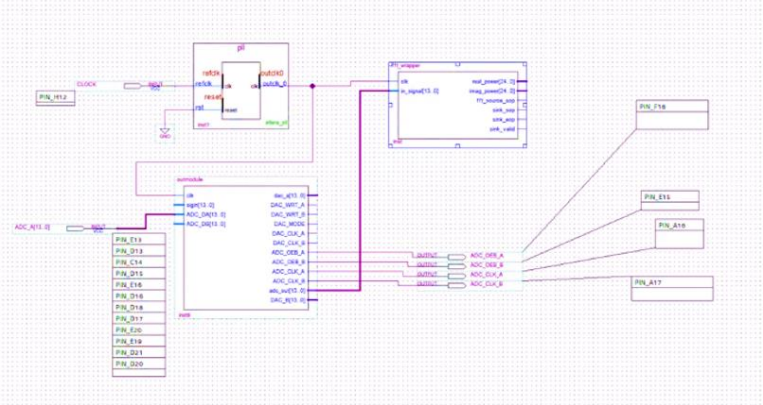

Figure 18: Simulation scheme in Proteus

Now to enter the written program, press the START button. press twice. (Figure 19).

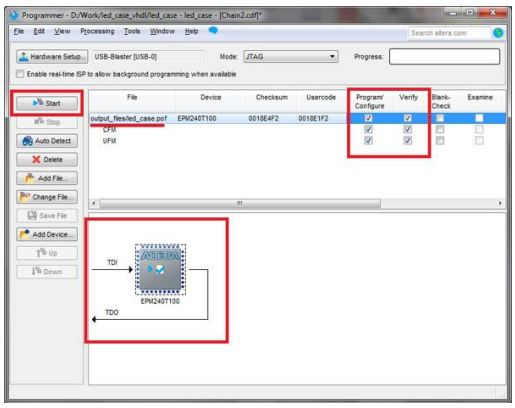

Figure 19: Folder icon

Select Start -> Start Analysis & Elaboration from the Processing menu. This command checks the presence of all files in the project and the correctness of their connection, and also displays a general matrix image of the results (Figure 20).

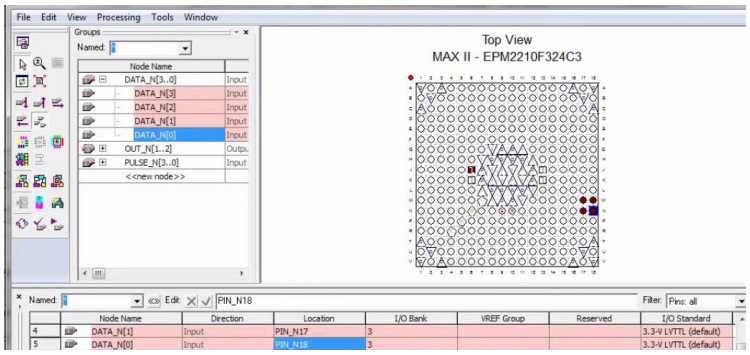

Figure 20: Result obtained in the form of a matrix

The results obtained from the sensors indicate the correctness of the algorithm. Quartus II allows you to use a megafunction with a logic analyzer in the project. The data is collected and stored in the internal memory blocks of the FPGA and transmitted via a boot cable to Quartus II. In addition, it is possible to supply internal signals to the FPGA pins for further control.

5. Discussion

FPGA is programmed over the entire area of the crystal. The signals come through complex transistor circuits. The main difference between an FPGA and a microcontroller is that in a microcontroller, a person cannot change the internal connections between elementary elements, programming an FPGA and working with them are based on establishing connections. FPGA is also distinguished by the fact that when programming a device, the programmer creates an architecture from the main logical elements. Thus, it will get high speed and chip functionality. This allows you to create many projects without changing a single chip. When choosing an FPGA, the main criterion is the number of programmable blocks-they should be enough to implement the project.

6. Conclusion

As a result, on the basis of the FPGA, the UAV control system as a whole and software coding, the implementation of the relationship between the Central Control and the UAV were created.

For the development of digital devices, low-level languages are used, which are more complex and have syntax. A simulation scheme using the Verilog HDL programming language is implemented.

A big step in FPGA security is to provide a basic level of security with a simple interface and adaptability. At the present stage, the FPGA has security features only for the system configuration, but for complete security during operation, application data protection is required.

7. References

[1] Aviation: Encyclopedia / gl. ed. G. P. Svishchev. — M.: The Great Russian Encyclopedia, 1994. — 736 p. — ISBN 5-85270-086-X.

[2] O.H. Zinchenko. “Unmanned aerial vehicle: Application for aerial photography for mapping” The website of the company "Rakurs". http://www . racurs. ru/wwwdownload/articles/UA V1 .pdf.

[3] V.S. Moiseev. Applied theory of control of unmanned aerial vehicles. Kazan: RCMKO, 2013. 768 p. (Series "Modern Applied Mathematics and Computer Science".

[4] K. Moldamurat, K. Akhmetov, A. Otegen, S. Brimzhanova, K. Otyzbayeva, A. Zhiyenbek. “Computer simulation of intelligent control systems for high-precision cruise missiles.” In recognition of outstanding presentation on 2022 International Conference on Smart Information Systems and Technologies, 28-30 April 2022.

[5] K. Moldamurat, S. Brimzhanova, B. Baizhumanova, O. Bizhanova, K. Akhmetov, A. Moldamurat. “Computer simulation of the path and control of an intelligent mobile robot in Python.” In recognition of outstanding presentation on 2022 International Conference on Smart Information Systems and Technologies, 28-30 April 2022.

[6] K. Moldamurat, S. Akhmejanov, K. Kariyeva, Zh. Omarov, D. Kalibekov, S. Nurbakytbek. “Design and optimization of the parameters of a hybrid unmanned aerial vehicle in the SolidWorks complex.” In recognition of outstanding presentation on 2022 International Conference on Smart Information Systems and Technologies, 28-30 April 2022.

[7] A. Akhmadiya, N. Nabiyev, K. Moldamurat, A. Kismanova, B. Prmantayeva, S. Brimzhanova. “Application of GLCM textural based method with Sentinel-1 radar remote sensing date for building damage assessment.” In recognition of outstanding presentation on 2022 International Conference on Smart Information Systems and Technologies, 28-30 April 2022.

[8] N.M. Boev. Analysis of the command and telemetry radio communication line with unmanned aerial vehicles// Bulletin of the Siberian State Aerospace University named after Academician M.F.Reshetnev. Issue 2 (42) / Editor–in–Chief, Doctor of Technical Sciences Kovalev I.V. – Krasnoyarsk: SibGAU, 2012. - pp.86-91.

[9] N.M. Boev. Adaptive change of parameters of digital communication systems of unmanned aerial vehicle complexes// 22nd International Crimean Conference "Microwave technology and Telecommunication Technologies", September 10-14, 2012: materials of the conference: in 2 vols.

[10] J. Yu. “Design and Optimization of Wing Structure for a Fixed-Wing Unmanned Aerial Vehicle (UAV).” Modern Mechanical Engineering, 2018, 8, 249-263p.

Fundamentals of Safety, Reliability and Testing Systems in the Course of Testing Spacecraft

Azhar Baimanova[1], Akmaral Moldamurat[2], Alikhan Utegen[1], Mirana Kabdulova[1], and Aruzhan Atanova[1]

[1] *L.N. Gumilyov Eurasian National University, Astana, Kazakhstan*
[2] *LLP «Management company «Kazmedia ortalygy», Astana, Kazakhstan*

Abstract

This paper describes the basics of testing spacecraft to ensure its reliability at all stages of operation of rocket and space complexes. A review of the types of tests of launch and technical rocket and space complexes was conducted. the goals and objectives of complex tests are described. The requirements for the content of the program and methodology for testing spacecraft are described, as well as examples of some of them are given. The features of test programs for the reliability of spacecraft are presented and the role of an automated test system in the design is proposed.

Keywords

Spacecraft, test, rocket, safety, reliability, factor, experiment

1. Introduction

The rocket and space complex is a complex technical system. Therefore, when experimental development of such systems, it is necessary to rely on the theoretical foundations of planning, maintaining and analyzing the results of tests of complex technical systems. this process, as a result, allows you to eliminate most of the possible defects during operation.

"In accordance with the address of the first president of the Republic of Kazakhstan – Elbasy Nursultan Nazarbayev to the people of Kazakhstan "strategy "Kazakhstan-2050", Kazakhstan should expand its niche in the world market of space services, in particular, the assembly and test complex of spacecraft in Astana, the space remote sensing system, the national system of space monitoring and ground infrastructure, the high-precision satellite communication system."

By 2030, Kazakhstan should expand its niche in the global space services market and bring a number of initiated projects to their logical completion.

The purpose of the article is to describe the basics of testing spacecraft, experiments conducted to ensure reliability.

2. Methods of testing spacecraft

The test methodologies consist of test objectives in accordance with the approved plans and test specifications, which must clearly indicate the verification criteria and the "passed or not" criteria [1].

The methodology includes at least a description:

- signs of compliance of the object being tested with the specification of this object;
- criteria for normal and abnormal processes of tests, goals, assumptions and limitations;
- test schemes;
- all controlled and recorded settings;
- input data;
- test equipment;
- expected intermediate test results;
- output data format;
- expected results.

In the world, it is customary to conduct tests both on natural objects and using mathematical or

physical modeling in accordance with Figure 1.

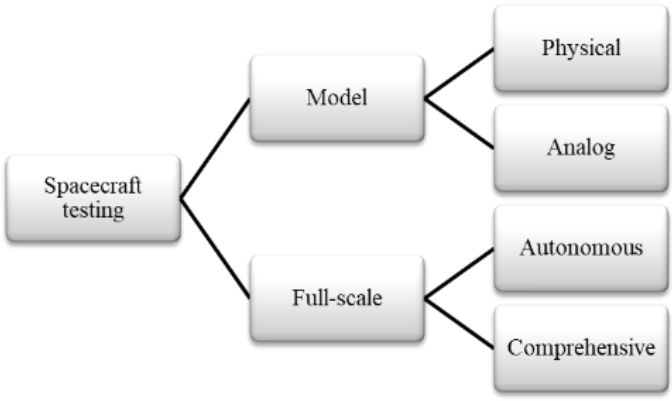

Figure 1: Classification of spacecraft tests

When testing spacecraft, the following mechanical factors are affected: linear acceleration, shock, vibration and their combinations. Mechanical tests are necessary to control the resistance of objects to vibrations and shocks, as well as to centrifugal loads. Aggregates and Assemblies of spacecraft must retain their properties during and after mechanical impact. All tests must comply with the standard operating conditions. As a rule, all types of tests include one sample of the unit [2].

2.1. Static tests

As static tests, it usually means testing an object or its individual parts and components in laboratory conditions with test loads that mimic possible loads that occur during operation. Such tests have the following goals:

- determination of the stress-strain state of the structure under load;
- determination of the stiffness parameters of the structure by measuring general and local displacements;
- verification of production technology;
- experimental verification of calculation methods and structure for strength;
- experimental determination of destructive loads.

2.2. Vibration tests

The vibration test is a complex type of test. During the test, the sample is subjected to random vibration with a given level in a wide frequency range. Due to the complex mechanical reaction of the sample and its fixation, vibration testing should be carried out very carefully, both during the preparation process and at the implementation stage. Tests are carried out on the effects of different vibrations:

- to the effect of sinusoidal vibration;
- to the effect of shock loads.

Its main purpose is to determine the degree of hardness of the object or its individual parts and elements, the ability to withstand the effects of possible random vibrations during actual use, as well as to identify possible mechanical damage and/or deterioration of the initial characteristics of the product. In addition, the results obtained are compared with the requirements of the relevant regulatory and technical documentation to assess the degree of suitability of elements, equipment and other products for specific operating conditions.

2.3. Inertial tests

When testing spacecraft and their systems, inertial loads are modeled in such a way that the spacecraft meets the loads quite accurately under normal operating conditions. However, in bench equipment, it is impossible to completely restore the operating conditions of the spacecraft, at least under the influence of gravitational forces, the direction of impact of which often does not correspond to the direction of overload that occurs under bench conditions. Therefore, we can talk about a greater or lesser degree of approximation to specific situations[3]. Centrifugal stands are used as the main test instruments. To achieve load conditions that are as close as possible to operating conditions, the following methods are used on centrifugal stands:

- changing the speed of rotation of the dynamic unit with the object under study;
- turning the object under study in a dynamic installation;
- linear movement of an object along one or more spatial axes in a dynamic installation.

2.4. Reliability and safety of the spacecraft

Reliability of a spacecraft is understood as the property of performing a given function, while maintaining the values of operational indicators within the limits set in accordance with the specified modes and operating conditions. Similar studies were conducted by scientists in the field of modeling heat and mass exchange in the combustion chamber during the combustion of solid fuel, especially coal. Many scientists specializing in the field of computational hydrodynamics and thermal power have a great impact on the reliability of spacecraft [11].

The following requirements apply to the reliability of the spacecraft:

- The probability of non - stop operation for 1 year should be at least 0.85, including a module of service equipment – at least 0.89, a module of scientific equipment-at least 0.95, taking into account the time of storage of the last electrical inspection before commissioning during the period of its active operation in orbit on a regular cyclogram.
- The criterion for refusal to receive useful information is an irrevocable violation of the operational state of the spacecraft, which leads to the impossibility of obtaining useful information.
- The service life of the spacecraft must be at least 2 years (1 year for IAS) and 1 year for storage and use in ground conditions; 1 year for use in orbit (under warranty).
- On-board systems should be designed taking into account the provision of full control over the operability of the main and backup circuits and channels without dismantling the system and the product as a whole [4].

The safety of the spacecraft is understood as its ability to survive in all specified modes of operation and not pass into a state that poses a threat to the life of operating personnel, adjacent objects and the natural environment.

The main components of the concept of" security " are shown in Figure 2.

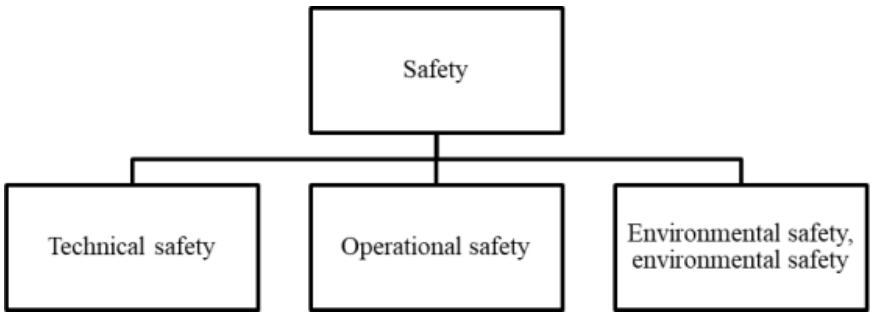

Figure 2: Key security components

The spacecraft is a complex multicomponent complex consisting of hardware and software [5]. Accordingly, it is necessary to promptly monitor their characteristics and analyze the situation during Operation. Reliability is one of the most important characteristics of a technical system. Since Ka has a complex structure (and, therefore, the complex nature of relationships between individual components),

the process of obtaining numerical values of reliability indicators is also complicated.

2.4.1. Reliability as the probability of a random event

This method is used if the device under study is activated immediately and once. For this method, it is not possible to use reliability characteristics relative to time. Therefore, reliability is defined as the probability of implementing a random event P(A) in an experiment that the device will not give up. Denote the probability of P (A) by N (confidence).

Experimental reliability is determined as follows:

$$H = \frac{n}{N}, \quad (1)$$

where *n* is the number of undefined elements; N is the number of elements set for the experiment.

Experts in the field of reliability rarely use this formula to quantify reliability, since it reflects only the average point estimate of reliability. A specialist often needs to know the upper and lower limits of reliability.

2.4.2. Reliability as a quality over time

Methods that study reliability believe that changes in reliability as a quality developed over time are subject to certain statistical laws that are determined only experimentally. In this case, the task of identifying the causes of failure and determining the possibility of their elimination is not set, but only the fact of refusal is indicated[6].

At moment when t = 0, the element starts working, and at the moment T = T, it fails. Then T is the time of "existence" of an element, which is a random variable with the law of division.

$$F(t) = P(T > t), \quad (2)$$

where F (t) is the failure Time Distribution Function; P is the probability sign.

On the basis of the study, an experimental reliability function is constructed. The operating time of an element is divided into some time intervals, and the reliability of each of them is estimated by the following formula for a certain time t from the interval.

$$H(t) = \frac{n(t)}{N}, \quad (3)$$

where $n(t)$ is the number of elements that are not defined at the moment of time.

The approximate representation of the experimental confidence function is shown in Figure 3.

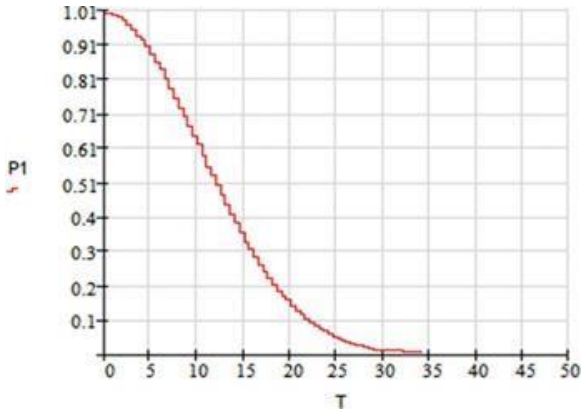

Figure 3: Example of constructing an experimental reliability function

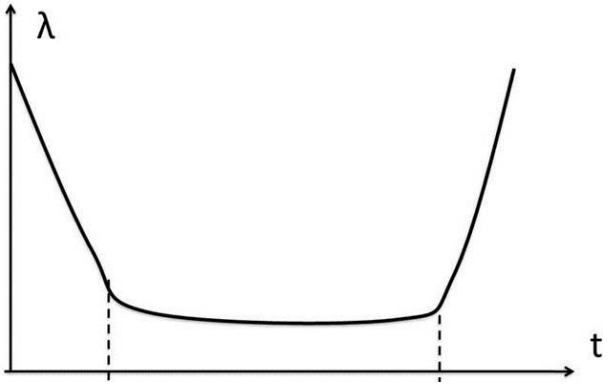

Figure 4: Example of constructing an experimental reliability function

If some product consists of many elements, and if the failure of the elements is independent and the product cannot be restored, then a graph of the intensity of failures can be constructed for it based on the results of experiments and/or operation. A typical graph of the failure intensity of a complex product is shown in Figure 4, which clearly shows three stages: the working period, the normal working period, and the aging period [7].

2.4.3. Reliability as a probability strength

An indicator of reliability in this method is the probability that the load-bearing capacity of the structure (element) R exceeds the existing loads N:

$$H = P(R > N), \tag{4}$$

In this method, the force R is understood as any random variable that determines the limit possibilities (lifting capacity) of an element, the excess of which means the failure of the element. The concept of external load N is a random variable acting on an element from external sources. External load is the tensile, compressive or cutting forces, bending or torque, tension, internal pressure in tanks, longitudinal or transverse overload, etc., including their combination, operational load. Moreover, it is not multiplied by safety coefficients, as in the calculation on deterministic quantities, but is considered as a category of probability.

Load capacity is understood as force, bending or torque, stress, pressure, overload, deformation, etc., which characterizes the limiting state of the element, limiting its further application.

Reliability will also be convenient to consider as the probability of not abandoning a random process. This is because the output of the trajectory of change in the quality of an element over time R(t) from the region of permissible States Q in the quality space V is called the failure of an element and/or system.

To find the reliability function, it is necessary to determine the quantitative characteristics of random processes from the region of permissible States, in particular, the mathematical expectation of positive intersections n(t) by the vector process V(t) of the marginal surface G in the quality space and the average number of emissions per unit time [20].

2.5. Testing the effect of acoustic loads

To study the acoustic effect on the product, the following tests are carried out:

- natural substances on the ground directly in the product;
- in an open stand with the engine running;
- in closed boxes with different noise sources;

- in the acoustic chambers.

In-kind tests on the ground are closer to the actual operating conditions in terms of their conditions and, as a result, make it possible to more accurately assess the design and operational strength of the onboard equipment. Such tests are usually performed at the very end of the general program of the CA for acoustic effects. However, such tests are very expensive, and in ground conditions, the flight conditions of the acoustic load are practically not increased.

Tests on an open stand with a running engine are cheaper, and large products can be tested here. In this case, the acceleration of tests and compliance with the required

The purpose of the test stage is to test the performance of the product as a whole and its individual systems. The importance of this stage is that it monitors the correct Assembly of the product, checks the logic of its systems and components. The advantage of the appearance of flying spacecraft in general is greater than that of monolithic spacecraft, since the failure in the appearance of a single spacecraft can be overcome by the rest of the structure, and the failure of monolithic spacecraft can lead to the failure of the mission. One of the main tasks of the formation of a flying spacecraft is guidance, navigation and control [10]. Verification is the transmission of a control effect to the object of control and the analysis of parameters that characterize the state of individual systems and the entire apparatus as a whole.

Currently, most domestic and foreign systems for automated testing of spacecraft and its parts have an established means of testing spacecraft systems.

2.6. System testing tool

The built-in system testing tool provides a secure ability to evaluate space systems installed on or integrated with host platforms. These test units consist of specialized environmental chambers, such as thermovacuum, echoic and aerodynamic tubes, where measurements are made during the operation of the space system. The tested system is exposed to various effects, and its response is evaluated to obtain critical integrated information about the performance of the system [12]. The main purpose of testing in these objects is to evaluate integrated systems under controlled conditions that simulate various situations encountered in the work environment. Such testing is carried out to determine the presence of any problems or to determine the reaction of the system to the simulated environment. This on-site testing helps identify problems that may not be detected by components, subsystems, or other tools, but are very important for testing the system before starting[13]. Failure to properly assess the performance of a system installed on Earth usually leads to unsatisfactory performance during launch or in space. The table below provides a brief overview of the capabilities and limitations of the system testing tools.

Table 1
Capabilities and limitations of the system's installed testing tool

What can the system's installed testing tools do?	What can't the system's installed testing tools do?	What makes installed systemtesting tools so special?
• Evaluates compatibility of the system with the host platform; • Provides the possibility of pre-flight inspection; • Checks the static performance of the integrated platform at • certain points in the shell dynamic performance testing in a free space environment;	• Evaluation of the performance of a closed circuit in a free space environment; • Performance assessment;	• Allows you to test the system on the host platform under controlled conditions;

An important role in ensuring long-term and uninterrupted operation of spacecraft is played by the

resistance of structural materials and elements of spacecraft to external factors. Analyzing the history of spacecraft operation, according to NASA, the cause of the spacecraft's failure is related to the deployment of solar panels. The unsuccessful placement of solar panels, antennas and other auxiliary devices for the placement of spacecraft is one of the main reasons for the initial failure of satellites and the reduction of their capabilities, while on average one failure occurs every two years. Since the spacecraft is "completely new", but cannot function in the intended way and does not meet the goals of its mission, the failure of deployed devices leads to very large losses. For example, as a result of the unsuccessful placement of solar panels over the past 23 years, insurance claims amounted to about 8 800 million. This document provides for malfunctions in the deployment of spacecraft and deviations that may be directly related to the deployment problems[14].

Deployed applications are very important components of spacecraft, and their failure has a very profound impact on the ability to achieve mission goals. Such failures were a prerequisite for servicing the spacecraft. The first major repairs and maintenance of a spacecraft in space occurred in 1973, when astronauts of the first and only national orbital station of the United States - Skylab-made open space trips to empty the solar panels stuck in one of the station's solar panels and replace the thermal screen. it was severely damaged during launch [15].

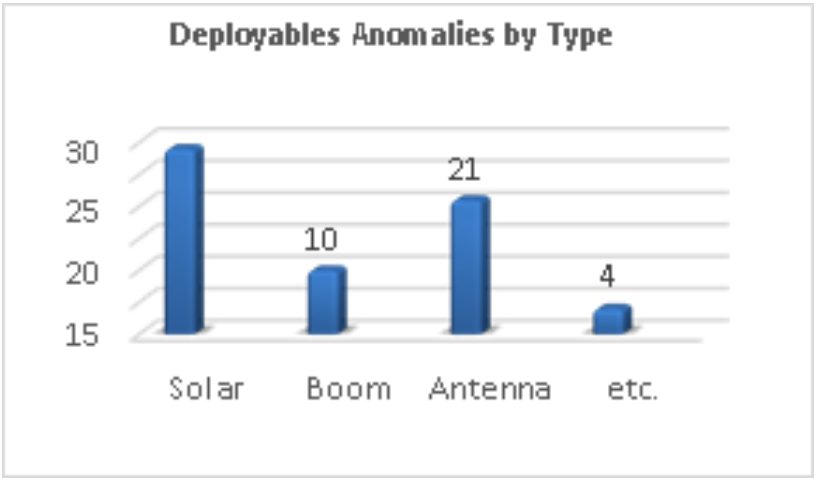

Figure 5: Anomalies by Type

Of the 54 tested spacecraft that suffered from deployed anomalies, 29 (54%) suffered from solar panel- related anomalies, 20 (37%) had problems with antenna placement, and 10 (18%) had problems with Arrow placement. It should be borne in mind that some spacecraft have problems with several types of devices to be deployed.

3. Conclusion

Within the framework of this article, the types of launches and tests of spacecraft of rocket and space complexes are described. They are a method of checking whether the spacecraft meets all the requirements in accordance with the terms of reference of the project. The main types of tests include design, qualification, acceptance, pre-flight and pre-launch tests.

The development, creation and operation of spacecraft is associated with the need to link the functioning of elements of complex rocket and space complexes. The composition of rocket and space complexes, programs and methods of testing spacecraft, reliability and safety of spacecraft are described for detailed study.

In the course of the analysis for testing spacecraft, the capabilities and limitations of an important automated complex - a system testing tool and tools-were identified, and the ability to test the system on the host platform under controlled conditions was highlighted.

When analyzing data, it was determined which types of failures are most common. According to statistics, more than 50% of spacecraft failures were associated with the placement of solar panels, 20

(37%) had problems with the placement of the antenna, and 10 (18%) had problems with the placement of the arrow. this led to the conclusion about the importance of testing solar panels.

The results of complex tests assess the readiness of the spacecraft for actual operation in the closest conditions in accordance with the flight plan. With positive test results, the spacecraft is ready to be sent to the starting position.

4. References

[1] Куренков В. И., Капитонов В. А. Методы расчета и обеспечения надежности ракетно-космических комплексов: учеб. пособие – Самара: Изд-во Самар. гос. аэрокосм. ун-та, 2007. – 26-37 с.

[2] Тестоедов Н. А. Особенности статических испытаний космических аппаратов. Сибирский аэрокосмический журнал, (1 (18)), 2008 – 91-94 сс.

[3] Бакулин Я.Ю., Журавлев В.Ю. Виброиспытания изделий ракетно-космической техники. Решетневские чтения, 1 (18), 2014 – 123-124 сс.

[4] ГОСТ Р 56469-2015 Аппараты космические автоматические. Термобалансные и термовакуумные испытания.

[5] Ли В. А. Основы теории испытаний. Экспериментальная отработка ракетно-космической техники.

[6] Болотин В.В. Методы теории вероятностей и теории надежности в расчетах сооружений – М.: Стройиздат, 1982.– 351 с.

[7] Черток, Б. Е. Ракеты и люди 3-е изд. – М.: Машиностроение, 2002. – 416 с.

[8] Баранов, Д. А., Еленев, В. Д., Смородин, А. В. Принципы построения систем и объектов космического ракетного комплекса среднего класса повышенной грузоподъёмности. Вестник Самарского государственного аэрокосмического университета им. академика С.П. Королёва, (2 (33)). 2012. – 25-34 сс.

[9] Семкин Н.Д., Телегин А.М., Калаев М.П. Космическое пространство и его влияние на элементы конструкций космических аппаратов. – Самара: СГАУ им. С.П. Королева, 2013. – 3 с.

[10] Development of a software simulator for small satellite swarm control Moldamurat, K., Utegen, A.S., Brimzhanova, S.S., Kalmanova, D.M., Yryskeldi.

[11] 11.Investigation of the different Reynolds numbers influence on the atomization and combustion processes of liquid fuel Askarova, A.S., Bolegenova, S.A., Maximov, V.Yu.,Baktybekov, K.S., Syzdykov, A.B. Bulgarian Chemical Communications, 2018, 50, pp. 68–77.

[12] The simulation of the interaction of dielectric materials with soft space radiation Baktybekov, K., Vasil'eva, I. European Space Agency, (Special Publication) ESA SP, 2003, (540), pp. 719–721.

[13] Coordination of movement of multiagent robotic systems Kyzyrkanov, A., Atanov, S., Aljawarneh, S. Proceedings - 2021 16th International Conference on Electronics Computer and Computation, ICECCO 2021, 2021.

[14] Navigation system based on Bluetooth beacons: Implementation and experimental estimation Kereyev, A.K., Atanov, S.K., Aman, K.P., Kulmagambetova, Z.K., Kulzhagarova, B.T. Journal of Theoretical and Applied Information Technology, 2020, 98(8), pp. 1187–1200.

[15] STUDY OF SPACECRAFT DEPLOYABLES FAILURES Alejandro Rivera , Alphonso Stewart, KBR / NASA Goddard Space Flight Center Bldg. 29 Rm 100, Greenbelt, MD 20771, USA.

Efficient Methods for Detection and Prevention of ARP Spoofing Attacks

Kymbat Z. Seilkhanova[1], and Sabyrzhan K. Atanov[1]

[1] *L.N. Gumilyov Eurasian National University, Astana, Kazakhstan*

Abstract

On the internet, the ARP protocol is frequently used to translate IP addresses into MAC addresses. Since it lacks authentication, it is vulnerable to an attack known as a "ARP spoofing attack". This spoofing may also result in a Man-in-the-Middle attack, a denial-of-service attack, etc. This document suggests a few techniques to identify and stop ARP spoofing.

Keywords

Cybersecurity, Network attacks, ARP spoofing

1. Introduction

ARP is a protocol that allows network communications to get to a particular network device. ARP converts Media Access Control (MAC) addresses into Internet Protocol (IP) addresses and the other way around [1]. Devices often utilise ARP to get in touch with the router or gateway that gives them access to the Internet, as it is shown in Figure 1.

Figure 1: Normal traffic

ARP spoofing or ARP poisoning is an attack in which an attacker poisons the ARP cache of the target hosts and places itself between legitimate traffic leading to attacks like MITM, sniffing, connection hijacking, connection spoofing and DoS. This, makes it necessary to secure ARP protocol [2].

The ARP protocol does not confirm that a response to an ARP request originates from an authorized party since it was not created with security in mind. Additionally, it enables hosts to receive ARP answers even though they have never made a request. The ARP protocol has a weakness like this that makes it vulnerable to spoofing attacks. Network devices such as switches are not designed to detect and prevent ARP attacks [3]. This paper proposes methods for detecting and preventing ARP spoofing.

2. Methodology

This work used operating systems such as Kali Linux and Windows 10. Kali Linux – the most popular and advanced distribution kit for conducting testing for penetration and security audit today [4]. Tools such as Ettercap and Wireshark were also used.

3. Statistics and relevance

In general, man-in-the-middle attacks are just a more innovative version of traditional eaves-dropping.[5] But it is not so obvious - other strategies used in MitM attacks also have to inject or modify data. More than one-third of exploitation of inadvertent weaknesses involved MitM attacks, according to IBM's X-Force Threat Intelligence Index 2018 [6].

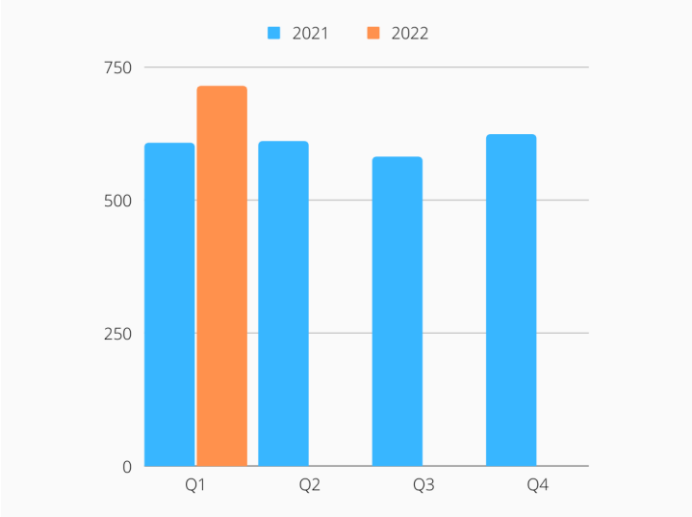

Figure 2: Number of attacks in 2021 and 2022 (quarterly)

As shown in Figure 2, attacks increased by 14.8% in Q1 2022 compared to Q4 2021. Most often, state and medical institutions and industrial enterprises were subjected to attacks. The number of attacks without reference to the industry sector also increased - from 18% to 23% [7].

The use of open protocols in the internal network, which was detected in 75% of systems, allows any internal attacker to intercept sensitive information, including administrator creden- tials, as a result of a man-in-the-middle attack, which in turn is also possible in 75% of cases due to the lack of protection against ARP Spoofing (Figure 2). The combination of these two shortcomings allows you to intercept confidential information and change data in transit [8].

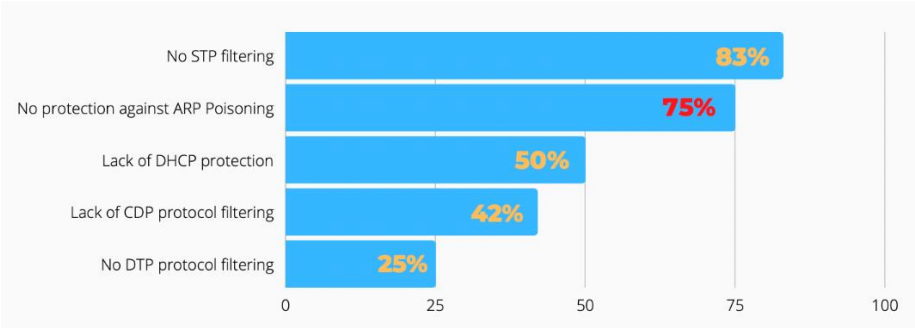

Figure 3: Weakness in the protection of service protocols of the channel and network level

The data above shows that the number of cyberattacks is gradually increasing every quarter. Learning from the past to predict future attacks can also be problematic in the continuously evolving threat landscape [9]. The danger of lack of protection against ARP spoofing attacks in combination with other vulnerabilities is still relevant [10, 11].

Although various mechanisms for combatting these attacks in the form of hardware switches or software like intrusion prevention and detection systems, specialised tools, port security feature or enhanced ARP protocols are available, still there is no 100% solution to these attacks [12].

4. How ARP spoofing works

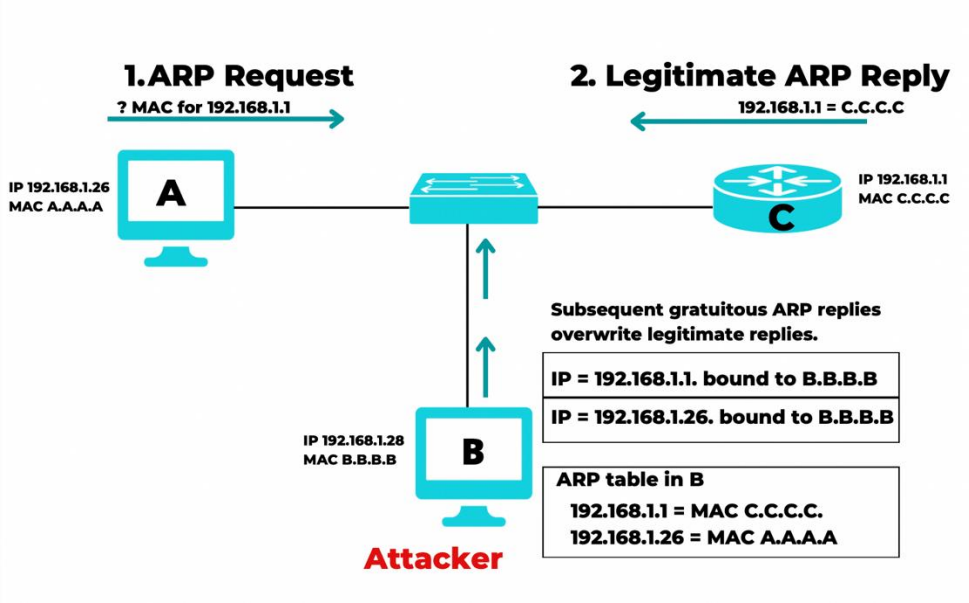

Figure 4: Poisoned ARP cache

ARP spoofing is a Man in the Middle (MitM) technique that enables attackers to listen to network device traffic. Figure 4 shows how the attack operates:

1. The attacker must have network access. The IP addresses of at least two devices—say let a workstation and a router—are found after they do a network search.
2. To send out faked ARP answers, the attacker uses the Ettercap tool.
3. Thefakeanswersclaimthattheattacker'sMACaddressistherightMACaddressforboth the router's and the workstation's IP address. By doing this, the router and workstation are tricked into connecting to the attacker's system rather than to each other [13].
4. The two devices then start communicating with the attacker instead of one another directly after updating their ARP cache entries.
5. The attacker is now covertly intercepting all conversations.

5. Threat modelling using Ettercap

First, it is necessary to simulate an ARP spoofing attack model.

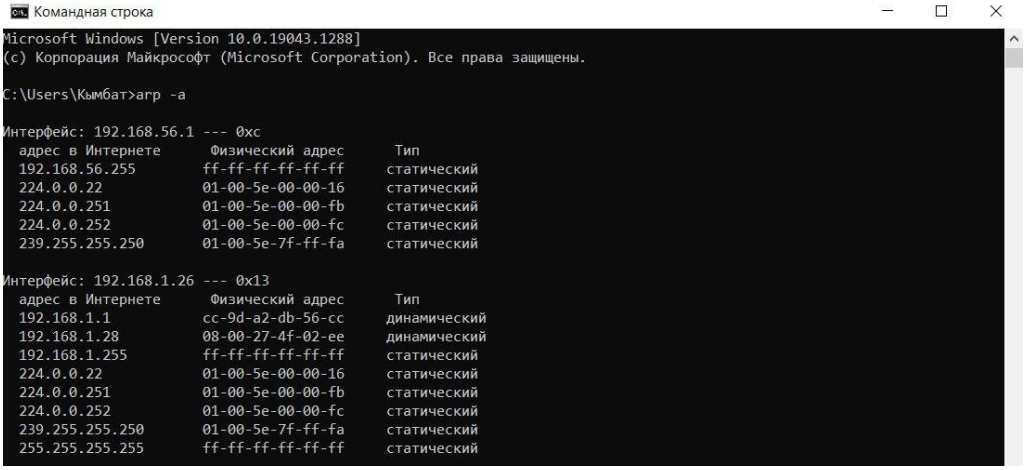

Figure 5: Screenshot of normal ARP cache

Figure 5 demonstrates the not poisoned ARP cache table from the command prompt. So, this table has information about IP and MAC addresses from the ARP cache. By the information above Table 1 below can be constructed:

Table 1
Source IP and MAC addresses

Source	IP address	MAC address
User	192.168.1.26	18-56-80-b4-3d-13
Router	192.168.1.1	cc-9d-aa2-db-56-cc
Hacker	192.168.1.28	08-00-27-4f-02-ee

The Ettercap tool built into the Kali Linux operating system was used for the ARP spoofing attack. The graphical interface of this program is shown in Figure 6. In this program, 2 attack targets are defined, such as User and Router.

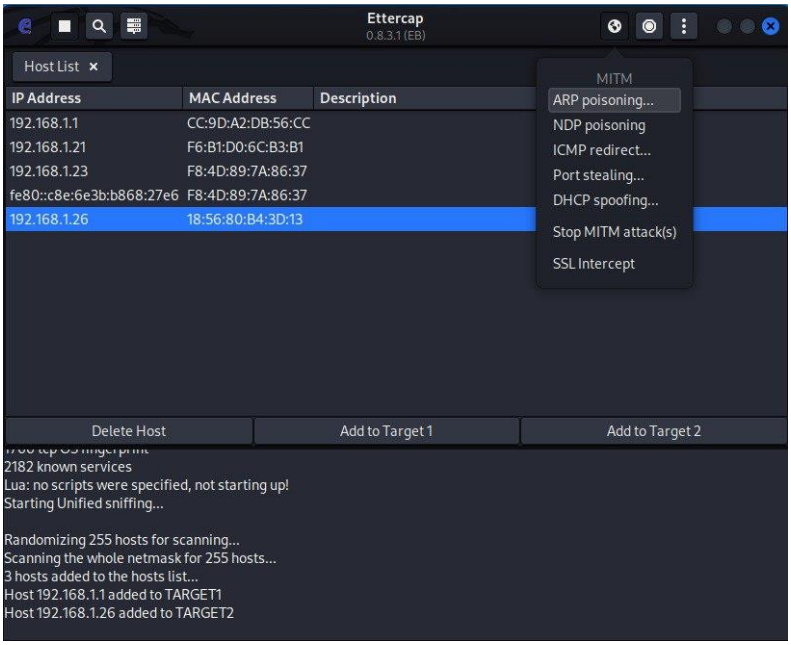

Figure 6: Ettercap tool

After defining the goals and launching Ettercap, real-time traffic monitoring was launched using the Wireshark utility with ARP protocol traffic filtering.

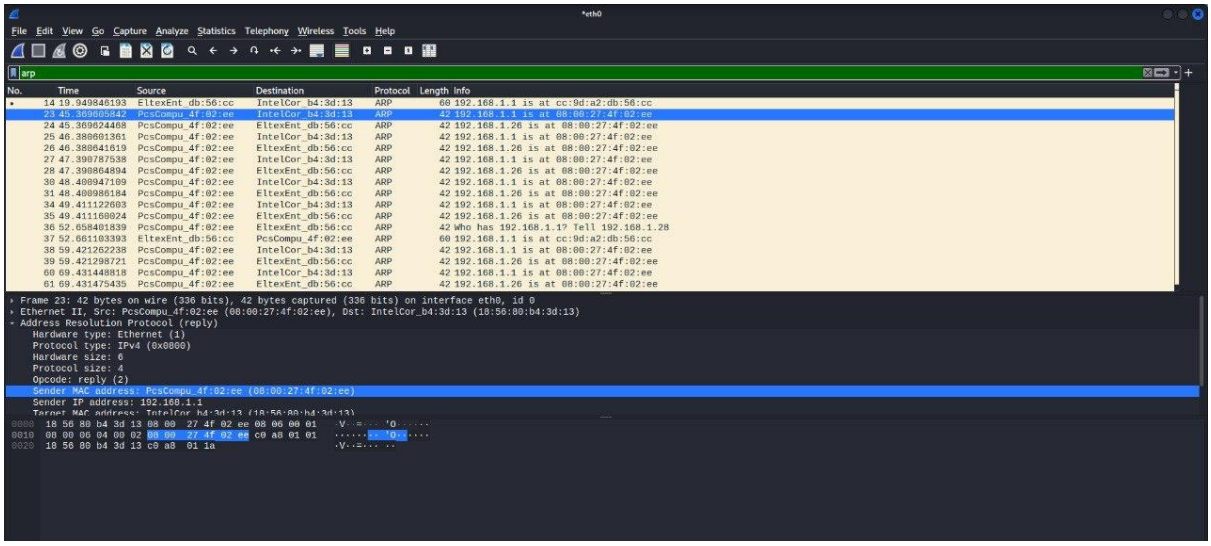

Figure 7: Traffic monitoring by filtering ARP protocol

Figure 7 shows the process of filling the ARP cache, which subsequently led to the substitution of the MAC addresses of the attacked victims.

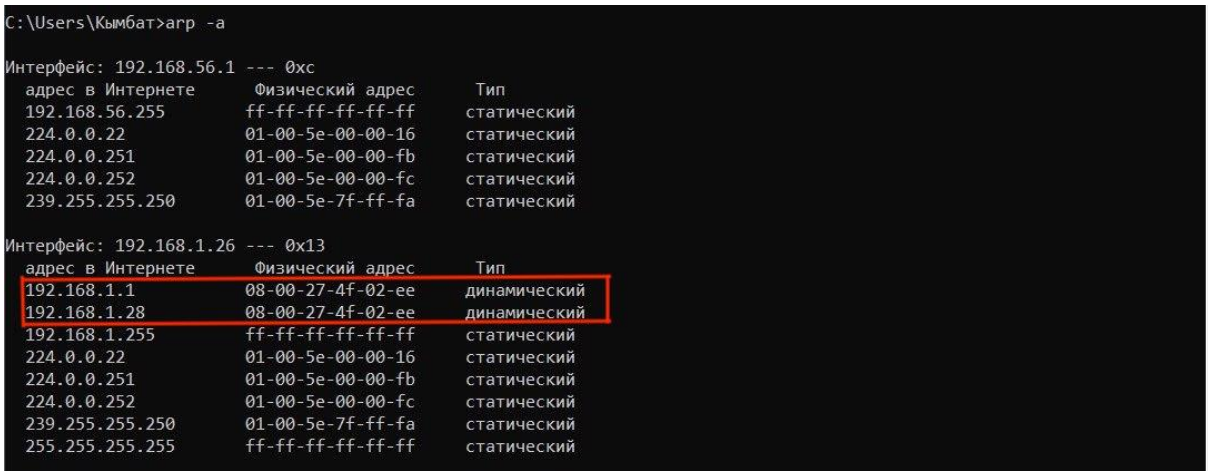

Figure 8: ARP poisoned cache table

As you can see in Figure 8, the MAC addresses of the hacker and the router are identical, resulting in a successful ARP spoofing attack. Now all traffic that will refer to the IP address of the router will also be available to the hacker.

The success of an injected attack can be verified by sending any request from the attacked user's host. For example, the *pinggoogle.com* command was chosen.

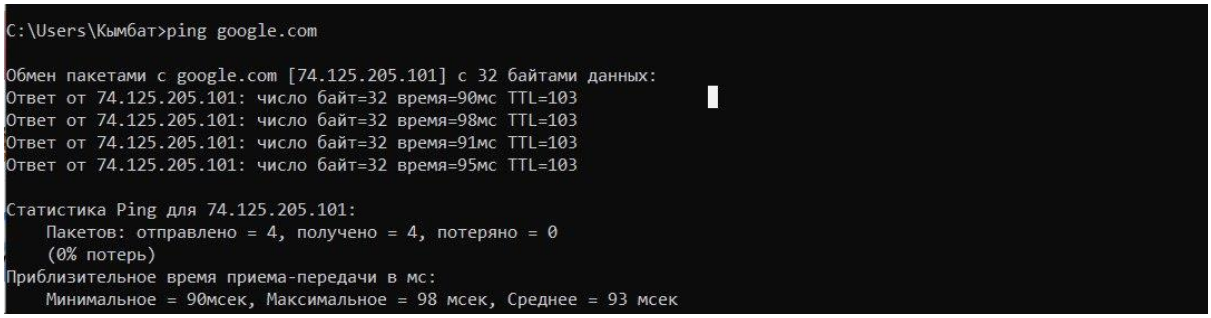

Figure 9: Example of request sending

This request is needed to check the integrity of connections based on TCP / IP, which goes along the route Router -> Internet.

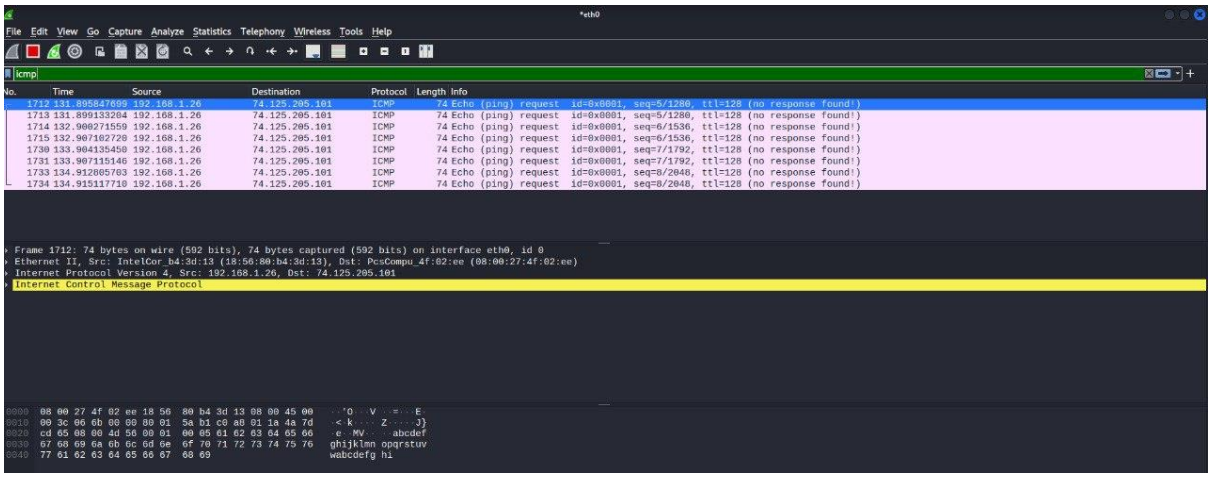

Figure 10: Traffic capturing of User and Router

Since requests sent by the user to the Internet pass through the Router, an attacker can intercept them using Wireshark. As described earlier in Figure 9, ping requests were sent, which were successfully intercepted by the attacker, and ICMP filtering was used to view these requests (Figure 10).

6. Detection method with Wireshark

The first method for detecting an embedded ARP spoofing attack is to check the ARP cache using the $arp - a$ command, as shown in Figure 8. If there are two identical MAC addresses in the table for both the gateway and the other host, then this indicates an ARP spoofing attack.

Also, to detect this attack, a script was written with several filtering in Wireshark, which allows real-time tracking of successful and unsuccessful attempts to implement an ARP spoofing attack.

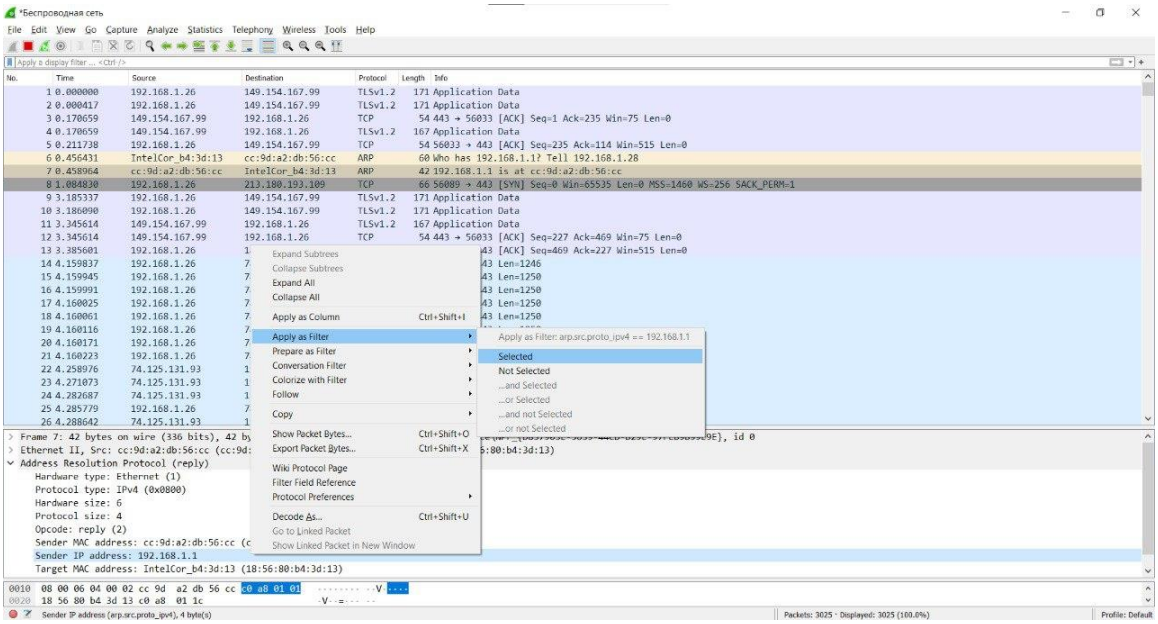

Figure 11: Filtering for an ARP poisoned attack

With the help of the work done, filters were selected, the totality of which reflects ARP spoofing attack attempts (Figure 11).

The first filter is needed to intercept all ARP protocol packets from the Router.

The next filter to be added is opcode: reply (2). This filter is needed to intercept packets with a Reply response.

And the final filter is capturing all packets whose MAC addresses do not correspond to the real ones.

In the aggregate of these filters, monitoring of ARP spoofing attacks is obtained (Figure 12): ((arp.src.proto_ipv4 == GATEWAY IP ADDRESS) && (arp.opcode == 2)) && !(arp.src.hw_mac == REAL GATEWAY MAC ADDRESS)

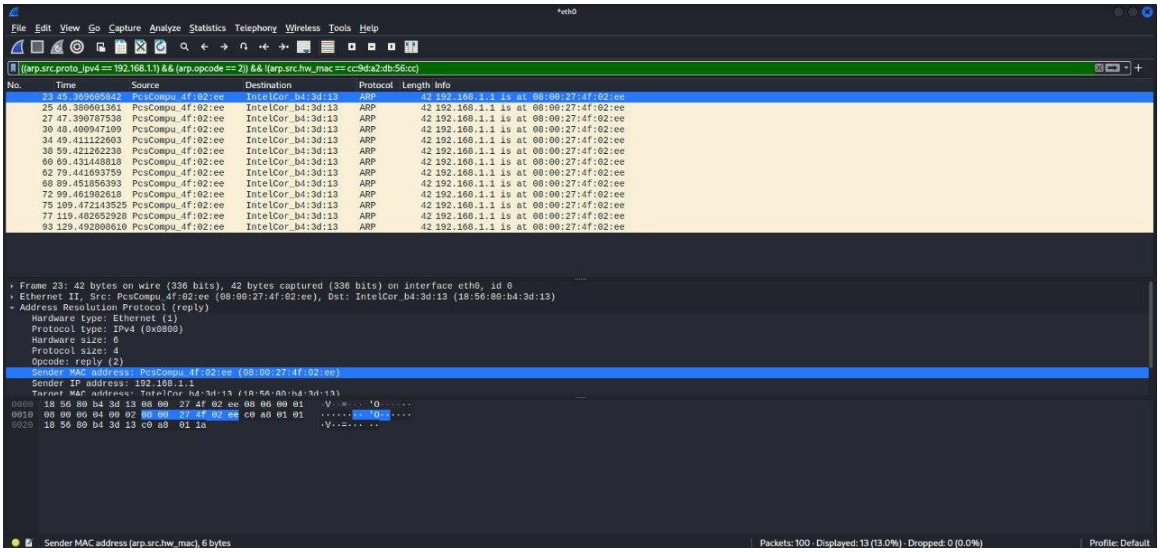

Figure 12: ARP spoofing attack monitoring in real time

7. Prevention methods

As is known, the prediction of future actions of an attacker is one of the most important goals here. However, these techniques are not very effective in predicting future action of the attacker.[14, 15] The following are guidelines that can help protect networks from ARP spoofing attacks:

1. Use static ARP to stop devices from listening for ARP answers for a certain IP address. Static ARP entries are defined using the ARP protocol. If a workstation consistently connects to the same router, for instance, you may set a static ARP entry for that router to thwart attacks.
2. UtilizepacketfilteringByseeingcontradictingsourceinformationinARPpackets, packet filtering solutions may detect poisoned ARP packets [16] and prevent them from reaching network devices.
3. Use a Virtual Private Network (VPN)—a VPN enables connections to the Internet over a secure tunnel for devices. This renders every communication encrypted and useless to an attacker using ARP spoofing.
4. Runaspoofingattack—checkifyourexistingdefencesareworkingbymountingaspoofing attack, in coordination with IT and security teams. If the attack succeeds, identify weak points in your defensive measures and remediate them.

8. Conclusion

As a result of the work carried out, a cyber threat imitation was modelled using Ettercap to determine methods for detecting and eliminating ARP spoofing attacks.

The manually simulated attack helped visualize the emerging threat on the internal network. Research work has been done in the Wireshark software to detect anomalous traffic and output- specific filters to detect ARP spoofing.

In conclusion, two ways to solve the problem of ARP spoofing were deduced, and recommendations were given to avoid most attacks by poisoning the cache.

9. References

[1] V. K. Tchendji, F. Mvah, C. T. Djamegni, Y. F. Yankam, E2basep: Efficient bayes based security protocol against arpspoofing attacks in sdn architectures, Journal of Hardware and Systems Security 5 (2021) 58–74. doi:10.1007/s41635-020-00105-x.

[2] M. Alam, Investigating ARP poisoning, 1st ed., LAP LAMBERT Academic Publishing, New Delhi, 2018. doi:10.6084/m9.figshare.14706240, (book).

[3] A.B. Al-Khalil, H. Khalid, Efficient mechanism for securing software defined network against arp spoofing attack, Journal of University of Duhok 22 (2019). doi:10.26682/sjuod. 2019.22.1.14.

[4] Y. Aitkhozhayeva, A. Ziro, Z. Zhaibergenova, A. Baltabay, Penetration testing, The Bulletin of the National Academy of Sciences of the Republic of Kazakhstan 6 (2018) 39–44. doi:10.32014/2018.2518-1467.25.

[5] J. D. Brown, T. J. Willink, Arp cache poisoning and routing loops in ad hoc networks, Mobile Networks and Applications (2018) 1306–1317. doi:10.1007/s11036-018-1039-6.

[6] SecurityOps., Critical Cybersecurity Statistics You Must Know for the Last Several Years, Technical Report, 2021.

[7] P. Technologies, Актуальные киберугрозы: I квартал 2022 года, Technical Report, 2022.

[8] P. Technologies, Статистика уязвимостей корпоративных информационных систем за 2011-2012 годы, Technical Report, 2013.

[9] M. Husak, P. Celeda, Predictions of network attacks in collaborative environment, Network Operations and Management Symposium, 2020, pp. 1–6. doi:10.1109/NOMS47738.2020. 91104725.

[10] T. Girdler, V. G. Vassilakis, Implementing an intrusion detection and prevention system using software-defined networking: Defending against arp spoofing attacks and blacklisted mac addresses, Computers and Electrical Engineering) 90 (2021) 106990. doi:10.1016/j.compeleceng.2021.106990.

[11] M.F. Baimuhamedov, S. Atanov, K. M. Zhunusov, A. Zhikeyev, A. Bugubaeva, A. Bulaev, System of cryptographic protection of information based on deterministic chaos, International Journal

of Innovative Technology and Exploring Engineering (IJITEE) 8 (2019) 1306–1317. doi:10.35940/ijitee.L3527.1081219.

[12] B. Prabadevi, J. Nagamalai, A framework to mitigate arpsniffing attacks by cachepoisoning, International Journal Advanced Intelligence Paradigms 10 (2018) 146–1059. doi:10.1504/IJAIP.2018.10010532.

[13] S. Atanov, A. Z. Bigalieva, N. K. Apachidy, A. V. Rusak, Process control issues of fine grinding in a planetary mill, Vestnik of Saint Petersburg University Applied Mathematics Computer Science Control Processes 16 (2020) 277–292. doi:10.21638/11701/spbu10.2020. 306.

[14] H. Albasheer, M. Siraj, A. Mubarakali, Cyber-attack prediction based on network intrusion detection systems for alert correlation techniques: A survey, Sensors 22 (2022). doi:10.3390/s22041494.

[15] A.K. Kereyev, S.K. Atanov, K.P. Aman, Z.K. Kulmagambetova, B.T. Kulzhagarova, Navigation system based on Bluetooth beacons: Implementation and experimental estimation, Journal of Theoretical and Applied Information Technologies 98 (2020).

[16] Z. Mukanova, S. Atanov, M. Jamshidi, Features of hardware and software smoothing of experimental data of gas sensors, International Journal of Innovative Technology and Exploring Engineering (2021). doi:10.1109/SIST50301.2021.9465981.