CHAPTER «ENGINEERING SCIENCES»

METHODS OF DETERMINATION OF INTERFERENCES IN WIRELESS COMPUTER NETWORKS

Andriy Dudnik[1]
Olexandr Usachenko[2]

DOI: https://doi.org/10.30525/978-9934-26-190-9-1

Abstract. The *subject* of the latest research is wireless security, which remains a major issue in LANs around the world. While wireless networks offer convenience and flexibility, they also increase network vulnerability. Security threats such as unauthorized access, denial of service attacks, IP and MAC address spoofing, session theft, and eavesdropping can be problems for WLANs. To counter these threats, various standard authentication and encryption methods are combined with other access control mechanisms. These protocols, devices and methods combine to provide a WLAN level of security equal to or even greater than that of a wired LAN. *The methods and technologies* used in WLAN security in relation to this study include: Wired Equivalent Privacy (WEP). An older encryption standard used to eliminate security threats. WEP secures the WLAN by encrypting transmitted information so that only receivers with the correct encryption key can decrypt the information; WPA / WPA2 (Secure WI-FI Access). Improvement of WEP by introducing the Temporal Key Integrity Protocol (TKIP). Even when using RC4 encryption, TKIP uses a temporary encryption key that is regularly updated, making it difficult to steal. In addition, data integrity has been improved by using a more robust hashing mechanism; Wireless Intrusion Prevention Systems / Intrusion Detection Systems. Intrusion Detection and Prevention focuses on the radio frequency

[1] Doctor of Technical Sciences, Associate Professor,
Associate Professor at the Department of Network and Internet Technologies,
Taras Shevchenko National University of Kyiv, Ukraine
[2] Candidate of Sciences in Public Administration,
Associate Professor at the Department of Public Administration,
Interregional Academy of Personnel Management, Ukraine

layers. This includes radio scanning to detect rogue access points or ad hoc networks for network access control. Advanced implementations are able to visually represent the network area along with potential threats and have automatic classification capabilities so that threats can be easily identified. *The purpose of the study* is to identify existing wireless sensor networks (WSNs) penetration methods by analyzing their methods of communication with each other, hardware and software for reliability and resistance to possible threats.

1. Introduction

Today, people are often faced with the task of creating research mechanisms that can read and analyze data from more than one source. Most often to monitor the performance of elements of other systems: complex determination of pressure, temperature, etc. Such systems are also necessary to ensure the safety of various facilities. In addition, it is important to study the peculiarities of natural phenomena, climate, seismic activity, which also use these systems [1, p. 5; 2, p. 3].

As society increasingly begins to use various networks, wireless sensor networks are no exception, the question of regulating and protecting such technologies arises. Networks are taking on more and more important tasks, and so they must be increasingly resistant to threats. As networks grow in number and importance, so does the number of people who want to invade them. Networks have been integrated into all areas of modern life, and taking control of them can cause serious damage to individuals and entire companies [1, p. 1; 2, p. 3].

So, the role of security cannot be overestimated. Security is always relevant in all areas, but now, with the growing popularity of wireless sensor networks, it is their security that comes to the forefront [1, p. 6; 2, p. 4].

Wireless enterprise networks are an important component of today's network architecture. They are needed to support mobile devices and provide connectivity to a variety of devices where wired connections are impractical or costly. However, the lack of physical control of the transmission medium requires additional precautions to control access to wireless networks. Most books and articles describe the problem and risks, but do not offer a completely secure solution with examples. The 802.11 standard for wireless networks does offer encryption and authentication methods such as WPA.

But in an enterprise environment, these controls need to be implemented in a scalable and manageable way. This article provides a practical guide to implementing a secure wireless network in an enterprise environment and provides an example of a proven secure solution.

Attacking wired networks in buildings requires physical access. A wireless network provides great convenience and many benefits, but it also comes with many risks. An attacker can position themselves in a company parking lot or with amplification equipment a few blocks away and infiltrate the network using wireless signals that make inroads in the network. When wardriving, warwalking, or warflying, the attacker is not locked in one physical place, but is constantly on the move. This movement makes the attacker a more difficult target to identify and prevent the attack.

2. The main part of the study

Computer and network security is a combination of all the strategies of mechanisms and services that address the needs of a computer system or network to protect against unauthorized access and unintended use. Most security mechanisms are designed for three basic security models: confidentiality, integrity, and availability. Confidentiality: Security mechanisms must ensure that only the intended recipient can correctly interpret the message and that unauthorized access and use is impossible. For example, Confidentiality secures information such as your Social Security number or credit card number that could be obtained by third parties.

Integrity: Security mechanisms must ensure that messages received cannot be altered as they are passed from sender to recipient, unauthorized users must not be able to destroy or alter the content of classified information [2, p. 1; 3, p. 4].

Availability: Security mechanisms must ensure that the system or network and its applications can perform tasks at all times without interruption. Availability is often measured as a percentage on standby. According to these classifications, the following attacks on WSNs are distinguished (Figure 1) [4, p. 2; 5, p. 1]:

The diagram shows examples of transmission attacks between the sender and the intended recipient. Eavesdropping refers to the receipt of a notification by an unauthorized person. This can be prevented by using confidentiality measures. A man-in-the-middle attack refers to a situation

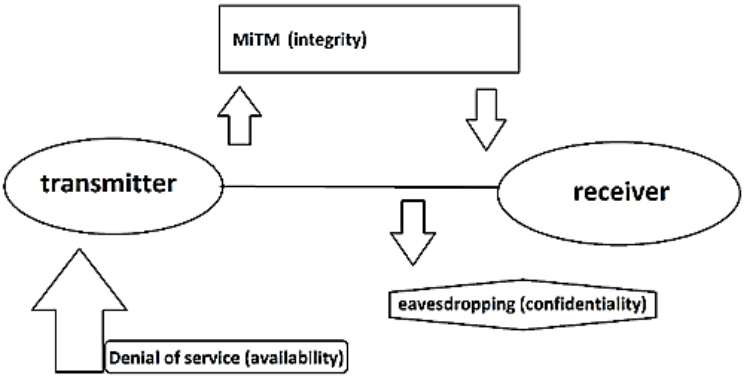

Figure 1. WSN attack

where an unauthorized person influences the position of the system between the sender and the receiver of the sender's notification and as a result – the messages are interrupted and re-transmitted modified to the receiver (in this situation, the receiver believes that the message received came directly from the original sender). This illustrates the need for the integrity of security mechanisms.

Finally, a denial-of-service attack refers to an adversary's attempt to disrupt the transmission or service provided by the sender. For example, the adversary might load the sender with requests and tasks that the sender cannot transmit in a timely manner to the recipient. This type of attack requires security mechanisms to guarantee availability [6, p. 5].

3. Wireless attack sensors networks and principles of protection

Sensor networks are vulnerable to many attacks that attempt to provide a breach of the network and the data generated by the sensor nodes. In particular, when sensor networks serve the purposes of programs such as battlefield assessment and civilian infrastructure control, they require protection against unauthorized access and interference [7, p. 1].

Denial of service (DoS):

A denial-of-service (DoS) attack can be characterized as an adversary's attempt to shut down networks or destroy network support services. In wireless sensor networks, DoS attacks can occur at different levels of the

protocol stack, some may involve multiple layers at once or attempt to exploit interactions between them.

Routing attacks:

Black Hole Attack. In this type of attack, the attacker tries to become the transmission means for one or more routes in the network. In this case, a malicious node can simply reject all traffic that should pass through that node, so that such traffic never reaches its destination. Such an attack is called a selective forwarding attack, where only packages that meet certain criteria are rejected, instead of discarding all packages indiscriminately. Selective forwarding attacks are much harder to detect and affect than black hole attacks because they are much harder to distinguish from package losses due to channel or mobility errors.

Attack Rapid pressure in the sensor network uses routing protocols request routing opening procedures, for example in protocols such as AODV and DSR. In this type of attack, the malicious node immediately transmits incoming route request messages to its neighbors, so it "rushes" these messages without respecting any protocol rules (e.g., setting a timeout or arranging a timeout) of the queue before transmission. As a result, the node is likely to be part of the selected route between source and destination.

The funnel attack is the second version of the "black hole" attack. However, by involving as much traffic as possible, the malicious node tries to stop the path of as much network traffic as possible. Therefore, traffic will be delayed until this drain well allows the attacker to destroy or prevent as much traffic as possible from passing through.

A Sybil attack occurs when an attacker claims to have multiple network credentials. The same principle is followed in location-based routing protocols, according to which the attacker is located in several places at once. If many nodes consider this malicious node to be their neighbor, there is a high probability that they will choose this node to transmit their network traffic.

Another attack on the sensor network routing procedure is the wormhole attack. This attack is carried out by nodes that have more available resources than typical sensor nodes in the network. For example, two attackers. cooperating with each other, may try to fool another part of the network that has an out-of-band channel to each other. For the other part of the network, there is a fast broadband channel, which is desirable for many routing methods.

Attacks at the transport level: The transport layer of the network protocol stack is responsible for managing the connection from start to finish, such as the two well-known transport layer protocols – Transmission Control Protocol (TCP) – for reliable thread-based communication, and User Datagram Protocol (UDP) – for unreliable packet-based communication. The spread of the Avalanche attack takes advantage of the fact that many transport protocols (such as TCP) maintain sensitive information and are therefore vulnerable to memory depletion. For example, an attacker can repeatedly make new connection requests, adding more and more sensitive information to a failed node each time, potentially causing the node to refuse further connections due to resource exhaustion. This, in turn, prevents successful connections to legitimate nodes.

In a desynchronization attack, the adversary tries to break the connection between two working nodes in the network by repeatedly forging messages to those nodes. For example, reliable transport layer protocols can use sequence numbers to track successfully received packets, identify lost packets, and detect copies. Fake packets released by an adversary can use these sequence numbers to make a node assume that the packets have not reached their destination, thereby revealing costly retransmissions of resources.

Attacks on data aggregation: Data aggregation and fusion are often used to combine multiple sensor data and eliminate redundant information. Aggregation can often have a favorable impact on the resource requirements of sensor streams, e.g., by reducing the transmission frequency or packet size. Even simple aggregation functions can easily fall under the influence of an attacker, who can change the behavior of the network. For example, the average function f(x1 ... xn)= (x1 + ⋯ + xn)/n dangerous even in the presence of one harmful node. When replacing one real size x1 with false data x*1, the average will change from y = f (x1, ..., xn) to y* = f (x* 1, x2, ..., xn) = y + (x* 1 x1)/n. An attacker can freely choose the value of x * 1 and therefore can control as a result of the aggregation. Similarly, the sum, minimum, and maximum functions are insecure. The sum f (x1, ..., xn) = x1 + ⋅⋅ ⋅ + xn can be replaced with real data x1 by false data x * 1 if desired. The minimum function f (x1, ..., xn) = min (x1, ..., xn) is also dangerous, although replacing real data with fake values does not always affect the result of the function. That is, replacing x1 with x * 1 increases the

minimum only if x1 is the unique smallest sensory data readable among all xi. However, an attacker can change the calculated minimum by choosing x * 1 very small compared to all the correct data. Because of symmetry, the maximum function is also dangerous, because an intruder can increase the maximum value by grabbing a single indication sensor. In contrast, the effect of fixing a single sensor reading may be relatively small for a read operation if the amount of correct data is large enough. The counter function is similar to the sum function, except that each sensor reading contributes only 0 or 1 to the result of the operation. That is, an attacker with control of the compromise nodes k can change the result of the majority function k, which may be insignificant if k is small compared to the total number of sensor inputs.

Confidentiality attacks: The security threats described earlier are aimed at disrupting the correct operation of the network, a large amount of information is collected by itself Wireless sensor networks are also at risk of potential abuse. That is, an adversary can attempt to obtain sensitive information by accessing information stored on a sensor node or listening network. Wireless networks of broadcast nature simplify the management and transmission of data between nodes, especially if no sensor cryptographic data protection mechanisms are used. Eavesdropping can also be combined with traffic analysis, which can be used by an adversary to identify sensor nodes of interest to the network. For example, an increase in the number of connections between certain nodes may indicate a high level of activity (and hence the presence of data that could be compromised) in that section of the network. In the same way, traffic analysis can be used to identify nodes that may be much more important to operational networks than others, such as base stations and gateways [7, p. 18].

4. Security protocols and mechanisms

Symmetric and public cryptographic keys. Although public key encryption can be used to ensure confidentiality, integrity, and authentication, public key algorithms are very computationally expensive, making them impossible to use in sensor networks with limited budgets. The symmetric cryptography approach may be more resource efficient, making it a better choice in WSN, even if there are RSA and ECC (Elliptic Curve Cryptography) implementations for sensors with limited resources.

The main drawback of symmetric key approaches is the problem of key distribution, i.e., the symmetric key used together must first be known to both nodes being connected before they can exchange data reliably.

Symmetric cryptographic schemes are the best choice for sensor networks when limited resources do not allow the use of more complex public key schemes. However, the main disadvantage of symmetric cryptography is the need for key management, that is, the reliable and secure installation of common cryptographic keys between neighboring nodes in the WSN. For example, the peer intermediary approach to key generation (PIKE) is a method that uses sensor nodes as trusted intermediaries for key distribution. In this approach, each sensor uses a different pairwise key with each O ($\sqrt{n}$) of the other nodes, where n is the number of nodes in the network. In addition, the keys are deployed in such a way that for any pair of nodes A and B there is at least one node C that shares an even key with both A and B. Each sensor in PIKE has an identifier of the form (x, y), where x, y {0,1,2, ..., $\sqrt{n}$-1}. That is, the sensor network is represented as a matrix with rows and columns $\sqrt{n}$, where the position of a node in the matrix is the node identifier. Then each node (x, y) shares an even key with each node in the next two sets:

$$(i, y) \forall i \in \left\{0,1,2,...,\sqrt{n}-1\right\}$$

$$(x, j) \forall j \in \left\{0,1,2,...,\sqrt{n}-1\right\}.$$

For example, node (x, y) shares key K (x, y), (1, y) with node (1, y) and another key K (x, y), (2, y) with node (2, y). In general, the node will support 2 ($\sqrt{n}$-1) keys. Figure 2 shows the virtual ID space for 100 nodes, where each number represents a node ID. Dark shadow fields denote all nodes that share a key with node 91, and light shadow fields denote all nodes that share a key with node 14.

With this approach, any two nodes in the network will be able to find two nodes with IDs that share pairwise keys with both of them. In particular, if node A has ID (xA, yA) and node B has ID (xB, yB), then nodes with ID (xA, yB) and (xB, yA) will share pairwise keys with both A and B.

If a node wants to perform a key setup with another node (e.g., node 91), A can identify potential intermediaries by finding cross shadow fields. For example, node 94 is in the same row as node 91 and in the same column as node 14, so it uses keys with both of them together and

can serve as an intermediary. Then node 14 encrypts a new key that is shared with node 91 using the existing key paired with node 94, and then sends the encrypted key to node 94. Node 94 decrypts the message, encrypts it again using the key shared with node 91, and sends a new message to node 91. Node 91 decrypts the message, receives a new key and confirms receipt of the new key by responding to node 14 [8, p. 76] (Figure 2):

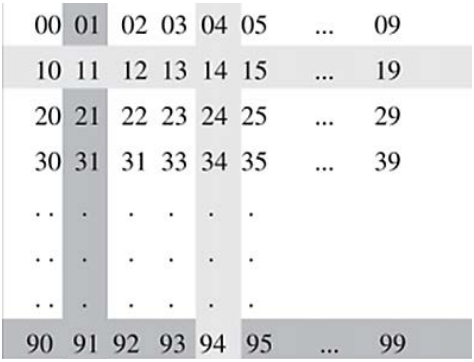

Figure 2. Virtual ID space in PIKE

5. Protection against the most common types of attacks

Protection against DoS attacks: A denial-of-service attack is an attack in which an attacker destroys nodes in a remote sensor network by avalanche-sending a multi-transit section of the end-to-end link either with replicated packets or with packets entered in any order. One-way hash chains are a sequence of numbers where it is trivial to compute y = F (x), but computationally impossible to calculate x = F-1 (y). Each node on the network uses chain hashing to verify the received packet, i.e., the node systematically traverses the chain to determine if the packet is from a trusted source. If the packet cannot be verified, it is discarded.

Protection against aggregation attacks: As discussed earlier, many simple aggregate functions, such as sum, minimum, and maximum, are inherently dangerous. However, several methods can be used to improve the stability of aggregate functions, for example, two such methods are delayed aggregation and delayed authentication.

These methods assume that the base station generates a one-way string for public keys by a one-way function F, where Ki = F (Ki + 1). Each device stores a key K0 before propagation, where K0 = Fn (K) (i.e., F is applied to the secret key Kn times). Next, the transmission of the first stage stations will be encrypted using the key K1 = Fn-1 (K). After receiving all messages transmitted using K1, the base station detects K1. As a consequence, all nodes can calculate F (K1) = F (Fn-1 (K)) and check that this corresponds to K0 = Fn (K). The sensor nodes can then decrypt the messages that were previously transmitted by the encrypted K0. Thus, consecutive keys can be detected until Kn = K (if more keys are needed, the base station can start a new sequence). Suppose that the four sensor nodes A-D send messages to the base station in a network structured as a tree, as shown in Figure 2. Each node message contains sender ID, sensor data and the MAC is calculated from the data using a temporary key. The parent node of a sensor node still cannot verify the MAC until the key from the child node is transferred to the parent node. The parent node (i.e., node E in Figure 2) stores this message and retransmits it to its father after a certain wait time. Message E to its father node G contains the messages received from its children's nodes (e.g., nodes A and B) and the MAC calculated from the dataset A and B, using the key E. This process continues, that is, each intermediate node combines that data from its children and adds its own MAC to the population of all data, using its own key. The base station soon receives the messages from its children and can calculate the final value.

The base station shares a temporary key with each sensor node, so it can verify if the received message was sent from H by calculating the MAC aggregation using KHi and comparing it to the MAC in the message. Although it checks that H sent the last message, it does not check if the message received from other nodes is displayed correctly.

To verify data, the base station shows the temporary keys of the network nodes, sending each key (along with the MAC) to all sensor nodes using their own current Ki key. After sending all node keys, the base station sends its own current Ki key so that nodes can verify the MAC values transmitted and move on to the next key in the chain for future messages.

Thus, the process described delays both aggregation and authentication, e.g., aggregation does not occur on the first jump, which would be possible to do, but occurs on the second jump. While this may increase resource

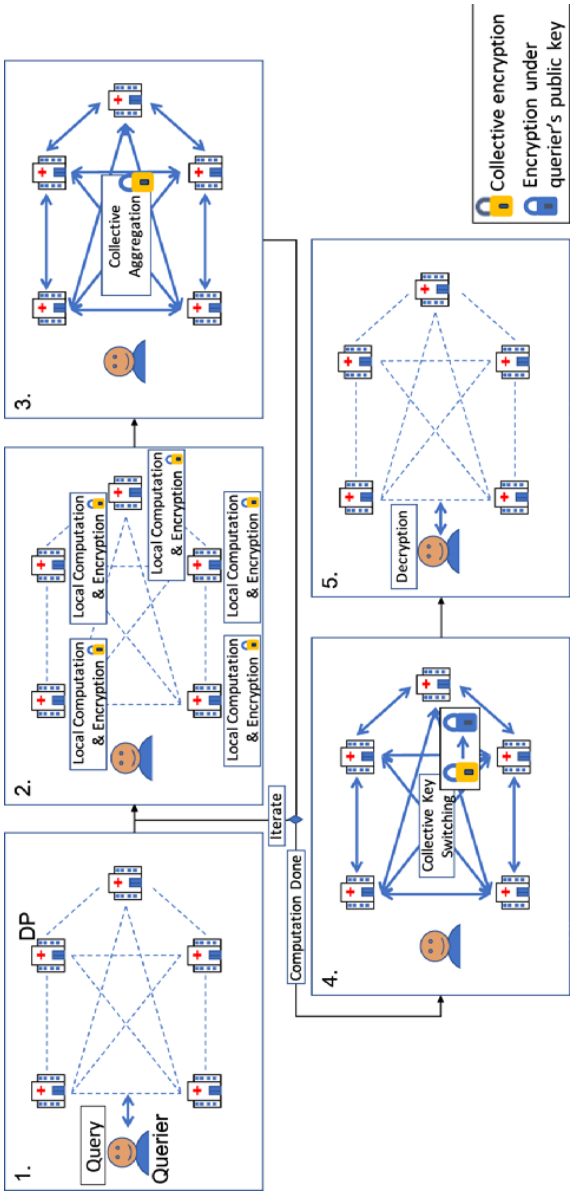

Figure 3. An example of safe aggregation

costs, it can also provide integrity where there are consistent nodes will not be compromised [9, p. 6].

Permanent memory is a 64-kilobyte area of memory that is read-only available to all multiprocessors. The cache is 8 kilobytes per multiprocessor. Quite slow – a delay of several hundred cycles if there is no necessary data in the cache.

The texture memory is a block readable by all multiprocessors. The data is sampled using the texture blocks of the video chip, so linear data interpolation capabilities are provided at no extra cost. Caches 8 kilobytes per multiprocessor. Slow as a global – hundreds of latency cycles if there is no data in the cache.

Naturally, global, local, texture and permanent memory are physically the same memory, known as the local video card memory. Their differences are in various caching algorithms and access models. The CPU can only update and query external memory: global, constant and texture memory [10, p. 5].

A wireless sensor network is a distributed network that is resistant to individual element failures. The total number of elements can range from hundreds to tens of thousands of sensor nodes. Sensor nodes exchange information not only with each other but also with the base station, which allows them to provide the collected data for remote processing, analysis and storage. The function of retransmitting messages between possible different elements of the network, which allows to increase the coverage area up to several kilometers. Thus, a generalized block diagram of a wireless sensor network can be represented as two groups of sensors monitoring two different areas of space and connected to the Internet using base stations [11, p. 2].

Although wireless sensor networks share many problems with other distributed systems, they have some key differences from other types of wireless information networks, such as wireless LANs and mobile episodic networks. Here are the key features of WSNs:

– large-scale network;

– the number of nodes in the network can reach tens of thousands;

– complex topology;

– the capacity of the autonomous power supply, the processing power and memory of the microprocessor, the bandwidth of communication channels, etc. are very limited;

– types of traffic;

– depending on the current application task support for traffic types “many-to-one”, “one-to-many” and “many-to-many”;

– placement of nodes;

– the location of nodes in space can be random or deterministic, their distribution over the coverage area of the network can be both uniform and uneven;

– self-organization and fault-tolerance;

– scalability is the amount of traffic of the service network and the required memory size of the node is almost independent of the total size of the network;

– nodes may have different energy resources, memory, etc., and wireless channels differ in data transmission speed, reliability, communication distance, etc. [12, p. 2].

Because of its obvious advantages, wireless sensor networks are a popular technology. This contributes to the rapid development of WSNs. But the main challenges in the development of wireless sensor systems remain the creation of smaller, cheaper and more efficient devices. But such requirements pose serious limitations to the versatility of WSNs. Because sensor nodes have low power consumption, they have very low processing power, which can be compared to computer systems of the last decade. The small sensor size and low power consumption also prohibit the integration of many desirable features and components, such as GPS receivers.

Many wireless sensor networks are used to collect sensitive information. However, remote and autonomous sensor operation increases the risk of malicious network attacks. In addition, it is the wireless data transmission that makes it easier to intercept information when transmitting sensor data. For example, one of the biggest threats to network operation is attacks aimed at disrupting the sensor network. This can be achieved through a variety of attacks, primarily with signal attenuation, which degrades the quality of communication between nodes. The consequences can be very serious and depend on the scale of sensor networks. There are many security solutions for distributed systems that prevent attacks or limit their impact, but most require significant computing resources. These requirements usually cannot be met due to the limited resources of sensor nodes. As a result, sensor networks require new solutions to create node authentication and information encryption [13, p. 4].

In small sensor networks, where sensors are located close to each other, a direct connection can be established between all sensor nodes and the base station. All sensor nodes can communicate with the receiver without relaying messages through other nodes. This direct communication model is the simplest implementation, where all data makes one jump to reach the target.

Therefore, for routing tasks in wireless sensor networks, we can distinguish two variants, which will differ in terms of route search criteria:

– the problem of finding optimal routes;

– the optimal route is considered a way to deliver information packets from the sender node to the destination node, which requires a minimum total resource costs nodes in this path;

– routing tasks with maximum network lifetime.

Depending on their purpose, widespread wireless sensor networks have their own limitations and characteristics to consider when designing a routing protocol. For example, most WSNs will be limited in power resources, performance, and storage capacity. Sensor networks can vary greatly in the scale and area of the geographic areas they cover. Therefore, routing parameters are used, which *b* describe the various purposes of routing protocols, taking into account the use of these resources. consider the most important parameters and criteria in developing a routing method.

The most common metric used in routing protocols is the minimum hop (or shortest hop), that is, the routing protocol tries to find the path from sender to receiver that requires the least number of intermediate nodes. In this simple algorithm, each link has a cost, and the routing protocol chooses a path that minimizes the total cost for distributing data from source to destination. The basic idea behind this metric is that using the shortest path will reduce transmission time and resource consumption because as few transmitting nodes as possible will be involved. However, since this approach does not take into account the actual resource availability at each node, the resulting route is likely to be suboptimal in terms of energy delay and congestion avoidance.

Undoubtedly, a key aspect of routing in WSNs is energy efficiency. As a rule, among the elements of a node, the receiver consumes the most energy, so the main way to reduce the average power consumption of a node is to minimize activity in the radio channel (transmitting and receiving

data, listening to the channel). Given that each node is not only a source or destination, but also, if necessary, an intermediate retransmitter of packets, optimizing the volume and direction of traffic flow is an important task of the routing layer.

In WSN-related work, the concept of battery life is often not distinct from the concept of energy efficiency. It is believed that greater energy efficiency provides longer battery life.

It is assumed that the operating conditions of WSNs can be harsh, so there will be a probability of nodes failing and links between them being disrupted. Therefore, to ensure high reliability of the system as a whole, the routing method should automatically generate new bypass routes of excluded nodes, spending as few resources as possible to reconfigure the route.

The term quality of service (QoS) refers to certain performance metrics in networks, such as determining packet latency, bandwidth levels, and error rates.

The choice of QoS metric depends on the type of program. Sensor networks that perform target detection and maintenance require low latency for urgent sensor data, while data-intensive networks (e.g., multimedia sensor networks) require high bandwidth.

A network resource is literally any resource that is consumed in the tasks of finding a suitable route, configuring and maintaining data transfer sessions, and maintaining routing tables. The following is a classification of network resources.

There are different ways to classify routing protocols. Most routing protocols clearly fall into one of three classes. Flat routing protocols assume that all nodes have equal functions and roles. Conversely, in hierarchical routing protocols, different nodes have different roles in the routing process, that is, some nodes can send data on behalf of others, while other nodes only generate and distribute data received from their own sensors. The location-based routing protocol relies on the location of information received from nodes to make further routing decisions.

Routing protocols are responsible for determining or opening a route from the sender to the desired recipient. This process can be used to distinguish between different types of routing protocols. For example, reactive protocols can create a route on demand, that is, any time a sender wants to send data to a recipient and does not yet have a route established.

While opening a reactive route causes certain delays in the implementation of data transmission, a proactive routing protocol establishes routes before they are needed. Some protocols exhibit characteristics of reactive and proactive protocols and therefore fall into the category of hybrid routing protocols.

The first category of routing protocols are flat protocols of the way the network is organized. To create a number of specialized routing methods in WSNs, the following feature was taken into account: WSN nodes perform the same set of functions and interact with each other to perform the same task of collecting data from multiple sensors. If, for example, sensor nodes measure any physical environmental parameters, there is a high probability that closely located nodes will register the same values, so it would be impractical to transmit readings from each individual node to the base station. As a result, a new routing concept, data-oriented routing, has been proposed.

SPIN is a family of protocols that provide data-based "negotiated" delivery procedures. It refers to routing methods with peer-to-peer nodes without guaranteed message delivery, carried out taking into account the energy consumption of the nodes. It is well suited for WSNs with dynamic topologies with mobile nodes. The adaptive variant uses a simple flooding technique, which significantly improves routing efficiency compared to the prototype. In this case, to avoid unnecessary messages, a polling is performed between neighboring nodes before data is transmitted. Messages from each node are distributed throughout the network, allowing a fairly simple way to get information from any node on demand with immediate delivery.

Rumor routing is a variation of the previous DD algorithm. It optimizes the routing scheme for those networks in which the number of events is small, but the number of requests is huge. In the RR routing algorithm, each node maintains a list of its neighbors and a table with information about the event. When events occur, information about them is entered into a table and special messages called "agents" are generated, which contain information about the local event. An agent is a durable packet that is sent over the network to distribute information about a given event and other events along its path to remote nodes. When such messages are received, remote nodes populate their event table and pass the agent to neighboring nodes until it runs out of TTL (time-to-live).

Gradient-Based Routing (GBR) is a routing method using gradients. It is another variant of the Directed Diffusion algorithm. This modification has a number of significant differences. In the process of distributing a request from a central node throughout the network, the number of transfers from node to node (hops) is taken into account. Each node calculates a parameter called the "height" of a node, which indicates the minimum possible number of hops in a route chain from that node to the central node. For each of the adjacent directions in a node, a gradient is denoted – the difference between the height of the node and the height of its neighbor. The direction with the highest value is selected for the routing gradient. In cases where the gradients for different directions are equal, the choice is made randomly.

The Optimized Link State Routing (OLSR) protocol is a proactive routing protocol for wireless sensor networks. It refers to proactive routing protocols. That is, the route is set before it is needed. In any case, there is a ready route to the destination node. The principle of the protocol is to reduce the number of broadcast messages in the network by transmitting these messages only through special nodes – Multi-point Relays (MPRs).

The Ad hoc On-Demand Distance Vector (AODV) protocol is a proactive routing protocol for wireless sensor networks with on-demand connection establishment. The route discovery procedure starts after a request from a central node. Routes are stored in the routing table as long as they are in use.

6. Conclusions

This paper analyzed the basic principles and requirements for the use of wireless sensor networks. The problems arising from the use of existing methods of information protection, as well as the peculiarities of WSNs, which must be taken into account when developing methods specifically for such networks, have been considered as the main ones. For wireless sensor networks, there are also considered indicators of reliability, which allow to assess the safety of the network as a whole during its operation. In the course of this work, possible network attacks were also considered. The way they are carried out, their manifestations and possible consequences. The following are examples of attacks. Because wireless sensor networks are deployed remotely and unattended, they are very vulnerable. Therefore, these attacks are carried out at all layers of the OSI model. From the physical impact of university failures to the impact

of the software that was used to run the network. So this issue is important and needs to be addressed at all levels.

This paper considers the development of routing methods in wireless sensor networks. The goal of the work is achieved, and the results correspond to the formulated objectives and satisfy them.

The routing process in wireless sensor networks was considered. Parameter improvement was achieved by selecting the optimal routing method using the available network resources. Classification of routing protocols has been investigated in wireless sensor networks. The algorithm describes in detail the operation of such protocols as SPIN, DD, RR, GBR, OLSR, AODV, LEACH, PEGASIS, GAF, GEAR. All routing protocols considered are widely used in WSN and are basic protocols with the possibility of further optimization and modification.

References:

1. Kvasnikov, V. P., Dudnik, A. S., Pysarchuk, O. O., & Domkiv, T. S. (2020). Using Cuda and Blockchain Technologies to Recover an Encrypted Pdf File Password. *Metrology and Instruments*, 6, 54–60. DOI: https://doi.org/10.33955/2307-2180(6)2019.54-60

2. Rokochinskiy, A., Volk, P., Kuzmych, L., Turcheniuk, V., Volk, L., & Dudnik, A. (2019, December). Mathematical model of meteorological software for systematic flood control in the carpathian region. In 2019 International Conference on Advanced Trends in Information Theory (ATIT) (pp. 143–148). IEEE.

3. Skuratovskyj, R. V., Dudnyk, A. S., & Kvashuk, D. M. Vlastyvosti skruchenoyi kryvoyi edvarsa, podilnist yiyi tochky navpil i yix zastosuvannya v kryptografiyi. *Problemy informatyzaciyi ta upravlinnya,* 4(60), 71–78.

4. Dudnik, A., Kuzmych, L., Trush, O., Domkiv, T., Leshchenko, O., & Vyshnivskyi, V. (2020, October). Smart Home Technology Network Construction Method and Device Interaction organization Concept. In 2020 IEEE 2nd International Conference on System Analysis & Intelligent Computing (SAIC) (pp. 1–6). IEEE.

5. Dudnik, A., Kvasnikov V., Trush, O., Domkiv, T. (2021). Development of Distributed Multi-Segment Wireless Networks for Determining External Situations. In Information Technology and Interactions (pp. 127–137). CEUR Workshop Proceedings, vol. 2845, ISSN 1613-0073.

6. Dudnik, A., Daria, P., Kobylchuk, M., Domkiv, T., Dahno, N., & Leshchenko, O. (2020, November). Intrusion and Fire Detection Method by Wireless Sensor Network. In 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT) (pp. 211–215). IEEE.

7. Domkiv, T., Dudnik, A., Dakhno, N., Kvasnikov, V., Trush, O., & Dorozhynskyi, S. (2020, November). Development of an All-Based Method Using

Blockchain Technologies and Cuda Technologies. In 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT) (pp. 200–205). IEEE.

8. Leshchenko, O., Trush, O., Dahno, N., Dudnik, A., Kazintseva, K., & Kovalenko, O. (2020, November). Methods for Predicting Adjustments to the Rates of Modern "Digital Money". In 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT) (pp. 222–226). IEEE.

9. Pysarchuk, O., Gizun, A., Dudnik, A., Griga, V., Domkiv, T., & Gnatyuk, S. (2019). Bifurcation Prediction Method for the Emergence and Development Dynamics of Information Conflicts in Cybernetic Space. In 1st International Workshop on Cyber Hygiene & Conflict Management in Global Information Networks (pp. 692–709).

10. Ivan Bakhov, Yuliya Rudenko, Andriy Dudnik, Nelia Dehtiarova, Sergii Petrenko (2021). Problems of Teaching Future Teachers of Humanities the Basics of Fuzzy Logic and Ways to Overcome Them. *International Journal of Early Childhood Special Education (INT-JECSE),* 13(2), 844–854. DOI: https://doi.org/10.9756/INT-JECSE/V13I2.211127

11. Kvasnikov, V. P., Dudnik, A. S., Pysarchuk, O. O., & Domkiv, T. S. (2020). Using Cuda and Blockchain Technologies to Recover an Encrypted Pdf File Password. *Metrology and Instruments*, 6, 54–60. DOI: https://doi.org/10.33955/2307-2180(6)2019.54-60

12. Dudnik, A., & Domkiv, T. (2020). CUDA architecture analysis as the driving force of parallel calculation organization. *Publishing House "Baltija Publishing"*. DOI: https://doi.org/10.30525/978-9934-588-38-9-59