Data Transfer Methods and Algorithms in Wireless Sensor Networks for IoT-based Remote Monitoring System of Hybrid Energy Supply Sources

Ilkhomjon Siddikov
Full Professor of the Department of "Use of electrical technologies and electrical equipment"
Tashkent institute of irrigation and agricultural mechanization engineers National research university
Tashkent, Uzbekistan
ikhsiddikov@mail.ru

Halimjon Khujamatov
Dean of the Faculty of "Komputer engineering"
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Tashkent, Uzbekistan
kh.khujamatov@gmail.com

Doston Khasanov
Associate Professor of the Department of "Data Communication Networks and Systems"
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Tashkent, Uzbekistan
dhasanov0992@gmail.com

Ernazar Reypnazarov
PhD student of the Department of "Data Communication Networks and Systems"
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Tashkent, Uzbekistan
reypnazar0vernazar@gmail.com

Abdurasul Iminov
Head of Department of "Information Technologies"
Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan
Tashkent, Uzbekistan
iminovabdurasul1970@gmail.com

2022 International Conference on Information Science and Communications Technologies (ICISCT) | 978-1-6654-7229-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICISCT55600.2022.10146865

***Abstract*— The most important requirement in the provision of telecommunication services is its continuous provision. Continuity of services depends mainly on the uninterrupted power supply of telecommunications equipment. for this reason, today, scientists are conducting research on continuous monitoring of energy supply sources, prediction and early detection of possible failures and outages. In particular, wireless sensor networks are widely used in real-time monitoring of energy supply sources and have become the center of interest. In this article, the data transmission processes and transmission problems of wireless sensor networks used in monitoring systems are studied. Also, several algorithms aimed at improving the effectiveness of wireless sensor networks and improving the efficiency of data transmission are proposed in the article.**

Keywords*— *Wireless sensor network, data block, CSMA/CA, Payload, CAA, ZigBee

I. INTRODUCTION

An important task of monitoring systems is to remotely identify problems that arise in controlled systems and quickly eliminate them. Typically, this system consists of 3 main components: (1) the main control panel of the system, (2) monitoring and automatic detection of inputs from reference points for the monitored object (using current and voltage, temperature, illumination and other similar sensors), and based on (3) activation of output components (management, database formation, monitoring data transmission over the Internet) [1], [2].

A modular design approach to process monitoring provides a flexible and versatile platform to meet the needs of a variety of applications [3], [8]. For example, depending on the sensors to be placed in monitoring systems, the alarm control unit can be reprogrammed or replaced. This allows the use of various sensors with a wireless sensor network node. Similarly, radio communication can be switched depending on the wireless range requirement of specific applications and the need for two-way communication. Here, a functional block diagram of a wireless sensor network node, a remote monitoring system based on IoT of hybrid power supply sources of telecommunication systems is presented in fig. 1 [4], [7].

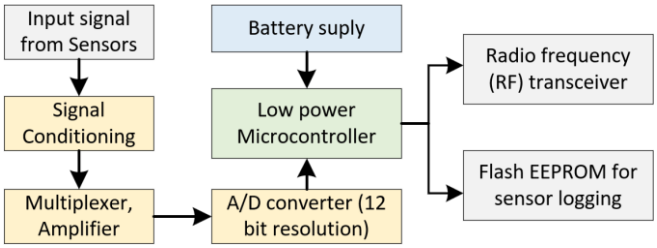

Fig. 1. Functional block diagram of the wireless sensor node

The use of EEPROM memory allows remote nodes to receive data on sensors by command from the base station or by one or more inputs to the node. In addition, the installed software can be updated via the wireless network in this area [3], [6].

In the process of remote monitoring, the microprocessor included a number of functions:

- management of data collection from monitoring system sensors;

- performance of power management functions during monitoring;

- transmission of information received from the sensor to the physical radio layer;

- radio network protocol management.

978-1-6654-7229-6/22/$31.00 ©2022 IEEE

Authorized licensed use limited to: Tashkent University of Information Technologies. Downloaded on November 23,2023 at 04:56:49 UTC from IEEE Xplore. Restrictions apply.

At the same time, in monitoring systems based on wireless sensor networks, the wireless network module is of great importance, the reliability of the monitoring process directly depends on its complete characteristics.

II. Remote Monitoring System Wireless Network Module Characteristics

The main feature of any wireless sensor node in remote monitoring is to minimize the power consumed by the system. Typically, the radio subsystem requires the most power. Therefore, it is useful to send data over the radio network only when necessary. This sensor based data collection model requires a node triggering algorithm to determine when to send data based on a sensed event. In addition, minimizing the power consumed by the sensor itself is one of the important conditions [1], [9], [10]. Therefore, the hardware must be designed so that the program written to the microprocessor can intelligently manage the power of the radio, sensor and sensor signal tuning.

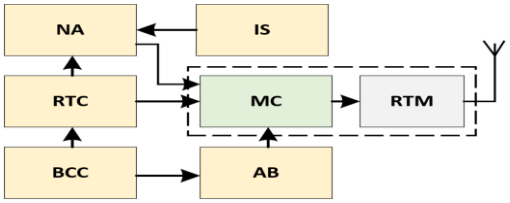

Fig. 2. Structural scheme of the wireless module of the remote monitoring system

The structural scheme of the wireless module of the remote monitoring system is shown in fig. 2 and is the same for each of the types of sensors used, they are:

- IS – intelligent sensors (primary converter);
- NA – normalizing amplifier;
- RTC - real time clock;
- MC – microcontroller;
- RTM – receiving/transmitting module;
- AB - accumulator battery;
- BCC – battery charging controller.

The basic protocols of all wireless sensor network systems (Zigbee, WirelessHART, etc.) recommended by the IEEE 802.15.4 standard for a remote monitoring system and based on it can work in three frequency bands [5], [11], [12]:

- 868 MHz in Europe;
- 915 MHz in the USA;
- 2.4 GHz worldwide.

Three additional modulation schemes are typically used in the 868 MHz and 915 MHz band frequencies: BPSK –Binary Phase-shift keying; OQPSK – Offset quadrature phase-shift keying; PSSS – Parallel Sequence Spread Spectrum. The general characteristics of these types of modulation are given in table 1.

Table 1. BPSK, PSSS, OQPSK modulation characteristics used in the IEEE802.15.4 standard

Modulation type	Physical layer (PHY) protocol standard, MHz	Frequency ranges, MHz	Chip speed rate, kb/s	Bit rate, kbit/s	Symbol rate, ksymbol/s	Sensitivity, Rx, dBm
BPSK	868/915	868-868,6	300	20	20	-92
		902-928	600	40	40	-92
PSSS	868/915	868-868,6	440	250	12,5	-85
		902-928	1600	250	50	-85
OQPSK	868/915	868-868,6	400	100	25	-85
		868-868,6	1000	250	62,5	-85
	2450	2400-2483,5	2000	250	62,5	-85

In the IoT-based remote monitoring system, the radio device supports different data transmission rates according to the modulation scheme: 250 kbit at 2.4 GHz, 20 kbit to 250 kbit at 868 MHz, and 40 kbit to 250 kbit at 915 MHz. The center frequencies fc of these channels are determined as follows [13], [14]:

- fc = 868.3 [MHz], k=0;
- fc = 906+2 [MHz], k=1, 2, …, 10;
- fc = 2405 +5 (k-11) [MHz], k=11, 12, …, 26;

where k is the channel number.

III. Transmission Data Structure of the IEEE 802.15.4 Standard

One of the main features of devices connected to the IEEE 802.15.4 standard in IoT-based remote monitoring is low power consumption due to the fact that the transmitter goes into “sleep” mode when there is no data to transmit. In the development of the standard, emphasis was placed on the speed of configuration and reconfiguration processes. In the process of remote monitoring on the basis of IoT, the time of transition of the receiver to the active state is 10-15 ms, and correspondingly, the connection of new devices to the network is 30 ms. In this case, reconfiguration and device connection times will depend on the frequency of “listening” by network routers [5], [15].

In the IoT-based remote monitoring process, the IEEE 802.15.4 standard CSMA/CA distributed access scheme is used. According to this standard, during each broadcast, the device waits for a random time interval, then determines if the channel is empty (Clear Channel Assignment – CAA). Also, the following waiting time is defined in this standard:

$$t_{wait}=R*a_{ubp} \quad (1)$$

where: R is an integer randomly selected from the range $[0…2^{BE}-1]$. The indicator of the BE level is 3; a_{ubp} is a constant equal to a period of 20 symbols (UBP – Unit Back Off Period).

Authorized licensed use limited to: Tashkent University of Information Technologies. Downloaded on November 23,2023 at 04:56:49 UTC from IEEE Xplore. Restrictions apply.

In all state transitions of the IEEE802.15.4 standard, one symbol period is 16 μs for the 2.4 GHz frequency range. If the channel is empty, the device transmits data, if it is the opposite, a new waiting time is selected. The worst-case latency can be 2.24 ms when R=7. Channel Idle Time The channel listening time to determine t_{CCA} is constant and equal to eight symbol periods or 128 μs [5], [16], [17].

Frame format. The frame format used in the IEEE 802.15.4 standard is shown in fig. 3.

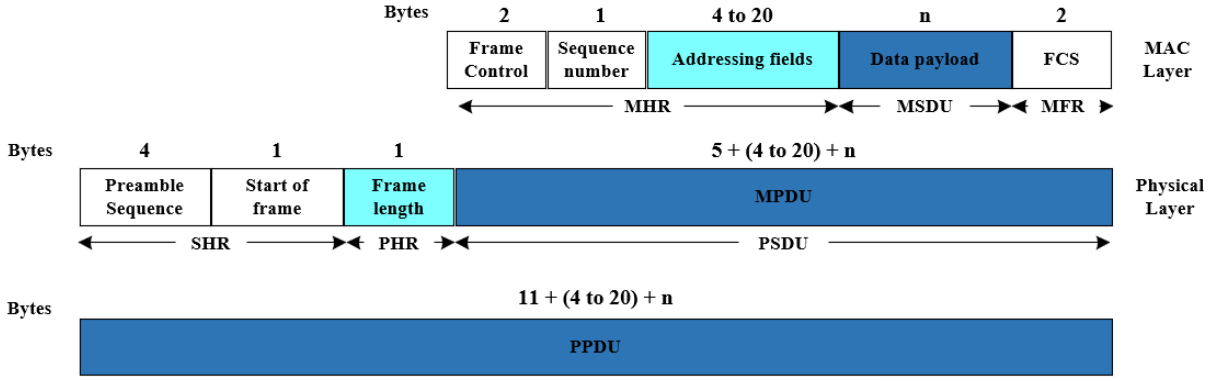

Fig. 3. IEEE 802.15.4 frame format at the physical and channel layers

By default, the maximum frame length at the physical level is $A_{max.phy}$ = 127 bytes. The maximum size of the frame payload depends on the length of the service fields of the frame. Thus, if the minimum size of the address space is used (4 bytes), then the payload size will be 112 bytes. When the address part is at its maximum length, the payload is 96 bytes [3], [18], [19].

Also, according to the standard, the data transfer rate in the frequency range of 2.4 GHz is given, which is f = 250 kbit/s. So, the time of transmission of one packet can be determined by the following formula:

$$t_{data} = \frac{L+O}{f} \quad (2)$$

where: L – packet size in bits; O – size of server bit fields.

The data field in which wireless module capability messages are collected is 96 bytes under the maximum address string length conditions, which corresponds to a maximum of 768 bits of binary data [5], [20].

Acceptance of confirmation. According to the rule, the frame of the confirmation acceptance information consists of 11 bytes (Fig. 4).

An average of 192 μs is always held before the device transmits data, which is the time required for the device to switch from receive mode to transmit mode. In addition, according to the standard, after the confirmation frame, the following minimum retention time is given, this time is designed to process the data received by the device [2], [21]:

- for frames up to 18 bytes long - 18 symbol cycles (288 μs);

- for frames longer than 18 bytes – 40 symbol periods (640 μs).

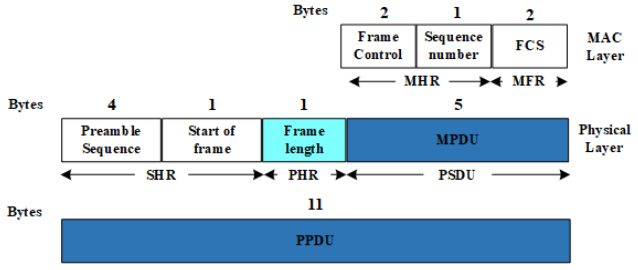

Fig. 4. Confirmation frame format

As a rule, these eclipses are covered during the preparation for the new frame transmission. As a result, the device goes through four different steps when transmitting each frame:

- passive waiting (Wait);

- channel listening (CCA);

- frame transmission (DATA);

- acceptance of confirmation (ACK).

It should be noted that such a sequence is typical for all standards using the CSMA/CA mechanism. Fig. 5 shows the distribution diagram of the time to find a device in different stages at different values of R [4], [22].

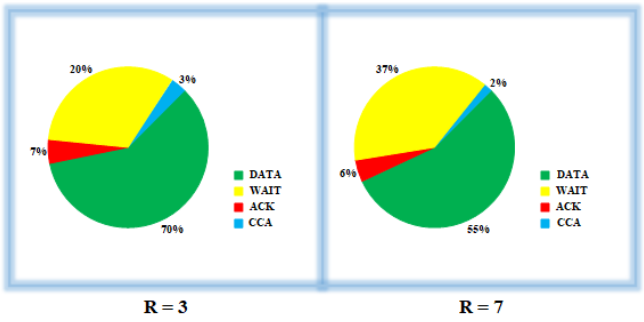

Fig. 5. Time distribution of packet transmission stages in the IEEE 802.15.4 standard network

This distribution is important enough for sensor networks in terms of understanding, comparison of each step of data transfer and power consumption [23].

IV. Algorithms of Network Connectivity and Data Transfer in Wireless Sensor Networks

In the process of remote monitoring, power consumption control is mainly carried out by the network management component, which operates over the Internet, but it is reflected at the wireless sensor network level. ZigBee networks belong to the personal area network (PAN) category [24].

ZigBee networks used for remote monitoring are identified by a unique private network identifier. 64-bit (extended) private communication network identifier and 16-

Authorized licensed use limited to: Tashkent University of Information Technologies. Downloaded on November 23,2023 at 04:56:49 UTC from IEEE Xplore. Restrictions apply.

bit private communication network identifier are supported by ZigBee modules [25].

When starting a wireless network during monitoring, the "Coordinator" first selects a channel and a private network identifier (both 64-bit and 16-bit) [26], [27]. The PAN ID must be separate to distinguish the network from others. When other nodes join the network, all nodes must have the same PAN ID. As with channel selection, in the initial phase of the network, an energy check is performed by the coordinator to find a channel with lower energy consumption. When a sensor node acting as a router or endpoint wants to join the network, they actively scan to find any available coordinators or routers to join. The initialization algorithm of the ZigBee network during monitoring is presented in fig. 6.

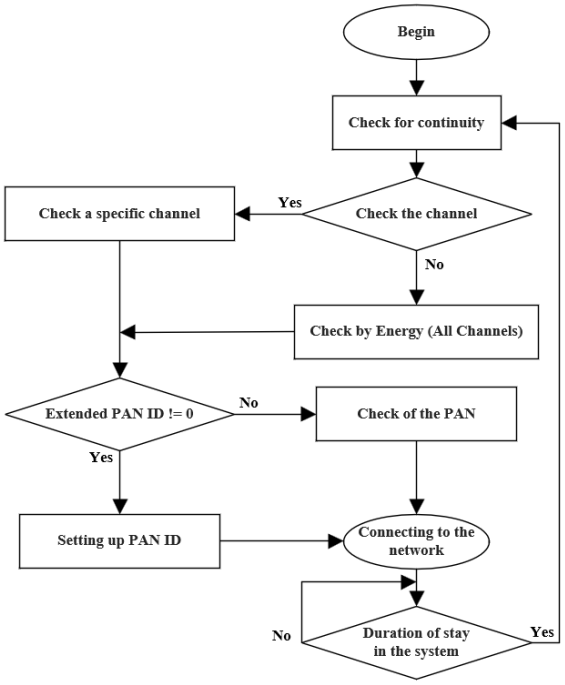

Fig. 6. Initialization algorithm of ZigBee network during monitoring

The extended PAN ID is a 64-bit number that identifies the network. To distinguish a network, it must be unique. All nodes in the same network must have the same PAN ID. There are two conditions for its installation:

Non-zero PAN ID: If the Coordinator sets this parameter to a non-zero value, this PAN ID is set as a 64-bit operating system PAN ID. If routers and endpoints set a non-zero value, they will only join the network with that WAN ID.

Null PAN ID: If the Coordinator sets this parameter to zero, it will select a random 64-bit PAN ID. Routers and end devices try to join this random network if they are not already connected to a network.

The diagram of the last device to be added to the ZigBee network during remote monitoring is shown in fig. 7. In fact, at the bottom of the flowchart, when the last device meets all 39 constraints, it sends a join request. This process introduces it to the network and forces the peer network to detect its presence.

As for sending packets within the network, ZigBee uses 16-bit addressing to reduce overhead. If the destination node's 16-bit address is known, it is displayed in the packet. So, once the route is determined, the transmission starts. Because the network address can change, and a ZigBee device cannot communicate with other devices that do not know the network address. Therefore, an "Addressing" process is performed to determine the 16-bit network address before data transmission. The "addressing" process is based on the fact that a 64-bit address is assigned by the manufacturer in a way that is unique to each ZigBee device and generally known to others [28], [29].

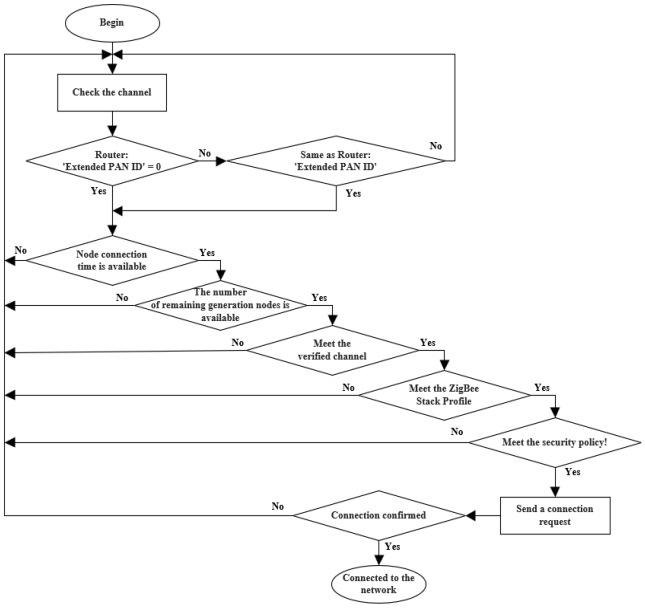

Fig. 7. Flow diagram of the end device joining the ZigBee network

So, if a ZigBee device needs to communicate with an unknown device with a 16-bit address, it will start broadcasting across the entire network. The 64-bit address of the desired device for this broadcast is included in the packet. Any device on the network receiving the broadcast compares the received 64-bit address to the 64-bit address in the broadcast packet. If the addresses match, the device responds to the packet to tell the initiator the desired network address [3], [30], [31]. After this answer comes to the initiator, they can communicate with each other. It should be noted that ZigBee creates a mesh routing network to transfer data between the source device and the destination device. Data packets in mesh routing travel from their source to their destination through multiple hops. Both coordinators and routers can contribute to routes between source and destination devices. The process of finding a suitable route is called route discovery. The routing process in Meshlium and Waspmote is based on the AODV (Ad-hoc on-request Distance Vector routing) protocol [5], [32].

As a physical layer, the WirelessHART protocol uses radio modules developed according to the IEEE 802.15.4 standard, which is widely used in wireless networks, which is one of the advantages of this solution [33], [34].

If a normal WLAN creates only a two-point connection, WirelessHART uses a single-level coding network, that is, a network is organized in which all radio modules are receivers and transmitters of signals. The originating module sends data to a nearby module, which in turn passes it on to the next module, a process that continues until the message reaches the base station. Thus, a sufficiently large area can be covered. If message delivery fails due to receiver failure, alternative

Authorized licensed use limited to: Tashkent University of Information Technologies. Downloaded on November 23,2023 at 04:56:49 UTC from IEEE Xplore. Restrictions apply.

routes are established at the initial stage. Therefore, the message is automatically forwarded via an alternate route. This approach further improves reliability in large-scale sensor networks.

In this case, each computing device of the system performs the tasks of a receiving/transmitting device and a router, which imposes additional requirements on the performance of nodes and work algorithms. As mentioned above, the data transfer process of remote intelligent monitoring based on IoT is divided into several stages (fig. 8).

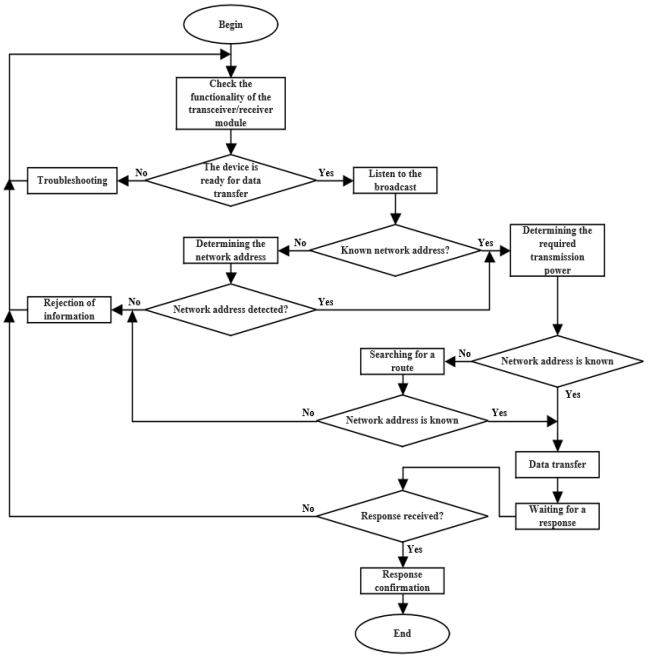

Fig. 8. Algorithm of data transmission between remote intelligent monitoring modules based on IoT

In the monitoring process, after receiving a command from the microcontroller, the device is checked for readiness for data transmission, the need to use a specific operation algorithm (normal, economical, night, day) is analyzed, then the receiving/transmitting device waits at a random time interval. During this time, the following processes occur:

- implementation of the broadcast listening process;

- transmission of monitoring data;

- waiting for a response to the transmitted data.

The maximum number of retransmissions (NR) parameter is used to set the maximum waiting time for a response when transmitting a message to a remote wireless module. Typically, the value of this parameter is set to NR=1.6 seconds per message transfer attempt. Because the data packet transmission time is 30-50 ms, and almost as much time can be spent on data processing, the number of retransmissions can be 8-10. So, if the module does not receive a response within 1.6 seconds, it will automatically make two more attempts. Thus, the total time spent by the stack to deliver one message for 8 rebroadcast networks is 4.8 seconds. If the message is being sent to the last sensor in sleep mode, then the delivery time must also include the sleep time, which can be up to 10 seconds.

V. CONCLUSION

As can be seen from the above, many problems in the remote transmission of data from sensors in the creation of remote monitoring systems have been solved by using wireless sensor networks. In particular, as a wireless sensor network, the IEEE802.15.4 standard has wide possibilities, and its use in monitoring systems can lead to high efficiency. Nevertheless, the issues of reliable data transmission and use of energy-efficient methods will always remain issue when using this standard. The main goal of researching this network is to increase its reliability and energy efficiency. The article proposes several algorithms for improving energy efficiency by ensuring the reliability and timely operation of wireless sensor networks.

REFERENCES

[1] Madhubala S., Nachammai R., Nandhini I., Preethisha A.M., Paulin J.J. (2018) Solar power based remote monitoring and control of industrial parameters using IoT. International Research Journal of Engineering and Technology. Vol. 5(3): March 2018.

[2] Um, J.Y.; Ahn, J.S.; Lee, K.W. “Evaluation of the effects of a grouping algorithm on IEEE 802.15.4 networks with hidden nodes”. J. Commun. Netw. 2014, 16, 81–91.

[3] Sahoo, P.K.; Pattanaik, S.R.; Wu, S.-L. “A Novel IEEE 802.15.4e DSME MAC for Wireless Sensor Networks”. Sensors 2017, 17, 168.

[4] Son, K.J.; Hong, S.H.; Moon, S.P.; Chang, T.G.; Cho, H. “Segmentized Clear Channel Assessment for IEEE 802.15.4 Networks”. Sensors 2016, 16, 815.

[5] IEEE Computer Society. (2015) IEEE Standard for Low - Rate Wireless Networks. IEEE Std 802.15.4™-2015.

[6] E. Navruzov, A. Kabulov. ``Detection and analysis types of DDoS attack,” 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2022, pp. 1-7, doi: 10.1109/IEMTRONICS55184.2022.9795729.

[7] A. Kabulov, I. Yarashov, A. Otakhonov. ``Algorithmic Analysis of the System Based on the Functioning Table and Information Security,” 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2022, pp. 1-5, doi: 10.1109/IEMTRONICS55184.2022.9795729.

[8] C. Ashyralyyev, M. Aripov, A. Kabulov, and etc., “Preface: International conference on “Modern problems of applied mathematics and information technologies-al-Khwarizmi 2021”,” AIP Conference Proceedings (2022).

[9] A. Kabulov, I. Kalandarov, I. Saymanov. ``Development of models and algorithms for transport and group equipment tasks,” Transportation Research Procedia, Volume 63, 2022, Pages 108-118. https://doi.org/10.1016/j.trpro.2022.05.013.

[10] A. Kabulov, I. Saymanov, I. Yarashov, A. Karimov. ``Using Algorithmic Modeling to Control User Access Based on Functioning Table,” 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2022, pp. 1-5, doi: 10.1109/IEMTRONICS55184.2022.9795850.

[11] Isroilov.J.D. Linearization spectral characteristics through passage by means of akusto-optical reconstructed filters // International Conference on Information Science and Communications Technologies ICISCT 2016, 2nd, 3rd and 4th of November 2016, Tashkent, Uzbekistan. DOI: 10.1109/ICISCT.2016.7777386.

[12] Davronbekov.D.A.,Aliev .U.T.Isroilov.J.D.. Using the energy of electromagnetic radiation as a source of power // International Conference on Information Science and Communications Technologies (ICISCT) Applications, Trends and Opportunities, 2nd, 3rd and 4th of November 2017, Tashkent, Uzbekistan. (Scopus) DOI: 10.1109/ICISCT.2017.8188565.

[13] Pulatov.Sh.U, Aliev.U.T.Isroilov.J.D.. Energy harvesters wireless charging technology // International Conference on Information Science and Communications Technologies (ICISCT) Applications, Trends and Opportunities, 2nd, 3rd and 4th of November 2017, Tashkent, Uzbekistan. (Scopus) DOI: 10.1109/ICISCT.2017.8188566.

[14] Davronbekov.D.A., Aliev .U.T.,Isroilov.J.D., Alimdjanov X.F. Power providing methods for wireless sensor // International Conference on

Authorized licensed use limited to: Tashkent University of Information Technologies. Downloaded on November 23,2023 at 04:56:49 UTC from IEEE Xplore. Restrictions apply.

Information Science and Communications Technologies ICISCT 2019, Tashkent, Uzbekistan - 2019. DOI: 10.1109/ICISCT47635.2019.9011850.

[15] Davronbekov D.A., Isroilov.J.D. Akhmedov B.I. Principle of organizing database identification on mobile devices by IMEI // International Conference on Information Science and Communications Technologies ICISCT 2019, Tashkent, Uzbekistan - 2019. DOI: 10.1109/ICISCT47635.2019.9012000.

[16] K. Khujamatov, E. Reypnazarov, N. Akhmedov and D. Khasanov, "Blockchain for 5G Healthcare architecture," 2020 International Conference on Information Science and Communications Technologies (ICISCT), 2020, pp. 1-5, doi: 10.1109/ICISCT50599.2020.9351398.

[17] K. Khujamatov, D. Khasanov, E. Reypnazarov and N. Axmedov, "Industry Digitalization Consepts with 5G-based IoT," 2020 International Conference on Information Science and Communications Technologies (ICISCT), 2020, pp. 1-6, doi: 10.1109/ICISCT50599.2020.9351468.

[18] K. Khujamatov, E. Reypnazarov, N. Akhmedov and D. Khasanov, "IoT based Centralized Double Stage Education," 2020 International Conference on Information Science and Communications Technologies (ICISCT), 2020, pp. 1-5, doi: 10.1109/ICISCT50599.2020.9351410.

[19] I. Siddikov, K. Sattarov, K. Khujamatov, O. Dekhkonov and M. Agzamova, "Modeling of Magnetic Circuits of Electromagnetic Transducers of the Three-Phases Current," 2018 XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE), 2018, pp. 419-422, doi: 10.1109/APEIE.2018.8545714.

[20] K. E. Khujamatov and T. K. Toshtemirov, "Wireless sensor networks based Agriculture 4.0: challenges and apportions," 2020 International Conference on Information Science and Communications Technologies (ICISCT), 2020, pp. 1-5, doi: 10.1109/ICISCT50599.2020.9351411.

[21] Khujamatov, K., Akhmedov, N., Reypnazarov, E., Khasanov, D., & Lazarev, A. (2022). Device-to-device and millimeter waves communication for 5G healthcare informatics. Blockchain Applications for Healthcare Informatics, 181-211. https://doi.org/10.1016/B978-0-323-90615-9.00019-0

[22] Siddikov, I., Khujamatov, K., Khasanov, D., Reypnazarov, E. (2021). IoT and Intelligent Wireless Sensor Network for Remote Monitoring Systems of Solar Power Stations. In: Aliev, R.A., Yusupbekov, N.R., Kacprzyk, J., Pedrycz, W., Sadikoglu, F.M. (eds) 11th World Conference "Intelligent System for Industrial Automation" (WCIS-2020). WCIS 2020. Advances in Intelligent Systems and Computing, vol 1323. Springer, Cham. https://doi.org/10.1007/978-3-030-68004-6_24

[23] S. I. Khakimovich, S. K. Abdishukurovich, D. O. Ravshanovich and K. K. Ergashevich, "Modeling of the processes in magnetic circuits of electromagnetic transdusers," 2016 International Conference on Information Science and Communications Technologies (ICISCT), 2016, pp. 1-3, doi: 10.1109/ICISCT.2016.7777393.

[24] D. Khasanov, K. Khujamatov, B. Fayzullaev and E. Reypnazarov, "WSN-based Monitoring Systems for the Solar Power Stations of Telecommunication Devices", IIUM Engineering Journal, vol. 22, no. 2, pp. 98118, 2021.

[25] Tanwar, S., Khujamatov, H., Turumbetov, B., Reypnazarov, E., Allamuratova, Z. Designing and Calculating Bandwidth of the LTE Network for Rural Areas. International Journal on Advanced Science, Engineering and Information Technologythis link is disabled, 2022, 12(2), pp. 437–445

[26] K. Khujamatov, A. Lazarev, N. Akhmedov, E. Reypnazarov and A. Bekturdiev, "Methods for Automatic Identification of Vehicles in the its System," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-5, doi: 10.1109/ICISCT52966.2021.9670123.

[27] I. Siddikov, D. Khasanov, H. Khujamatov and E. Reypnazarov, "Communication Architecture of Solar Energy Monitoring Systems for Telecommunication Objects," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 01-05, doi: 10.1109/ICISCT52966.2021.9670354.

[28] K.A. Bin Ahmad, H. Khujamatov, N. Akhmedov, M.Y. Bajuri, M.N. Ahmad, A. Ahmadian. Emerging trends and evolutions for Smart city healthcare systems. Sustain. Cities Soc. (May 2022), p. 103695, 10.1016/J.SCS.2022.103695

[29] H. Khujamatov, I. Siddikov, E. Reypnazarov and D. Khasanov, "Research of Probability-Time Characteristics of the Wireless Sensor Networks for Remote Monitoring Systems," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-6, doi: 10.1109/ICISCT52966.2021.9670122.

[30] I. Siddikov, K. Khujamatov, E. Reypnazarov and D. Khasanov, "CRN and 5G based IoT: Applications, Challenges and Opportunities," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-5, doi: 10.1109/ICISCT52966.2021.9670105.

[31] K. Khujamatov, A. Lazarev and N. Akhmedov, "Intelligent IoT Sensors: Types, Functions and Classification," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 01-06, doi: 10.1109/ICISCT52966.2021.9670340.

[32] Khujamatov, K., Akhmedov, N., Reypnazarov, E., Khasanov, D. Traditional vs. the blockchain-based architecture of 5G healthcare. Blockchain for 5G Healthcare Applications: Security and privacy solutions, 2022, pp. 131–167

[33] Ibraimov, R., Sultonova, M., Khujamatov, H. The Integral Distribution Function of the Kilometric Attenuation of Infrared Radiation in the Atmosphere Fergana Region of the Republic of Uzbekistan. Webology. Volume 18, Issue Special Issue, 2021, Pages 316-327. DOI: 10.14704/WEB/V18SI05/WEB18231

[34] Kamal, A., Ahmad, K., Hassan, R., Khalim, K. (2021). NTRU Algorithm: Nth Degree Truncated Polynomial Ring Units. In: Ahmad, K.A.B., Ahmad, K., Dulhare, U.N. (eds) Functional Encryption. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-60890-3_6

Authorized licensed use limited to: Tashkent University of Information Technologies. Downloaded on November 23,2023 at 04:56:49 UTC from IEEE Xplore. Restrictions apply.