Software Modeling and Implementation of Information Network for Smart Home Technology

Juliy Boiko[1,*,†], Volodymir Druzhynin[2,†], Ilya Pyatin[3,†] and Lesya Karpova[1,†]

[1] *Khmelnytskyi National University, 11, Instytuts'ka str., Khmelnytskyi, 29016, Ukraine*

[2] *Taras Shevchenko National University of Kyiv, 60 Volodymyrska str., Kyiv, 01033, Ukraine*

[3] *Khmelnytskyi Polytechnic Professional College by Lviv Polytechnic National University, 10, Zarichanska str., Khmelnytskyi, 29019, Ukraine*

Abstract

The article discusses the design and control of the Internet of Things networks. The requirements for effective network management are defined. A model of the information network based on Smart Home technology in the Cisco Packet Tracer environment is built, user authentication is established, the address space is partitioned, smart devices are selected, and the requirements for the bandwidth of the information network are analyzed. A popular approach to implementing a Smart Home is to use sensors and cameras to monitor the home environment and detect motion and control the home environment, which alerts homeowners in the event of a security breach. Indoor temperature, humidity levels, motion detection data, and water level readings collected by sensors can be stored in a database on the server for further analysis. The system also uses the generated logs to monitor performance and identify potential threats and signal in the event of security breaches. The proposed Smart Home strategy, in comparison to traditional approaches, is characterized by enhanced system integration, improved scalability, optimized resource utilization, and heightened security.

Keywords

internet of things, smart home, information network, Wi-Fi, smart devices

1. Introduction

At present, the specifics of the deployment of the Internet of Things (IoT) environment are characterized by the presence of a wide range of diverse and generally resource-limited applications. There are a number of developed and standardized IoT protocols [1, 2]. Among such technologies, it is worth highlighting Zigbee, BLE, LoraWAN and Sigfox solutions, as well as individual solutions for network management in the LWM2M, CoMI format [3]. Communication protocols are relevant when using means with limited resources, and solutions have been developed for routing such devices, such as 6LowPAN and RPL, respectively.

However, as the analysis of works [4, 5, 6] shows, due to heterogeneity and certain resource limitations, the implementation of IoT networks is associated with a number of problematic issues that ultimately affect their performance. Mainly, as discussed in [7], such problems are caused by the quality of reliable communication, the consequences of network overload, and failure of IoT devices. In this context, an important problem arises, directly related to the implementation of the flexible IoT network management format to maintain performance indicators. Here, as noted in [8], it is important to ensure a low level of end-to-end latency or satisfactory energy efficiency. Analysis of

Information Technology and Implementation (IT&I-2024), November 20-21, 2024, Kyiv, Ukraine

* Corresponding author.

† These authors contributed equally.

boiko_julius@ukr.net (J. Boiko); v_druzhinin@ukr.net (V. Druzhynin); ilkhmel@ukr.net (I. Pyatin); rtlesya@gmail.com (L. Karpova)

0000-0003-0603-7827 (J. Boiko); 0000-0002-5340-6237 (V. Druzhynin); 0000-0003-1898-6755 (I. Pyatin); 0000-0001-5015-2107 (L. Karpova)

current works on IoT [9, 10] allows us to formulate a list of requirements for the implementation of flexible control of IoT networks, among which it is necessary to highlight the functions of resource provision, authentication, routing and monitoring [11]. In addition, it is important to ensure timely software updates for the relevant devices, in particular their firmware, error correction [12, 13, 14], etc. Thus, the implementation of the above functional slots allows us to form a network service environment in order to maintain the performance indicators of IoT, in the form presented in Figure 1.

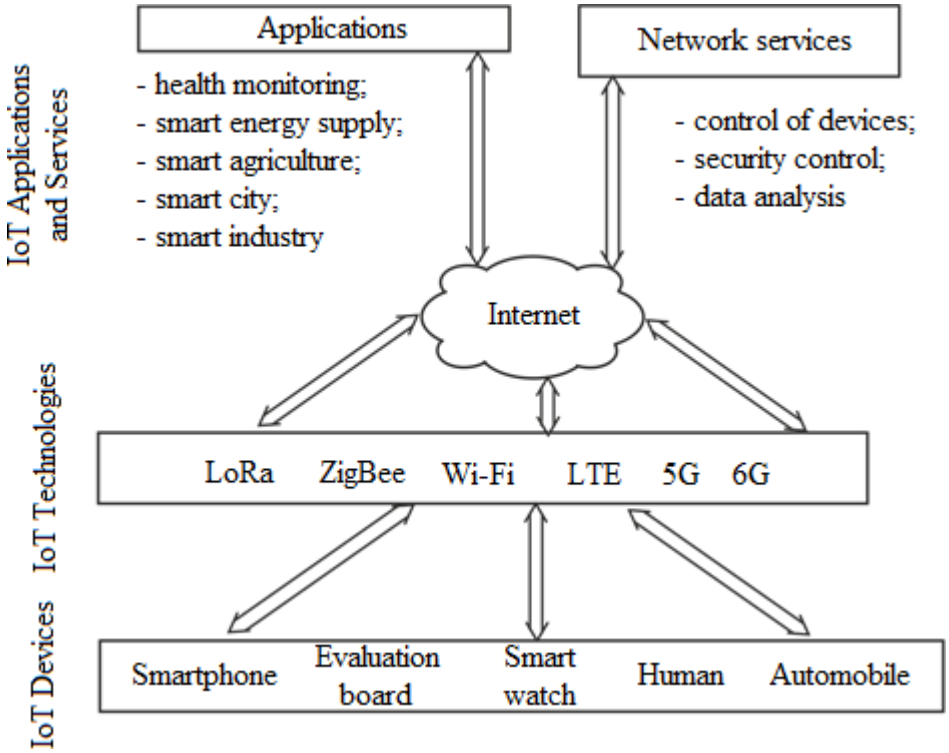

Figure 1: The concept of forming the IoT architecture.

The model in Figure 1 includes IoT devices, IoT technologies, and IoT applications and services. Devices usually have a wireless module that corresponds to a specific IoT technology: LoRa, ZigBee, Wi-Fi. Information exchange is provided by a specific protocol. In this case, in the presented article, when organizing the smart home (SH) network, we use Wi-Fi technology [15, 16]. At the top level of the model, there are applications that allow you to configure the interaction of intelligent devices. These are some applications and network services.

In the works [17, 18] it was emphasized that the implementation of the SH project allows for an unprecedented level of control and volume in order to gain access and control over home devices from the subscriber's current location at the required time. In general, as noted in the works [19], the main purpose of smart devices is to create an interconnected ecosystem inside the home, where IoT technology is used as the main one for device control. As discussed in the works [20, 21], in this context we can talk about the formation of a network of physical devices containing appropriate sensors and allowing for data exchange in the IoT format [22].

The content of the presented work is aimed at supplementing and implementing through modeling the proposed concept of building an information network of the SH type. We used the Cisco Packet Tracer (CPT) environment to design such a network. The implementation of the proposed network architecture is realized through a user authentication mechanism, partitioning the address space, choosing reasonable devices and analyzing the bandwidth requirements of the proposed network. The proposed SH system uses generated logs to monitor performance and identifies potential threats and signals in case of security breaches.

2. Control methods in IoT networks

This section of the article analyses possible approaches to control methods in IoT networks. A classification of control solutions in the network is presented. A low-power IoT control architecture is described. Low-power IoT network management protocols have been developed to ensure and optimize network performance while using small resources for network control operations.

2.1. Conceptual foundations in IoT control solutions

The concept of network control is based on a number of operations, among which it is advisable to highlight: monitoring in relation to devices; providing the control process with routing and security. The main direction of such operations is associated with increasing network performance, in particular, in the context of minimizing delays, reducing energy consumption, localizing packet loss, etc. Consequently, it is possible to highlight a typical control structure based on the formation of logical subsystems based on a network manager, managed devices and agents. Thus, Figure 2 presents the concept of engaging functional elements activating the network control process [23].

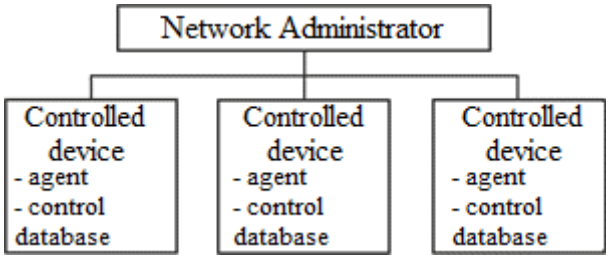

Figure 2: Devices participating in the control network.

According to Figure 2, the "Network Administrator" provides overall control of a group of nodes. The "Controlled device" refers to a network device that provides a set of parameters (e.g. IP address, CPU load, remaining battery charge, etc.) that are control (via read/write operations) by the network manager. The "Agent" refers to the software running on the managed device. It collects raw data from the control device and transmits it in a usable format to the network manager. The control database contains information about the parameters of the control device. Messaging protocols can be used to exchange information between the network manager and the control devices. This allows the network manager to receive parameters from the control devices and make appropriate decisions on reconfiguring the network devices.

There are several key requirements for managing IoT networks. Accordingly, the key requirements for effective IoT performance can be formulated as follows: scalability, fault tolerance, energy efficiency, quality of service (QoS) [24], and security. Consequently, IoT must provide low power consumption with the ability to expand by adding new devices (Figure 3).

It is equally important to satisfy the fault tolerance requirement. The point is that such a requirement must guarantee that the network will perform as expected in the presence of a fault (e.g. node fault, network fault, receiver fault, software fault) in the network. QoS characterizes the degree of consumer satisfaction. This requirement includes mechanisms for localizing packet loss, minimizing delays, etc. The energy efficiency requirement imposes obligations to perform the main functions of IoT with minimal power consumption, which is especially relevant in the context of using battery power.

Next, we discuss such a requirement as security. Having a secure network is the key to preventing potential risks of data forgery. Self-configuration refers to the ability of IoT devices to adapt their behavior in accordance with the network state.

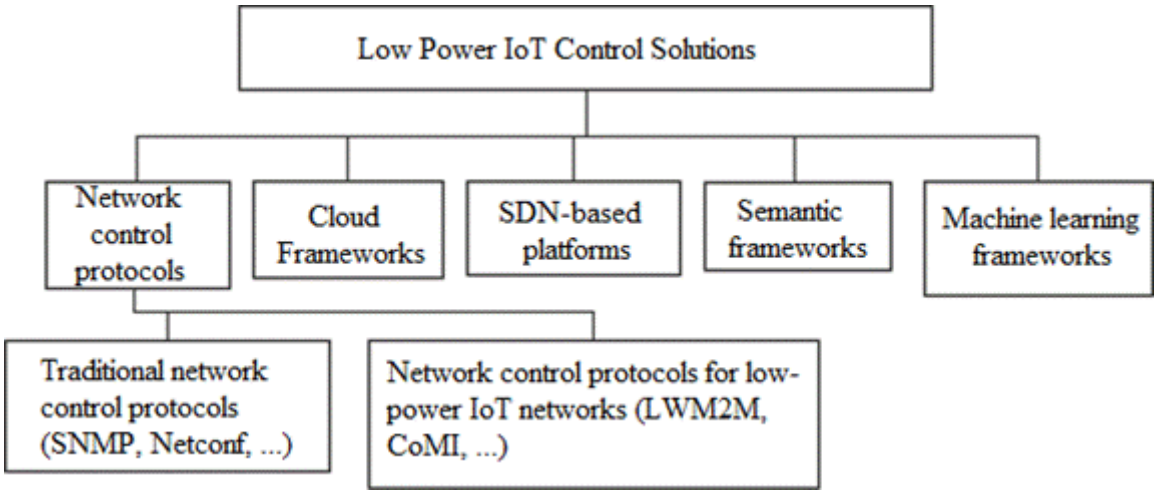

Figure 3: Low power IoT Control Solutions.

By analyzing the listed requirements for IoT, approaches to implementing network control solutions for devices with limited resources can be formed. These solutions can be used to create certain categories (Figure 3) of control, in particular, as network control protocols for low-power IoT networks, SDN-based platforms, cloud platforms, semantic frameworks, and machine learning frameworks.

2.2. Low-power IoT network control approaches

There are various network management protocols for remote control of devices with limited resources. These protocols include: LWM2M [25], CoMI, NETCONF Light and 6LowPAN-SNMP (Figure 4).

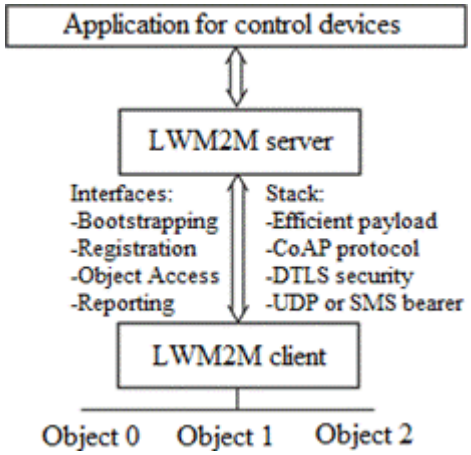

Figure 4: LWM2M Architecture.

LWM2M is a client-server protocol designed for low-power IoT device control. The LWM2M server resides on the network manager device, and the LWM2M client is typically hosted on the control devices. IoT device resources are organized into objects (e.g., a location object that contains all the resources that provide location information for IoT devices). CoMI is a control interface designed for low-power IoT devices and networks. This network control protocol enables resource management operations of IoT devices. 6LowPAN-SNMP is an adaptation of SNMP for IPv6 low-power wireless personal area network (6LowPAN). An example of such an architecture is shown in Figure 5.

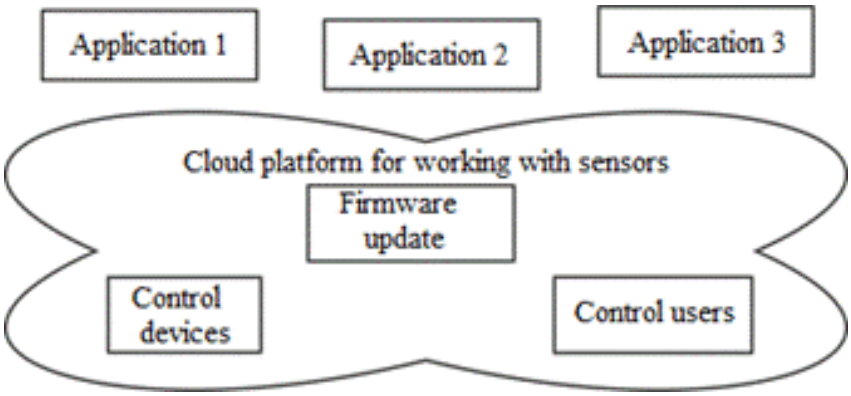

Figure 5: Architecture of control of smart devices based on a cloud platform for working with sensors.

3. Building a smart home model

In this chapter, we introduce the proposed SH network model. The process of setting up a wireless SH network will be discussed. The format for setting up the connection between smart devices and the server will be described.

3.1. Setting up the SH network model

SH systems are now being deployed in private companies, government agencies, and residential buildings to automate operations that make life and work more convenient: they control lighting, household appliances, monitor the home, etc. To build an SH model, we will use CPT. In Figure 6, we present a structural diagram of the designed information network using SH technology. The network has sections with wired and wireless connections. The global network provider connects two offices using routers Router 1 and Router 2.

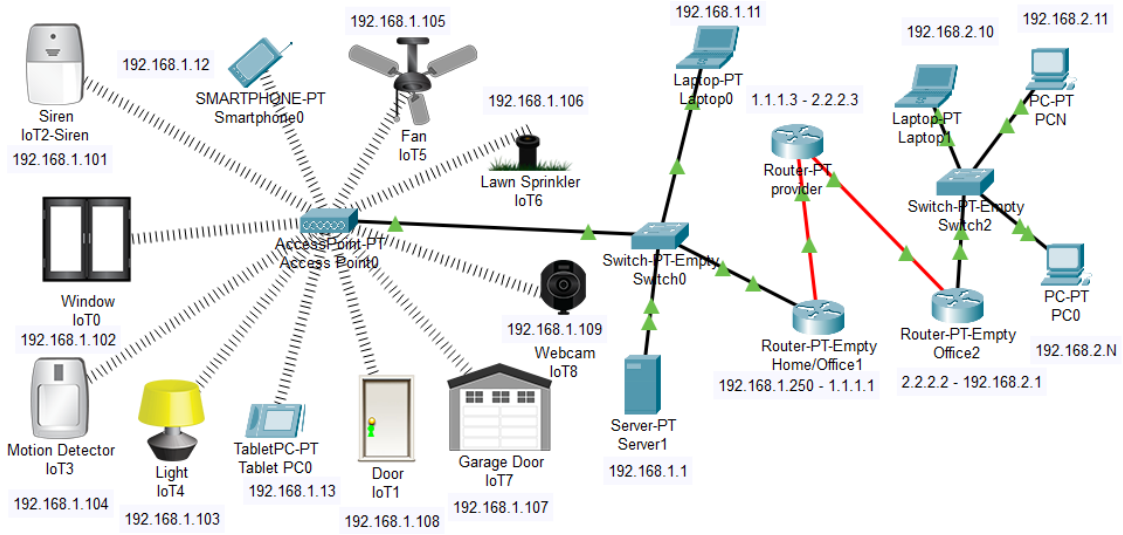

Figure 6: Structural diagram of the proposed information network using SH technology: IoT0 is the window control; IoT1 is the door control; IoT2 is the siren control; IoT3 motion detector; IoT4 is the light control; IoT5 is the wall fan control; IoT6 is the lawn sprinkler; IoT7 is the garage door; IoT7 is the webcam control.

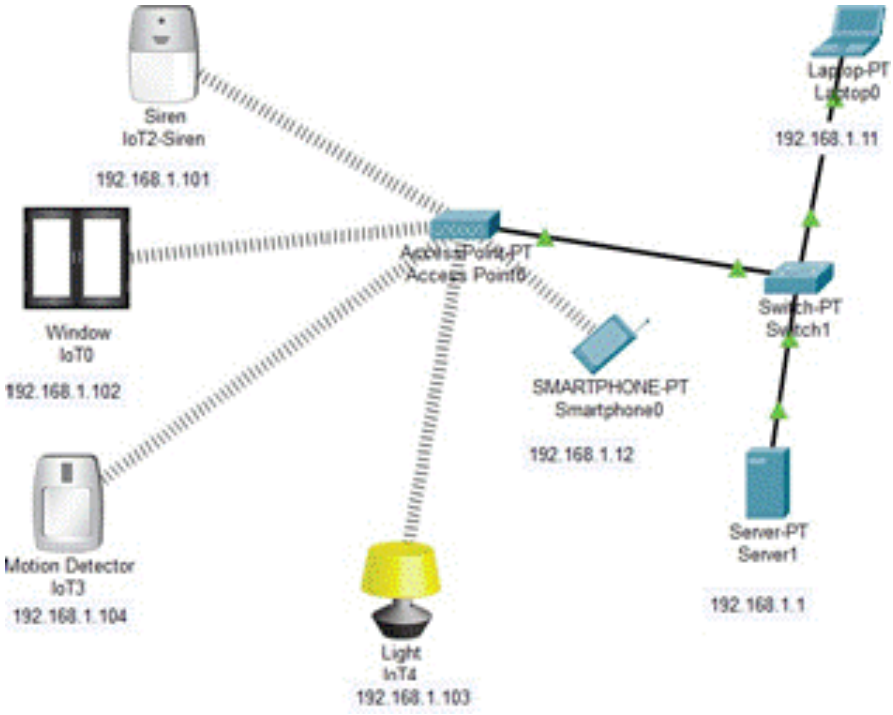

Figure 7: First office network.

SH network and monitoring of connected devices in the laptop web browser. Figure 8 shows the settings window for connecting smart devices to the network - siren (IoT2 - Siren).

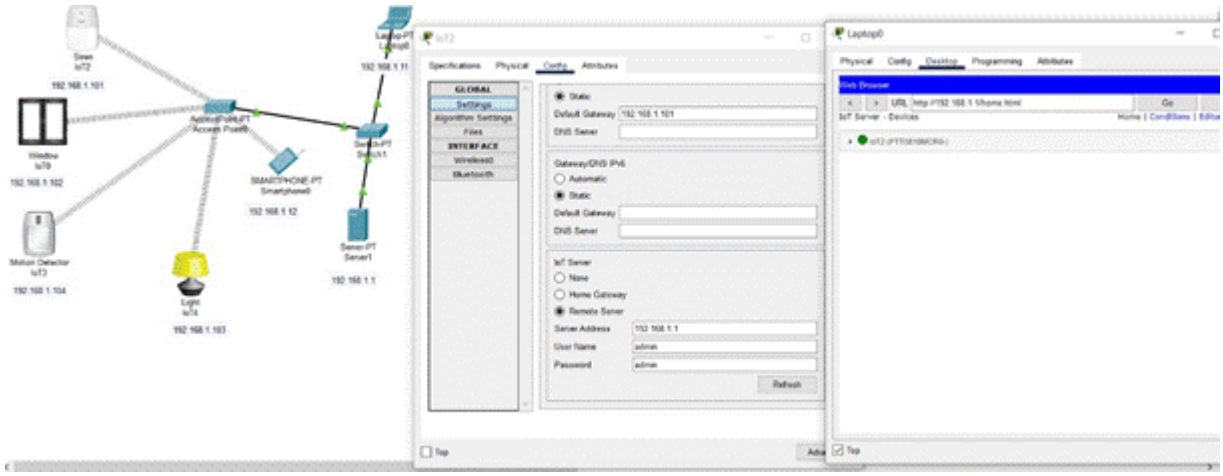

Figure 8: Settings for connecting smart devices to the network.

The physical level configuration for connecting a device named IoT4 is shown in Figure 9. After all smart devices are connected to the network, it is necessary to configure the actions performed when certain events occur: when a window is opened, a siren is triggered, which can only be excluded by the user; when a motion detector is triggered, the lighting is turned on. To do this, go to the Conditions tab in the laptop web browser (Laptop 0) from the Home tab. The settings window in the laptop browser is shown in Figure 10. The alarm setup - turning on the siren when a window is opened is shown in Figure 11.

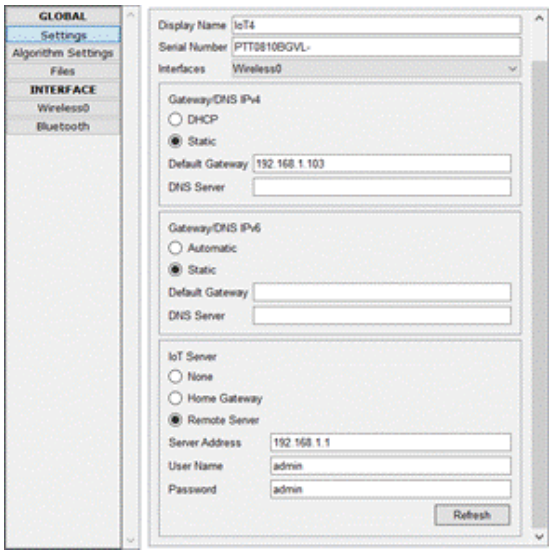

Figure 9: Settings window for connecting a device named IoT4.

Figure 10: Settings window in laptop browser.

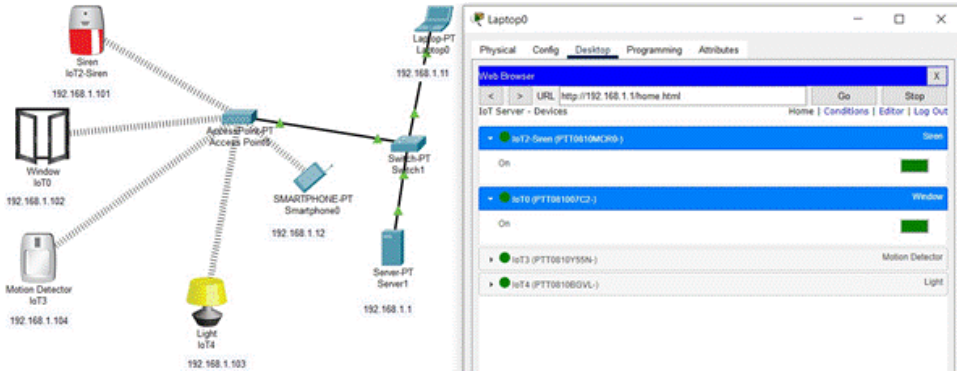

Figure 11: Display the ability to turn on the siren when opening a window.

If the alarm is not needed, we turn off the siren. Setting up smart devices in the laptop web browser (Laptop 0) is shown in Figure 12.

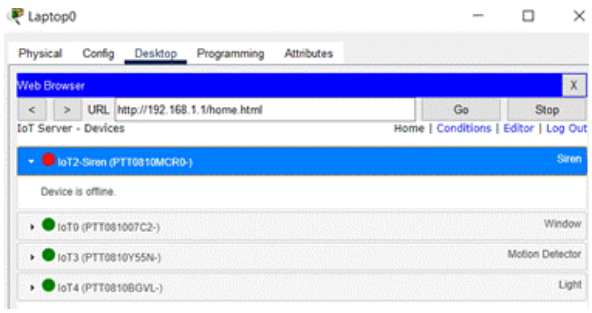

Figure 12: Setting up smart devices in your laptop's web browser.

Routers and switches of the local network are connected using twisted pair category 5e (see Figure 6). For four pairs the transmission rate is up to 1000 Mbit/sec, for a two-pair twisted pair, respectively, up to 100 Mbit/sec. The frequency band is 100 MHz [26].

Global connections with the provider are made using single-mode optic fiber [27].

To transmit packets to the global network, the first office has a gateway 192.168.1.250 with a white IP address of 1.1.1.1. Another office has a gateway 192.168.2.1 with a white IP address of 2.2.2.2. To work with smart devices in the network, there is a server 192.168.1.1 and workstations with a wired and wireless connection.

3.2. Setting up and control of the global SH network

When setting up a global network, we must be able to connect from the second office via the global network to the first office. This is done using a gateway. In the network of the first office, the gateway has the address 192.168.1.250. The Home/Office1 node setup window looks like (Figure 13).

For the second office, the gateway has the address 192.168.2.1. For each network device, we must write down the IP address of this device, the subnet mask, and the gateway. The Office2 node configuration window looks like this (Figure 14).

For office 2, we also need to specify a gateway to access the global network. In order for us to have access from the first office to the second and from the second to the first, we need to set up global connections. We have two routers. They have global IP addresses: for the first office 1.1.1.1 and for the second office 2.2.2.2. We need to record the default gateway in each office node - this is the router at 192.168.1.250. We need to do the same with the second office.

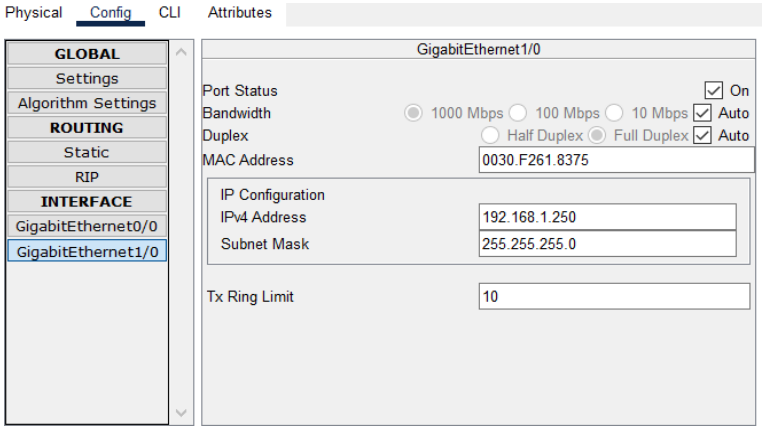

Figure 13: Home/Office1 Node Configuration Window.

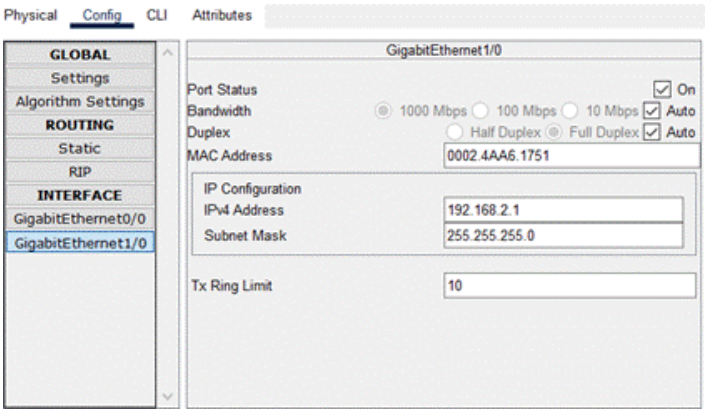

Figure 14: Office2 Node Configuration Window.

The window for configuring Gigabit Ethernet addresses of the provider node looks like (Figure 15).

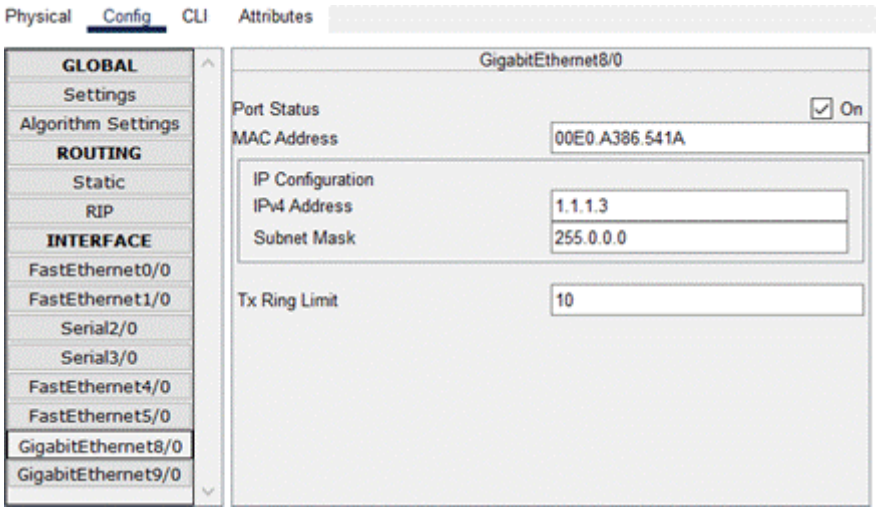

Figure 15: Gigabit Ethernet address configuration window for the provider node.

Before setting up routing tables on the routers, let's check for a connection with the first router in the second office. On the Laptop 1 node, open the command line, as shown in Figure 16.

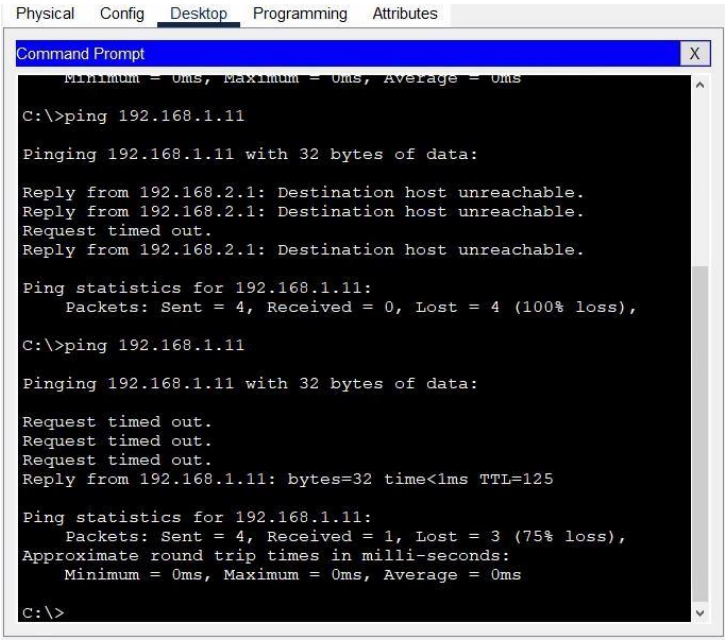

Figure 16: Command line on node Laptop 1.

To ensure communication between the second office and the first, requests from nodes at the first address 192.168.1.0 with a mask of 255.255.255.0 must be redirected to the router port with the address 2.2.2.3.

Open the static address settings window for the Home/Office1 node and write down that all requests from nodes 192.168.2.0 should be forwarded to router 1.1.1.3.

Only after this we will configure the routing table on the provider router. All requests coming to the 192.168.1.0 network should be transmitted to the router with the address 1.1.1.1, and requests to the address 192.168.2.0 should be sent to the router with the address 2.2.2.2.

Open the command line in the node (Laptop 0) of office 2 and ping node 11, located in the first office. In this case, it is possible that the first three sent packets were lost, which is related to the compilation of the routing table. When the routing table is configured with the server 192.168.1.1, the first ping remains unanswered. Then three packets arrive successfully.

Let's add a new device to the network - a tablet, from which we can control the operation of smart devices in the house and configure them according to Figure 17.

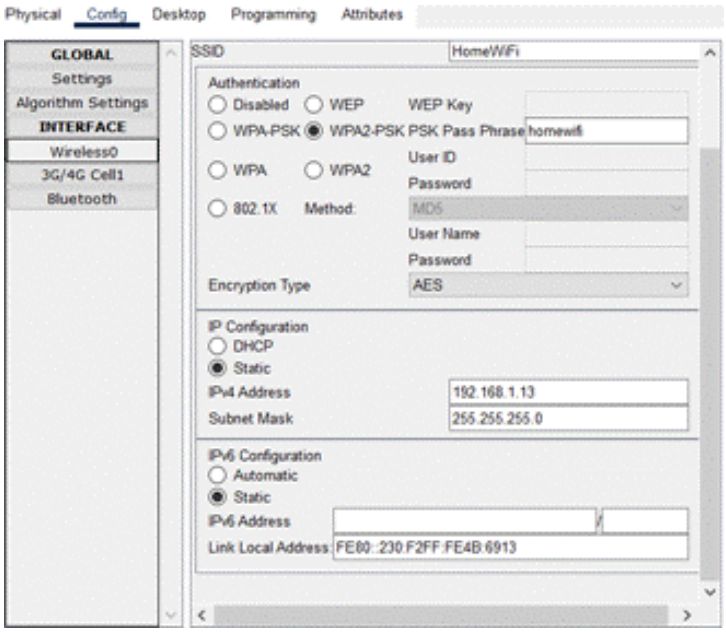

Figure 17: Wireless network settings window for tablet

In Figure 17 we have shown the configuration in case of configured Wi-Fi parameters.

After pinging the presence of Tablet PC 0 on the network, we connected to the web server and checked the ability to control smart devices at home.

After entering the login and password, a window opens in which all connected smart devices are displayed, as shown in Figure 18.

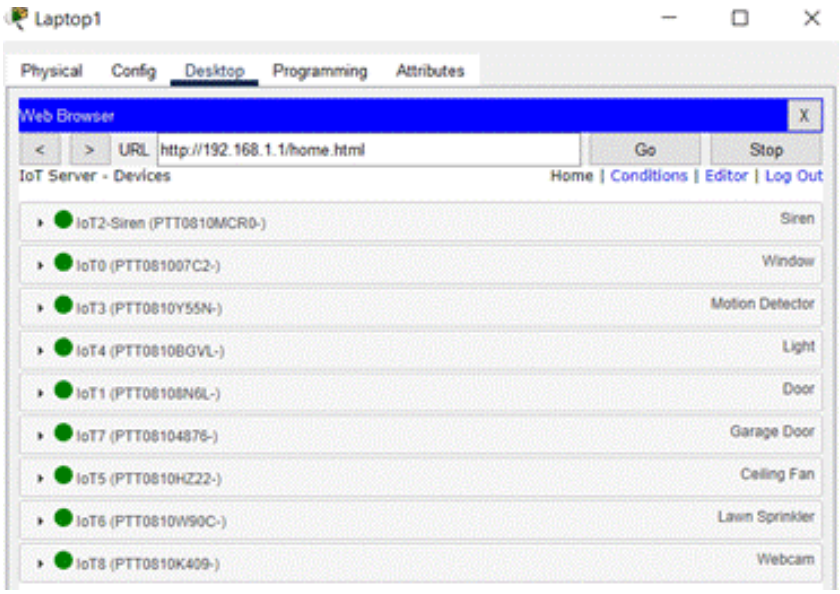

Figure 18: Smart Devices Settings Window of the laptop1 node

3.3. Modeling the scaling process of the SH network

By scaling the SH network, we added entrance doors to the building and garage. There is a device at the door that records the state of closing and opening, which is connected to the network using a radio module. We configure the connection of this device according to Figure 19.

We set up the garage door in a similar way. We also included a sensor that works via Wi-Fi [16].

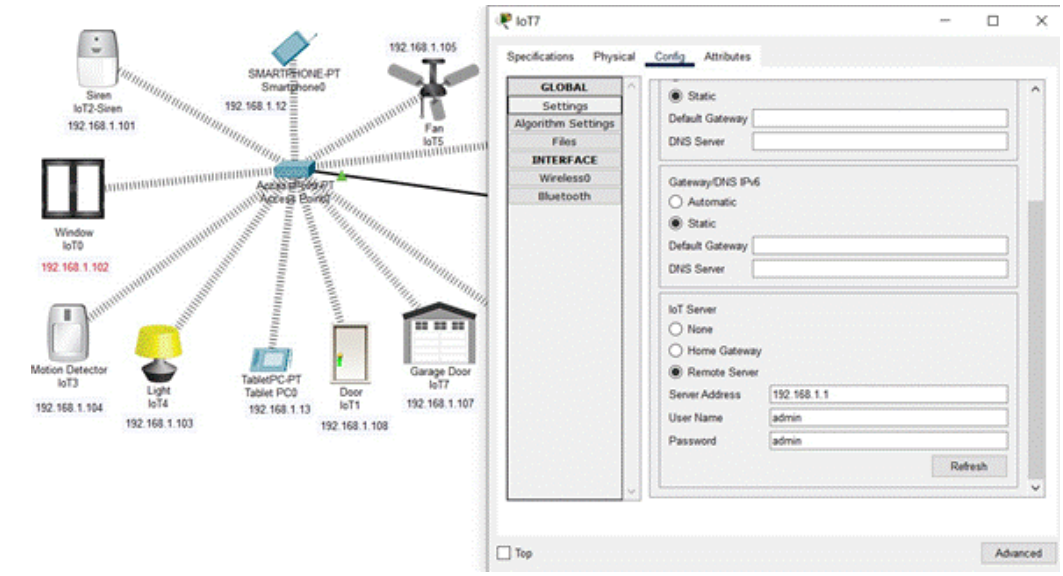

Figure 19: Connecting a Smart IoT7 Device

Next, we established a connection between the smart devices and the server that controls them. Everything is shown in Figure 20.

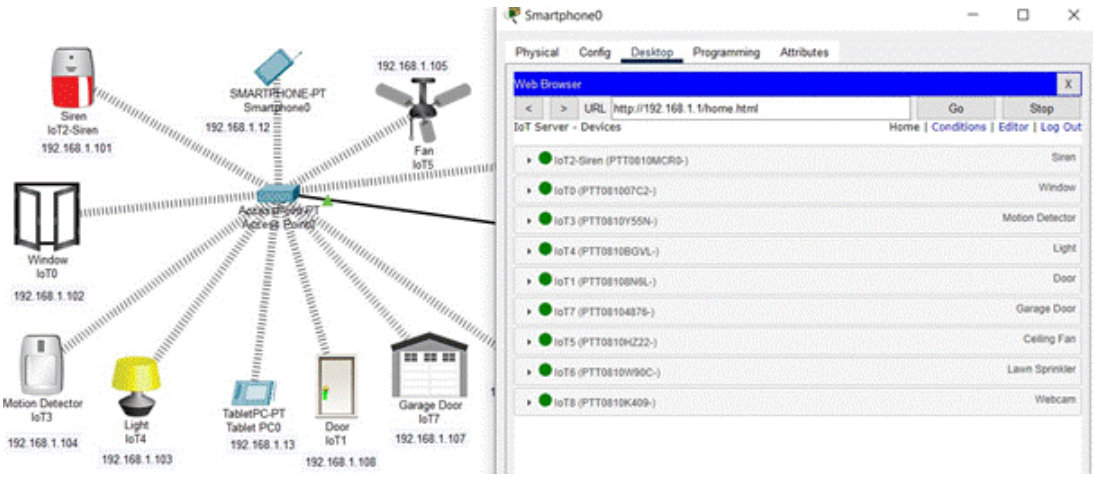

Figure 20: Communication between smart devices and server

Now the user needs to remotely check whether the door lock is closed – he can do this using the IoT Server – Device Conditions window, as shown in Figure 21.

Below we present the calculation of the required SH network bandwidth [28, 29]. We take into account that for each 0.1-megapixel resolution of the webcam, two Mbit/s of Internet rate are required to ensure reliable connection (Table 1).

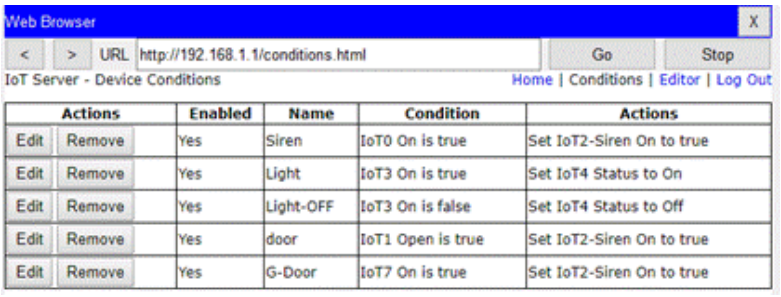

Figure 21: IoT Server Settings Window – Device Conditions

Table 1
Determining the bandwidth of a camera with different resolutions

Frame size	Number of pixels	Frame frequency (frames/sec)	Rate (Mbit/s)
320·340	76800	25	1.6
640·480	307200	25	6.0
1296·972	1259712	25	26.0
1640·1232	2020480	25	40.0

To calculate the bandwidth of the SH network at home using an IP video camera, the following expression was used:

$$B = \frac{F_{fs} \cdot 1024 \cdot 8 \cdot R \cdot N}{10^6}, \quad (1)$$

where F_{fs} is the frame frequency; R is the video resolution; N is the total number of cameras involved in the network.

Below we present the calculation of the bandwidths of cameras with different codecs and summarize it in Table 2.

Table 2
Key camera bandwidth indicators depending on codec type

Frame size	Video resolution (MP)	Codec type	Rate (Mbit/s)
1280·720	1	H.264	2.0
1280·720	1	mjpeg	6.0
1920·1080	2	H.264	4.0
1920·1080	2	mjpeg	12.0
2560·1440	4	H.264	8.0
2560·1440	4	mjpeg	24.0

It is important to note that increasing the frame size affects the quality of recognition of small details. If we set the camera to turn on when the motion detector is triggered, we can reduce the required Internet rate. It should be emphasized that depending on the location of the video camera, different bandwidth can be obtained. Here it is important to determine whether the cameras are located outdoors or indoors. It should also be taken into account that some cameras have high resolution or purity of recording of frame sequences, due to the built-in image processing algorithm. In this case, the bandwidth increases.

We also provide a flow chart for sending messages to an IoT network user (Figure 22).

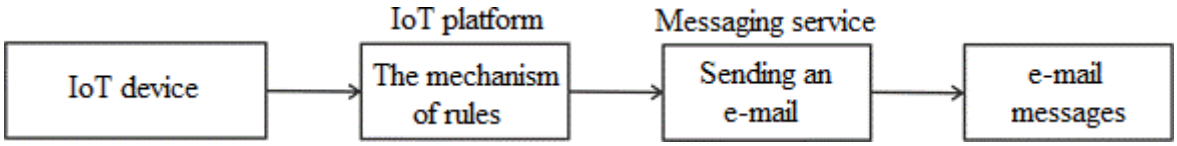

Figure 22: IoT Server Settings Window – Device Conditions

So, in accordance with Figure 22, we record the following sequence of actions. Using the built-in Wi-Fi [12, 16], the IoT device sends information from the sensors to the cloud service. The IoT platform forms a certain set of rules that have the ability to activate according to certain signs - opening the garage, opening the window or using the motion detector, that is, what is described above in our network [30]. The resulting set of rules includes a message service and information is sent to e-mail. Thus, the rate of IoT response in the cloud service [31, 32] database increases.

However, network control protocols are not able to meet all the requirements of low-power IoT networks mentioned earlier. Let us consider cloud platforms for control low-power Internet networks. Cloud computing is a model that provides ubiquitous, convenient, on-demand network access to a shared pool of computing resources [33]. The architecture of low-power IoT network control on a cloud platform consists of three layers: 1) the first layer consists of resource-constrained devices; 2) the second level consists of cloud infrastructure; 3) the third level consists of IoT applications.

The IoT network deployment solutions described in Section 2 formed the basis for the SH network design process presented in Section 3.

4. Conclusion

This paper describes the process of building a model of the SH network in the environment. According to the simulation results, user authentication is established, the address space is partitioned, smart devices are selected, and the bandwidth requirements of the IoT network are analyzed. The owner can access the SH from anywhere in the world using a smartphone. The use of sensors and cameras is configured to monitor the home environment and detect motion and control the home environment, which alerts homeowners in the event of a security breach. Different programming languages of sensor boards and smart devices are used to build the network. The indoor temperature, humidity level, motion detection data and water level readings collected by the sensors can be stored in the database on the server for further analysis. The system also uses the generated logs to monitor performance and identify potential threats and alarms in case of security breaches. The calculation of the required network bandwidth to support video data from multiple IP cameras in SH settings is provided.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," IEEE Internet of Things Journal, 4.5 (2017): 1125-1142, doi:10.1109/JIOT.2017.2683200.

[2] Kamaldeep, M. Malik, M. Dutta, J. Granjal, "IoT-Sentry: A Cross-Layer-Based Intrusion Detection System in Standardized Internet of Things," IEEE Sensors Journal, 21.24 (2021): 28066-28076, doi:10.1109/JSEN.2021.3124886.

[3] A. Garcés-Jiménez, A. Rodrigues, J. M. Gómez-Pulido, D. Raposo, J. A. Gómez-Pulido, J. Sá Silva, F. Boavida, "Industrial Internet of Things embedded devices fault detection and classification. A case study," Internet of Things, 25 (2024): 101042, doi:10.1016/j.iot.2023.101042.
[4] X. Deng, J. Zhu, X. Pei, L. Zhang, Z. Ling, K. Xue, "Flow Topology-Based Graph Convolutional Network for Intrusion Detection in Label-Limited IoT Networks," IEEE Transactions on Network and Service Management, 20.1 (2023): 684-696, doi:10.1109/TNSM.2022.3213807.
[5] A. Campbell, M. E. Hariri, M. Parvania, "Asynchronous Distributed IoT-Enabled Customer Characterization in Distribution Networks: Theory and Hardware Implementation," IEEE Transactions on Smart Grid, 13.6 (2022): 4392-4404, doi: 10.1109/TSG.2022.3182210.
[6] M. Rostami, S. Goli-Bidgoli, "An overview of QoS-aware load balancing techniques in SDN-based IoT networks," Journal of Cloud Computing, 13.89 (2024), doi:10.1186/s13677-024-00651-7.
[7] K. Erzun, R. Avoub, P. Mercati, T. Rosing, Improving Mean Time to Failure of IoT Networks with Reliability-Aware Routing, in: Proceedings of the 2021 10th Mediterranean Conference on Embedded Computing, MECO, IEEE Press, Budva, Montenegro, 2021, pp. 1-4, doi:10.1109/MECO52532.2021.9460211.
[8] G. Zhang, F. Shen, Z. Liu, Y. Yang, K. Wang, M. -T. Zhou, "FEMTO: Fair and Energy- Minimized Task Offloading for Fog-Enabled IoT Networks," IEEE Internet of Things Journal, 6.3 (2019): 4388-4400, doi:10.1109/JIOT.2018.2887229.
[9] P. Anitha, H. S. Vimala, J. Shreyas, "Comprehensive review on congestion detection, alleviation, and control for IoT networks," Journal of Network and Computer Applications, 221 (2024): 103749, doi:10.1016/j.jnca.2023.103749.
[10] X. Li, S. Wang, J. Cao, "An IoT-Enabled Control Paradigm for Building Process Control: An Experimental Study," IEEE Internet of Things Journal, 11.9 (2024): 15465-15474, doi:10.1109/JIOT.2023.3348125.
[11] C. Li, T. Yashiro, AFWA: Flexible IoT Access Control Framework with Web API Integration, in: Proceedings of the 2022 IEEE 4th Global Conference on Life Sciences and Technologies, IEEE Press, LifeTech, Osaka, Japan, 2022, pp. 354-356, doi:10.1109/LifeTech53646.2022.9754921.
[12] J. Boiko, I. Pyatin, O. Eromenko, L. Karpova, Evaluation of the Capabilities of LDPC Codes for Network Applications in the 802.11ax Standard, in: Joby, P.P., Alencar, M.S., Falkowski-Gilski, P. (Eds.), IoT Based Control Networks and Intelligent Systems. Lecture Notes in Networks and Systems, volume 789, Springer, Singapore, 2024, pp. 369–383, doi:10.1007/978-981-99-6586- 1_25.
[13] J. Boiko, V. Druzhynin, S. Buchyk, I. Pyatin, A. Kulko, "Methodology of FPGA Implementation and Performance Evaluation of Polar Coding for 5G Communications", CEUR Workshop Proceedings, 3654 (2024): 15-24, urn:nbn:de:0074-3654-7.
[14] B. Zhurakovskiy, J. Boiko, V. Druzhynin, I. Pyatin, "Performance Analysis of Concatenated Coding for OFDM Under Selective Fading Conditions", CEUR Workshop Proceedings, 3624 (2023): 403-413, https://ceur-ws.org/Vol-3624/Paper_33.pdf.
[15] A. Boni, V. Bianchi, A. Ricci, I. De Munari, "NB-IoT and Wi-Fi Technologies: An Integrated Approach to Enhance Portability of Smart Sensors," IEEE Access, 9 (2021): 74589-74599, 2021, doi:10.1109/ACCESS.2021.3082006.
[16] J. Boiko, I. Pyatin, V. Druzhynin, Possibilities of the MUSIC Algorithm for WI-FI Positioning According to the IEEE 802.11az Standard, in: Proceedings of the 2023 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo, IEEE Press, Kyiv, Ukraine, 2023, pp. 1-6, doi:10.1109/UKRMICO61577.2023.10380354.
[17] B. Zhurakovskyi, O. Nedashkivskiy, M. Klymash, O. Pliushch, M. Moshenchenko, Smart House Management System, in: Klymash, M., Luntovskyy, A., Beshley, M., Melnyk, I., Schill, A. (Eds.), Emerging Networking in the Digital Transformation Age. Lecture Notes in Electrical Engineering, volume 965, Springer, Cham, 2023, pp. 268–283, doi:10.1007/978-3-031-24963-1_15.
[18] M. Khan, B. N. Silva, K. Han, "Internet of Things Based Energy Aware Smart Home Control System," IEEE Access, 4 (2016): 7556-7566, doi:10.1109/ACCESS.2016.2621752.

[19] D. Pal, S. Funilkul, N. Charoenkitkarn, P. Kanthamanon, "Internet-of-Things and Smart Homes for Elderly Healthcare: An End User Perspective," IEEE Access, 6 (2018): 10483-10496, doi:10.1109/ACCESS.2018.2808472.
[20] P. Malini, Dr. K.R. Kavitha, "An efficient deep learning mechanisms for IoT/Non-IoT devices classification and attack detection in SDN-enabled smart environment," Computers & Security, 141 (2024): 103818, doi:10.1016/j.cose.2024.103818.
[21] S. Wan, Q. Li, H. Wang, H. Li, L. Sun, "DevTag: A Benchmark for Fingerprinting IoT Devices," IEEE Internet of Things Journal, 10.7(2023): 6388-6399, doi:10.1109/JIOT.2022.3225580.
[22] D. Wajgi, J.V. Tembhurne, R. Wajgi, T. Jain, Communication in IoT Devices, in: Gunjan, V.K., Ansari, M.D., Usman, M., Nguyen, T. (Eds.), Modern Approaches in IoT and Machine Learning for Cyber Security. Internet of Things. Springer, Cham, 2024, pp 21–44, doi:10.1007/978-3-031-09955-7_2.
[23] A. Jamali, B. Shahgholi Ghahfarokhi, M. Abedini, "Improving Performance of Association Control in IEEE 802.11ah-Based Massive IoT Networks," IEEE Internet of Things Journal, 9.11 (2022): 8572-8583, doi:10.1109/JIOT.2021.3114192.
[24] M. Singh, G. Baranwal, Quality of Service (QoS) in Internet of Things, in: Proceedings of the 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages, IoT-SIU, IEEE Press, Bhimtal, India, 2018, pp. 1-6, doi:10.1109/IoT-SIU.2018.8519862.
[25] A.J. Simla, C. Rekha, L.M. Leo, "Agricultural intrusion detection (AID) based on the internet of things and deep learning with the enhanced lightweight M2M protocol," Soft Computing (2023). doi: 10.1007/s00500-023-07935-1.
[26] B. Zhurakovskyi, J. Boiko, V. Druzhynin, I. Zeniv, O. Eromenko. "Increasing the efficiency of information transmission in communication channels," Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), 19.3 (2020): 1306-1315. doi:10.11591/ijeecs.v19.i3.pp1306-1315.
[27] P.S. Macheso, F.G.D. Thulu, Roles of Optical Fiber Sensors in the Internet of Things: Applications and Challenges, in: Ranganathan, G., EL Allioui, Y., Piramuthu, S. (Eds.), Soft Computing for Security Applications. Advances in Intelligent Systems and Computing, volume 1449, Springer, Singapore, 2023, pp. 923–933, doi:10.1007/978-981-99-3608-3_64.
[28] E. Manziuk, O. Barmak, I. Krak, O. Mazurets, O. Pylypiak, Method of features analysis on transition data, in: Proceedings of the 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT, IEEE Press, Kyiv, Ukraine, 2021, pp. 272-277, doi:10.1109/ATIT54053.2021.9678787.
[29] M. Kushnir, H. Kosovan, P. Kroialo, "Method of encrypting images based on two multidimensional chaotic systems using fuzzy logic," Radioelectronic and Computer Systems, 4 (2022): 117-128, doi:10.32620/reks.2022.4.09.
[30] J. Boiko, I. Pyatin, O. Eromenko, Analysis of Signal Synchronization Conditions in 5G Mobile Information Technologies, in: Proceedings of the 2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET, IEEE Press, Lviv-Slavske, Ukraine, 2022, pp. 01-06, doi: 10.1109/tcset55632.2022.9766899.
[31] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang, D. Chen, "Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of Security and Reputation Approach," IEEE Access, 7(2019): 9368-9383, doi: 10.1109/ACCESS.2018.2890432.
[32] O. Jukić, I. Heđi, E. Ciriković, "IoT cloud-based services in network management solutions," in: Proceedings of the 2020 43rd International Convention on Information, Communication and Electronic Technology, MIPRO, IEEE Press, Opatija, Croatia, 2020, pp. 419-424, doi: 10.23919/MIPRO48935.2020.9245117.
[33] I. Pyatin, J. Boiko, O. Eromenko, "Algorithmization and Hardware Implementation of Polar Coding for 5G Telecommunications," Transport and Telecommunication Journal, 25.3 (2024): 300-310, doi: 10.2478/ttj-2024-0022.