Analysis and protection of IoT systems: Edge computing and decentralized decision-making

Nadiia M. Lobanchykova[1], *Ihor A.* Pilkevych[2] and *Oleksandr* Korchenko[3]

[1]*Zhytomyr Polytechnic State University, 103 Chudnivsyka Str., Zhytomyr, 10005, Ukraine*
[2]*S.P. Korolev Zhytomyr Military Institute, 22 Mira Ave., Zhytomyr, 10004, Ukraine*
[3]*University of Bielsko-Biala, Willowa 2, 43-300 Bielsko-Biała, Poland*

Abstract. This article presents a detailed analysis of the Internet of Things (IoT) systems and the methods used to protect them. The article highlights the potential of edge computing to minimize traffic transmission and the decentralization of decision-making systems to enhance security. The analysis examines attacks on IoT system components and provides protection recommendations. Furthermore, the article explores the prospects of information protection in IoT systems.

Keywords: Internet of Things, IoT systems, edge computing, decentralized decision-making, information protection, traffic transmission, security, attack analysis, protection recommendations

1. Introduction

In the last few years, the Internet of Things (IoT) systems has been widely developed and implemented. The Internet of Things market research notes a steady and rapid increase in the number of such devices every year. If analysts currently estimate the number of active IoT devices at 21 billion, in a few years their number will exceed 50 billion [8, 10]. Due to the development and widespread introduction of IoT technologies, information security experts are concerned about their level of protection [1, 2, 9, 12, 14]. According to them, the huge number of poorly protected Internet devices gives new opportunities to cybercriminals. Yes, there are already known cases of breakage of several IoT systems. This task is especially relevant when using these tools at critical infrastructure.

New technologies and new tools are creating new types of cyber threats. Many companies today have introduced their protection models, which are constantly trying to standardize, correlate and implement.

The development of information technology makes its adjustments in the field of information security. Therefore, the advent and edge of computing technologies allow solving several cybersecurity problems. The main trend of edge computing is remote monitoring and data processing directly on IoT devices. The main advantage of this approach is the minimization of processing time and decision-making due to the absence of the need to transfer all data to a data center (data center) or cloud. The combination of IoT and edge computing is a promising area and can be used in industry, hospitals, climate control systems, and “smart” buildings, in the management of the infrastructure of the city or region, in trade and logistics networks [6]. Of particular interest is the use of edge computing for network security monitoring and access control systems. This technology is quite effective in preventing certain types of attacks and the spread of malicious software. Also, performing calculations immediately after receiving a signal allows you to decide whether to generate an alarm, move the “object” to quarantine, isolate, if necessary, several IoT devices to prevent network compromise or system failure. The widespread

introduction of IoT devices creates large amounts of information that are increasingly difficult to transfer to a data center or cloud, process and store them, so the use of edge computing is a necessity for many areas of the digital society. The study of traffic minimization technologies, data storage, resources, and security in IoT using edge computing is a crucial task today for the development of digital society and the entry of humanity into the fourth industrial revolution (Industry 4.0) [13].

2. Theoretical background

The analysis of works [5, 8, 10] confirms the relevance of research in the field of IoT, which is associated with the benefits of these devices and technologies, as well as the transition of mankind to the use of Industry 4.0. In [1, 8, 10], the authors note the incredibly rapid pace of IoT implementation in various areas of the digital society. Immerman [8] testifies that at the beginning of the implementation of IoT, sensors sent data to the cloud, where they were processed, analyzed, and stored, and making management decisions. As the number of devices increased exponentially, the load on both the data channels and the storage cloud (trillions of gigabytes) increased, so the use of edge computing became a necessity, not a whim. The author notes that the use of edge computing and cloud technologies together is possible, and in some cases necessary, especially in industry. Edge computing is the most important component of IoT, which helps reduce latency and increase the reliability of deployed systems [8]. In [10] the models of IoT architecture are presented, the need for IoT protection is determined, the results of research on the construction of information protection systems for IoT devices, including shared and centralized, conducted simulation load depending on the number of devices.

Security issues are quite relevant and aimed at the comprehensive protection of information. Thus, Blyler [1] focuses on the complexity of IoT protection and presents eight key security technologies: network security, authentication, encryption, security attack, security analytics, and threat forecasting, interface protection, delivery mechanisms.

Prospects for implementation and threats facing IoT systems are presented in [5, 9, 11, 12, 14, 15]. The analysis of these works confirm the relevance of security issues, areas of protection, and the main conceptual approaches to security. Loud cyberattacks have occurred more than once and the number of hacker attacks is growing [2–4, 7]. The urgency of the problem is underscored by incidents, the loss of capital from which is measured in billions of dollars.

In total, HP experts have identified about 25 different vulnerabilities in each of the studied

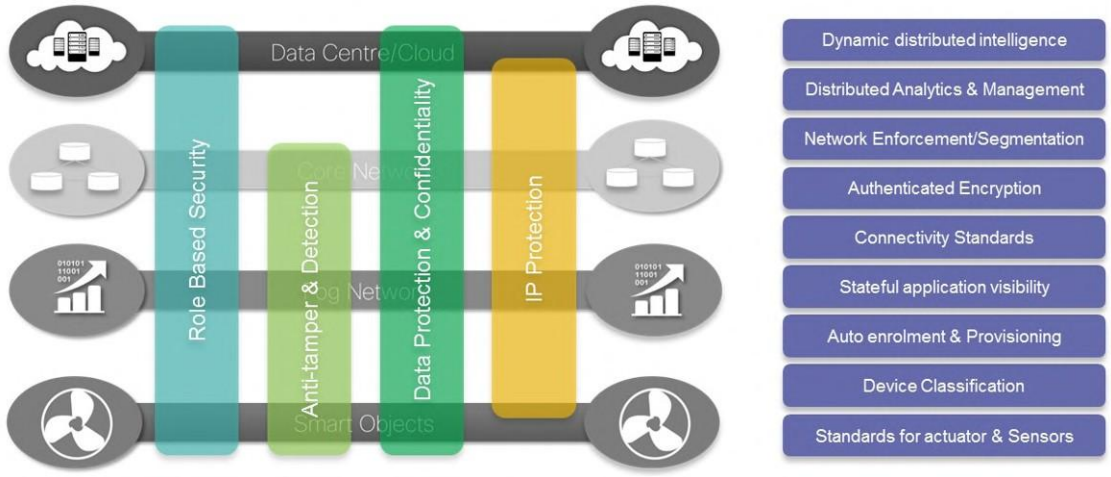

Figure 1: IoT security environment.

devices and their mobile and cloud components [7]. The conclusion of HP experts is disappointing: a secure IoT system does not exist today. The particular danger to the Internet of Things is hidden in the context of the spread of targeted attacks. It is only necessary for intruders to show interest in anyone, and our helpers from the world of IoT turn into traitors, openly open access to the world of their owners.

Because the issue is extremely acute, companies that develop equipment, communications, network devices, software, and cybersecurity companies are looking for means to protect IoT devices [3]. One of the leading companies in the development of security in IoT is Cisco Systems, which played a leading role in the development of the IoT model at the World IoT Forum, developed the IoT security framework, which became a useful addition to the reference model [7]. Figure 1 shows the security environment associated with the logical structure of the IoT.

The Cisco IoT model is a simplified version of the World IoT Forum model. Figure 1 shows specific functional areas of security on top of the four levels of the IoT model. The Cisco document also proposes an IoT security concept that defines the components of the IoT security feature, covering all levels: authentication, authorization, network policy and security analytics.

Humanity's entry into the Industry 4.0 [5] creates new challenges and opportunities for Ukraine. The new cyber threats are associated with the widespread use of Industry 4.0 technology, which can have catastrophic consequences when attacking regime facilities. This task is especially relevant in the organization of temporary protection of the perimeter of the regime object when there are limited resources, adverse weather conditions, and unforeseen terrain.

Portable devices account for the largest number of attacks, and the use of wireless communication technologies between system elements creates the preconditions for a cyber-attack on the system. According to [5, 9, 11, 12, 14, 15], unauthorized access is most often carried out by hackers through entry points (access) to the corporate network or used to launch a DDoS attack. Given the large number of sensors connected to the system, the use of wireless networks, cloud services, etc. does not provide a reliable perimeter of cybersecurity of the object. Another area is the theft of confidential user data (companies). The powerful potential of cyber

threats has the technology of machine learning and the use of artificial intelligence systems through dual-purpose (the algorithms used can both counteract cyber-attacks and create them). New technologies create new cyber threats, which can be resisted only with the use of new information technologies.

Global statistics compiled by Cisco in 2017 [5] show:

- vulnerabilities ("holes") in modern security systems allow up to 65% of cyber incidents,
- human factor – critical (if we scale it to the number and complexity of cyber threats) reduction of the level of literacy of users – up to 48% of incidents,
- 55% of organizations are unable to establish the cause of the incident,
- the average time to establish such a cause in the modern informational security and cybersecurity industry is 100 days.

Leading companies and specialists implement multi-level comprehensive protection systems based on the use of the latest technical tools, qualified personnel, control procedures, administrative regulations with strict compliance with them. In such systems, the emphasis is on setting up early warning systems that monitor the operation of IT equipment in real-time, notify administrators in the event of any abnormal activity, allow timely detection of attacks, as well as analyze potential threats. The criteria for the stability of such a defense system are the ability to respond to attacks in a timely and adequate manner and to restore the operation of the object with minimal losses [5].

3. Results

Our research system is a wireless IoT system, the hardware of which can be divided into the following elements [1, 9, 11, 14, 15]:

1. communication subsystem (wireless communication in the sensor network, includes a radio receiver),
2. computing subsystem (data processing, node functionality),
3. sensor subsystem (network connection with the "outside world"),
4. power subsystem.

Tasks facing the system to the hardware:

- low electricity consumption,
- the ability to work with a large number of nodes at relatively short distances,
- relatively low cost,
- work autonomously and without maintenance,
- have a camouflage effect,
- be resistant to the environment.

We choose the 7-level architecture of IoT systems, proposed by Cisco (figure 2).

Given the fact that sensor networks are vulnerable to many attacks, the issue of cybersecurity is especially relevant in the implementation of IoT systems to protect the perimeter of the regime object.

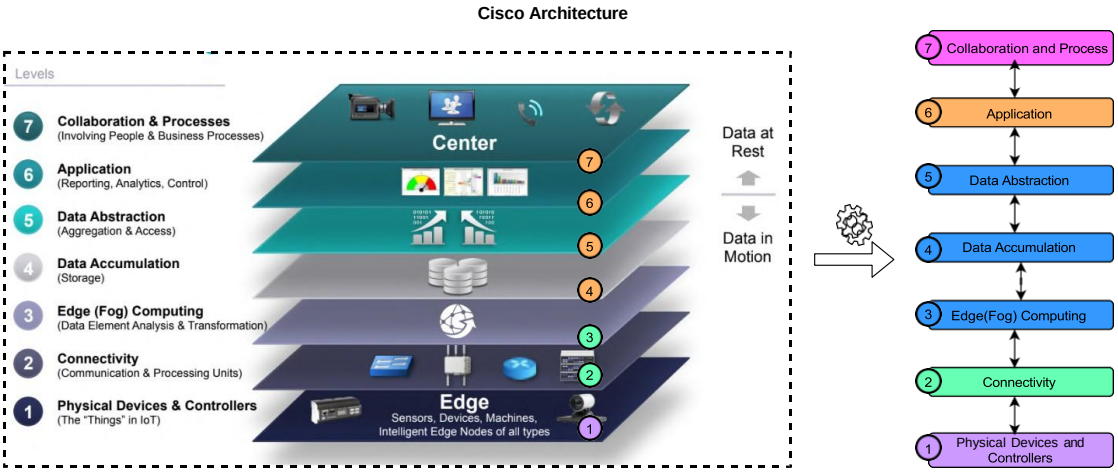

Figure 2: Cisco IoT Architecture.

We assume that it is necessary to carry out temporary protection of the perimeter during the transportation of cargo/person/reconnaissance operation. Created using Cisco Packet Tracer simulation of one protection zone of the IoT perimeter security system is presented in figure 3. This scheme contains a set of devices used to create a zone of the temporary perimeter security system.

Also performed modeling of a typical fire alarm system of a separate room on the example of a garage (figure 4). The set of devices is typical.

The constructed computer models, figures 3 and 4 allow us to research to identify potential cyber threats and develop recommendations for the protection of IoT components. The results of modeling and countering cyberattacks will be presented in future studies.

Modeling of systems allowed to determine that the main areas that need attention from cybersecurity are:

- communication security,
- protection of the devices themselves,
- control over the operation of devices,
- control of network interaction.

As a result of research and analysis of the most likely attacks on simulated systems, the following classification of attacks is proposed (figure 5):

- Denial-of-Service (DoS) (□):
  - physical level (□):
    - obstacle attack ($□_1$)
    - attack of interference in the IoT system ($□_2$)
  - channel level (□):
    - collision attack ($□_1$)

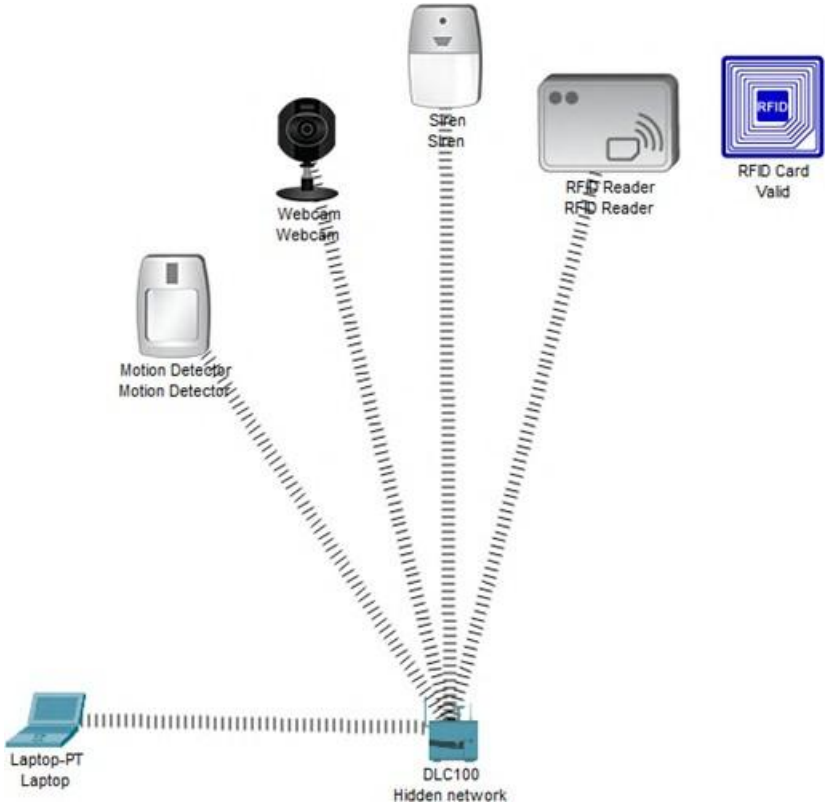

Figure 3: Cluster protection zone.

- attacks on routing protocols (□):
  - "Black Hole" attack (□$_1$)
  - selective forwarding attack (□$_2$)
  - "Rapid onslaught" attack (□$_3$)
  - "Funnel" attack (□$_4$)
  - Sybil attack (□$_5$)
  - "wormholes" attack (□$_6$)
  - flood attack (□$_7$)
- attacks at the transport level (□):
  - avalanche attack (□$_1$)
  - desynchronization attack (□$_2$)
- attacks on data aggregation (□);
- privacy attacks (□).

Attacks can be represented in the form of open classification groups.

□ = □ ∪ □ – a set of attacks that lead to denials of service, involves combining sets of attacks at the physical and channel level.

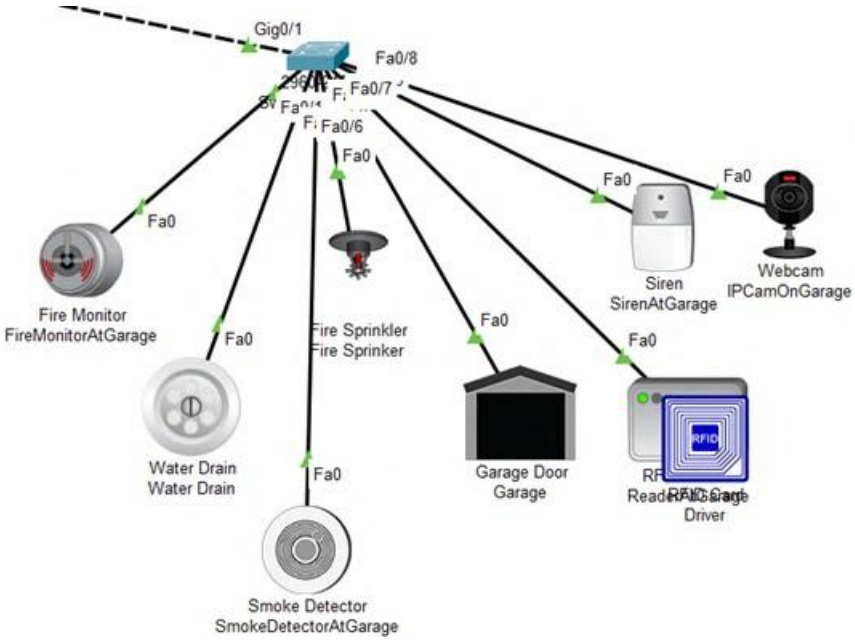

Figure 4: Scheme of fire alarm system of a separate room on the example of a garage.

Many attacks that lead to denials of service at the physical level:

$$\square = \sum_{\square=1}^{\square} \square_{\square}$$

The set of attacks that lead to denial of service link-level:

$$\square = \sum_{\square=1}^{\square} \square_{\square}$$

The set of attacks on routing protocols:

$$\square = \sum_{\square=1}^{\square} \square_{\square}$$

The open classification grouping of transport layer attacks is presented in the form of a set:

$$\square = \sum_{\square=1}^{\square} \square_{\square}$$

The set of attacks on data aggregation is represented as follows:

$$\square = \sum_{\square=1}^{\square} \square_{\square}$$

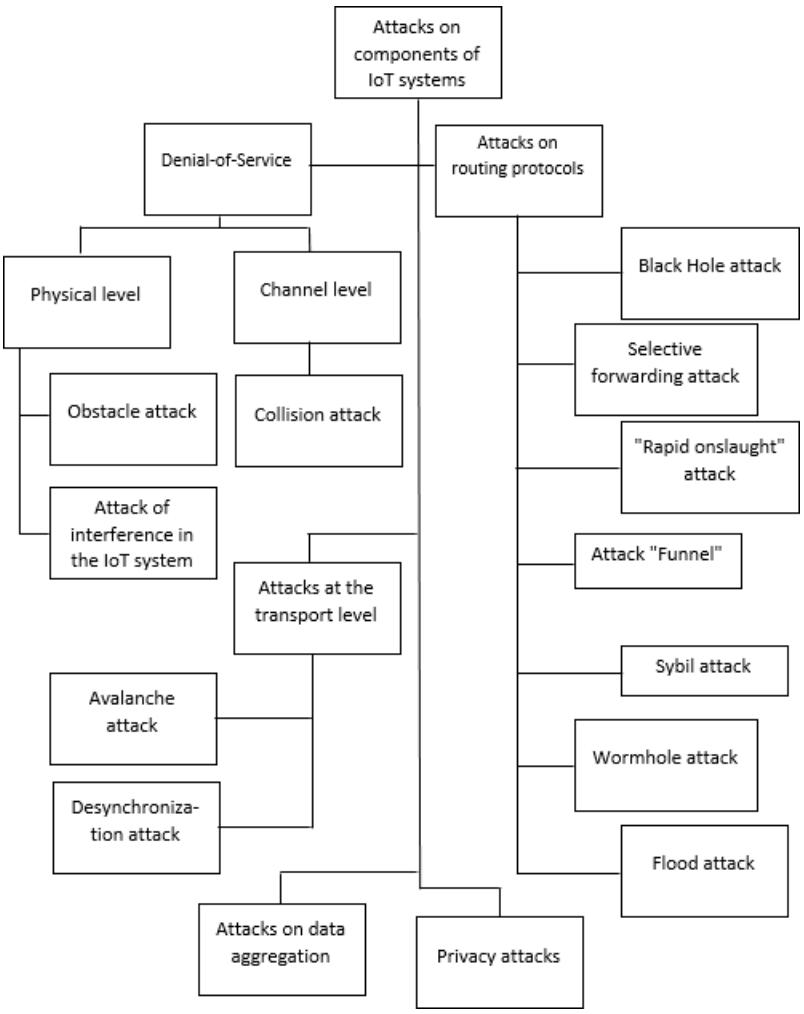

Figure 5: Attacks on IoT system components.

The set of attacks on privacy:

$$\square = \square_{\square}$$
$$\square=1$$

In general, attacks can be represented as a union of all classification groups:

$$\square = \square \ \square \ \square \ \square \ \square$$

Let's analyze each attack that is part of the classification group.

DoS attack on the physical level. A DoS attack is characterized by an attempt by an enemy to stop a network or destroy a network security service. In an IoT system, a DoS attack can occur at different levels of the protocol stack, can affect several levels simultaneously, and use the

interaction between them. DoS attack at the physical level can be carried out by interfering with the radio frequencies on which the system operates. In such an attack, one attacking node may disconnect all or part of the network (for example, blocking data transmission).

An attack on the IoT system's detection of a sensor (in our case, a sensor/camera around the perimeter of a security object) and an attempt to physically access it is critical to our system. In this case, an attacker can destroy the device, try to replace the data, access sensitive information (including cryptographic keys), use the device to log on to the network.

DoS channel level attack. DoS collision attack at the channel level is usually aimed at depleting the resources of nodes. This attack affects the packet transmission process, causing exponential delay and packet retransmission procedures in some MAC protocols. Thus, when a large number of bits are damaged in a packet, the node will try to use error correction codes to recover the damaged bits, thus wasting limited energy resources. Another example of such an attack is a "collision" at the end of the frame, which leads to the retransmission of the entire packet. Another embodiment of the attacks inherent in the IEEE 802.11 protocols may be the generation of an RTS message to a base station or neighboring node, which will lead to the processing of this message and generate a CTS message, followed by waiting for signal reception, and all other nodes stop transmitting data to receiving node for the time specified in the RTS message. Handshake methods can also be implemented.

Let us analyze attacks on routing protocols. The known Black Hole attack aims to use a routing protocol to redirect packets from or to the target node through a specific node. This attack can be used to drop packets or a "middle man" (a method of compromising a communication channel in which an attacker, by joining a channel between counterparties, interferes with the transmission protocol by deleting or modifying information). Another type of attack is a selective forwarding attack, which is similar to a Black Hole attack, but in this attack will be rejected packets that meet certain criteria, not all.

When implementing the "Rapid Pressure" attack, the procedure of opening the route at the request of routing protocols is used. The malicious node generates and transmits a route request to its neighbors, and as a result, the node is more likely to be part of the selected route between the source and destination.

The "Funnel" attack is characterized by the fact that the attacker tries to either compromise the node, or place its own in the path of as many networks flows as possible, and the latter then begins to act on the type of funnel – collecting all the traffic of the sensor network. In protocols that use broadcast, the attacker, listening to the channel, informs neighbors that he "knows" the shortest route to the base station. Once it has managed to stand between the transmitting sensor node and the base station, it can perform any action with the data packets coming to it. Sybil attack is characterized by the fact that the attacker tries to compromise the existing node, or connect your own with several pseudo-identifiers and thus pretending to be several nodes at once. Thus, neighboring nodes may perceive it as "their own". Such attacks are used to disrupt the mechanism of distributed storage, routing mechanisms, data aggregation mechanisms, voting mechanisms in the network.

A wormhole attack poses a serious threat to the security of sensor networks because it does not require compromising the sensor node. For example, an attacker listens to a channel, receives a broadcast to request a route from the base station, and forwards it to the nearest neighbor. The node that received this message will consider it the parent, that is, the one closest

to it, although this is not the case. The attack is based on creating a special path between two or more network nodes to transmit intercepted packets, and the nodes will think that they transmit packets by the shortest path.

One type of attack is a flood attack (HELLO flood attack). The peculiarity of this attack is the attempt to transmit to the network many optional messages that will deprive the network of various resources (computing power, channel capacity, energy resources). Having a high-frequency radio transmitter with sufficient computing power, the attacker sends Hello packets of many nodes of the sensor network. Upon receipt of this message, the nodes perceive the compromised node as a neighbor and include the received address of the sender in the mailing list. In this way, the attacker gains access to data sent from the nodes.

Transport layer functions include the delivery of packets (TCP) and datagrams (UDP) from sender to recipient. Attacks at the transport level are aimed at analyzing the regularity of traffic and sending parallel duplicates of messages in other ways used at this level. Given the fact that most transport protocols support sensitive information and are therefore vulnerable to memory depletion, an avalanche attack attacker makes new connection requests each time increasing the amount of confidential information in the attacking node, gradually leading to the node becomes faulty (failure of the node from further connections) due to resource depletion) and uses this shortcoming.

Another typical attack of this level is the desynchronization attack, because of which an attacker tries to break the connection between two working nodes in the network, repeatedly forging messages to them. In particular, transport layer protocols can use sequence numbers to track successfully received packets, identify packet loss, and detect copies. Attacker-generated packets can use these sequence numbers to reassure the node that packets have been lost and to provoke retransmission, which can have the effect of depleting the resource and filling the data channel when valid information does not arrive at the database or arrives with a delay.

Attacks on data aggregation are aimed at changing the behavior of the network. Data aggregation and merging procedures are used in networks where the location of typical sensors is close to each other. Such procedures are used to combine multiple data to eliminate redundant information. To save resources, this is positive, but it is dangerous from the point of view of cybersecurity. Thus, the calculation of simple mathematical functions (minimum, maximum, average, sum) used in aggregation in the presence of a single malicious node or the replacement of real data from sensors can change the behavior of the network in part or completely.

Privacy attacks are aimed at capturing information collected by sensors and can be implemented by listening to the network, analyzing traffic, and/or capturing the node. This is especially true for those networks that do not use data encryption.

3.1. Recommendations for counteracting attacks on components of the IoT system

Resist DoS attacks at the physical level. IEEE 802.11 (Broadband) standards use frequency hopping. In this case, the interference transmitter must "know" the sequence of hopping or create interference with a larger frequency band. It is proposed to use spectrum expansion technology to protect against such attacks. The transmission of such a signal will be similar to noise, which will reduce the risk of intentional interference with the information signal.

Besides, when the signal disappears from any part of the network or node, network element, DSS should generate an alarm on the unit. Nodes that have detected an interference attack must send a short message to their "neighbors" and the base station about the attack on the network. In this case, if the message "does not reach" the base station from the attacked node, it is likely to receive an alarm message from the node that was not attacked.

To counteract IoT intrusion attacks, each sensor used in the system must be equipped with a tamper (a miniature button on the board of the device that is squeezed when opening the case or disconnecting it from the mounting location). When the tamper is triggered, the hub sends push-messages and SMS to all users of the security system (if there are such messages in the devices to be used), as well as the transmission of the message to the base station.

Besides, it is desirable to provide software that when the tamper is triggered during "arming", all data stored on the device was destroyed automatically. To avoid detecting sensors, they should be placed in hidden places, but suitable for their installation, use materials that are resistant to external influences. Sensors and cameras have their range, so when placing such devices should take into account this figure and install them with an overlap to avoid insensitivity. If installed correctly, the sensor will detect the danger and send an alarm to the base station until the attacker approaches it.

The proposed system uses an RFID tag to identify a person. The decision support system provides a situation where the RFID tag and motion sensor is activated, but we do not receive a signal from the camcorder. This situation may indicate that the tag was "removed" or "replaced" and the motion sensor detected movement, but attackers could disable the camera to avoid being identified as violators. This set of parameters will generate an alarm on the unit.

To counter a DoS attack at the channel layer, there is authentication to verify that the node generating the message is authorized on the network in combination with encryption. In our case, we use the WPA2-PSK authentication standard with an AES encryption type. Given the energy limit, the use of asymmetric encryption becomes impossible in such systems. The main disadvantage of using symmetric encryption is the problem of key distribution. When using a symmetric cryptographic scheme, it is necessary to ensure the reliable and secure installation of shared cryptographic keys between two nodes before they can exchange data. Key installation and management techniques should be suitable for use with hundreds and thousands of nodes.

Another way to improve security is to install an RFID tag on all devices on the network and conduct a combined (two-factor) node authentication procedure.

It is proposed to use blockchain technology to protect against interference with the program code and substitution of sensors. This technology is a distributed database that is potentially available to everyone. Thanks to the use of blockchain technology, it is possible to counteract fraud, manage identification, transactions, verify the status of elements of various systems, and ensure data integrity. Combining blockchain and Internet of Things technologies can solve several security issues, namely: tracking sensor data measurements and preventing duplication of any other malicious data; authentication and secure data transmission.

Cryptography is proposed to protect against eavesdropping, injection, and packet modification.

To counter aggregation attacks, it is proposed to use aggregation delay and authentication methods. To prevent routing attacks, we use channel-level encryption and authentication using a global public key. Sybil attacks can be prevented by verifying the identity of the sensor

nodes (using a shared symmetric key from a trusted base station) and limiting the number of neighbors that the node may have. In this way, the compromised node will only be able to contact trusted neighbors. You can counter a funnel attack using a geo-routing protocol, in which traffic "naturally" directed to the physical location of the base station is difficult to redirect to create a funnel.

The proposed system uses static sensors that require one-time authentication in the network. Edge computing in information security systems can be used to counter several considered attacks and is the subject of further research. The use of clusters of security systems, IoT clusters in combination with edge computing creates new approaches to technologies for building secure IoT with decentralized data processing.

The list of attacks is an open classification group that can be supplemented and expanded.

The implementation of IoT clusters in combination with edge computing requires further research.

They need to develop a cluster model and mathematical software for IoT systems in combination with edge computing to minimize information processing and decision-making time.

4. Conclusions

The analysis allowed us to generalize cyber threats to the components of IoT systems. As a result, it is determined that the largest number of attacks occur on network nodes, and the use of wireless communication technologies between the elements of the system creates the preconditions for a cyber-attack on the system.

It is determined that today multi-stage complex protection systems are being implemented, based on the use of the latest technical means, qualified personnel, control procedures, administrative regulations with their strict observance.

The analysis of attacks allowed determining their list and exploring the features of implementation. As a result of the analysis and generalization, recommendations for counteracting attacks on the components of the IoT system have been developed.

References

[1] Blyler, J., 2020. 8 Critical IoT Security Technologies. Available from: https://www.electronicdesign.com/industrial-automation/article/21805420/8-critical-iot-security-technologies.

[2] Cisco Systems, 2014. The Internet of Things Reference Model. Available from: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf.

[3] dos Santos, M.G., Ameyed, D., Petrillo, F., Jaafar, F. and Cheriet, M., 2020. Internet of Things Architectures: A Comparative Study. Available from: https://arxiv.org/pdf/2004.12936.pdf.

[4] Frahim, J., Pignataro, C., Apcar, J. and Morrow, M., 2015. Securing the Internet of Things: A Proposed Framework. Available from: http://web.archive.org/web/20210323170935/https://tools.cisco.com/security/center/resources/secure_iot_proposed_framework.

[5] Gnatyuk, S.L., 2019. Cybersecurity in the context of the fourth industrial revolution (INDUSTRY 4.0): challenges and opportunities for Ukraine.

Available from: https://niss.gov.ua/doslidzhennya/informaciyni-strategii/kiberbezpeka-v-umovakh-rozgortannya-chetvertoi-promislovoi.

[6] Herts, A., Tsidylo, I., Herts, N., Barna, L. and Mazur, S.I., 2020. PhotosynQ - Cloud platform powered by IoT devices. *E3S Web of Conferences*, 166. Available from: https://doi.org/10.1051/e3sconf/202016605001.

[7] Hewlett Packard, 2020. HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack. Available from: https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676.

[8] Immerman, G., 2020. The Importance Of Edge Computing For The IOT. Available from: https://www.machinemetrics.com/blog/edge-computing-iot.

[9] Jing, Q., Vasilakos, A.V., Wan, J., Lu, J. and Qiu, D., 2014. Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, 20(8), pp.2481–2501. Available from: https://doi.org/10.1007/s11276-014-0761-7.

[10] Khomich, S.V., Fedosiuk, A.V. and Kulikovsky, M.I., 2015. Research of System of IoT Devices Information Security. *Digital technologies*, 18, pp.166–171.

[11] Korchenko, O., Alexander, M., Odarchenko, R., Nadzhi, A. and Petrenko, O., 2016. Analysis of threats and mechanisms for information security in sensor networks. *Information protection*, 1, pp.48–56.

[12] Kuznetsov, D.I. and Ryabchina, L.S., 2019. Information security of the Internet of Things systems. *Bulletin of Kryvyi Rih National University*, 49, pp.80–83.

[13] Shokaliuk, S.V., Bohunenko, Y.Y., Lovianova, I.V. and Shyshkina, M.P., 2020. Technologies of distance learning for programming basics on the principles of integrated development of key competences. *CEUR Workshop Proceedings*, 2643, pp.548–562.

[14] Turanska, O.S., 2018. *Development of methods of information protection in wireless sensor networks*. Master's thesis. NTU of Ukraine "KPI named after Igor Sikorsky".

[15] Vovk, A.V., 2018. *Methods of information security IoT*. Master's thesis. NTU of Ukraine "KPI named after Igor Sikorsky".