






The Model of WBAN Data Acquisition Network Based on UFP

S. Vladimirov¹(✉) , V. Vishnevsky², A. Larionov² , and R. Kirichek¹ 

¹ St.Petersburg State University of Telecommunications, 22 Bolshhevikov Pr.,
St.Petersburg 193232, Russian Federation
vladimirov.opds@gmail.com, kirichek@sut.ru

² V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences,
65 Profsoyuznaya Street, Moscow 117997, Russian Federation
larionandr@gmail.com

Abstract. The paper determines the general model of an unmanned flying platforms based network for collecting information from wearable wireless body area networks. There are considered several possible approaches to its implementation. A list of tasks to be solved and their features in the framework of building a network are given. There are proposed variants of optimal network radio technologies and topologies, antenna devices and types of unmanned flying platforms to create the acquisition network. Variants of implementation of the interaction protocol and methods of organizing secure data transmission, taking into account the peculiarities of the problem being solved, are recommended.

Keywords: WBAN · Data acquisition network · Unmanned flying platform

1 Introduction

In the modern world there is a need for prompt receipt of information. An important part of information collection systems are sensor networks that combine different types of sensors and control units that take readings, process it and send it to the recipient [13, 14].

One of the important types of sensor networks are wearable wireless body area networks (WBANs), which are formed from small-sized body sensor units (BSU) located on the human body and taking readings from it, and a central body control unit (BCU), which collects that readings from BSU and processes them [16, 19]. The BCU is usually a general purpose user device such as a smartphone or tablet, or a specialized microcontroller-based device. In the first case, the WBAN is built on the basis of widely used radio technology supported by most smartphones, such as Wi-Fi or Bluetooth. In the second case, the most suitable wireless personal area network (WPAN) radio technology is selected, for example, ZigBee or another IEEE 802.15 standard [7, 9, 16].

Supported by RFBR according to the research project No.20-37-70059.

© Springer Nature Switzerland AG 2020

V. M. Vishnevskiy et al. (Eds.): DCCN 2020, LNCS 12563, pp. 220–231, 2020.

https://doi.org/10.1007/978-3-030-66471-8_18

The main application of WBAN networks is monitoring of human health indicators. Therefore, they are widely used in medical institutions, professional and amateur sports and military sports games. Also, wearable nets are being actively implemented in the army and rescue services. In all these cases, there is a situation when a certain number of WBANs carrying persons are located in a limited area. Information from WBAN controllers needs to be promptly transmitted to some data collecting center (DCC). For example, timely data on the athletes' health obtained by referees during tournaments can prevent accidents and allow doctors to react more quickly to possible injuries and pre-critical conditions [7, 12].

2 Approaches to Collecting Data from WBAN

Various approaches are used to transfer data from the WBAN controller to the data collecting center. If the WBAN is geographically located within the coverage area of a larger radio access network, be it a wireless local area network (WLAN), a city-wide network (WMAN), or a global wireless network (WWAN), it makes sense to use this larger network to transfer operating data. However, if the location of the WBAN is not covered by the existing radio access network, or information cannot be transmitted over open networks, it is necessary to deploy a dedicated wireless network, so called data acquisition network (DAN), to collect data from the WBAN.

For most radio networks, the best signal reception conditions are obtained with a clear line of sight between the transmitter and receiver. Therefore, it is logical to place the data acquisition node high above the ground. The higher the node is placed, the more coverage it will provide. Naturally, the height of the acquisition node depends on the maximum operating range of the applied wireless technology, which determines the maximum distance from the acquisition node to the most distant WBAN from which information can be collected.

In order not to depend on the presence of buildings, towers or poles on the territory of the DAN location, it is convenient to implement the acquisition node as an unmanned flying platform (UFP). This method allows to place the acquisition node at the optimal place and height for the provided territory and, if necessary, change its location during operation [8, 11].

We represent the organization of a WBAN data acquisition network based on UFPs of various types in the form of Fig. 1.

The parameters that must be taken into account when building an acquisition network based on UFPs, and the issues associated with them, are shown in Fig. 2. In general, their relationship with each other can be represented by the function

$$[z_1, z_2, \dots, z_n] = F(p_1, p_2, \dots, p_m), \quad (1)$$

z_i —issues to solve; p_j —network parameters.

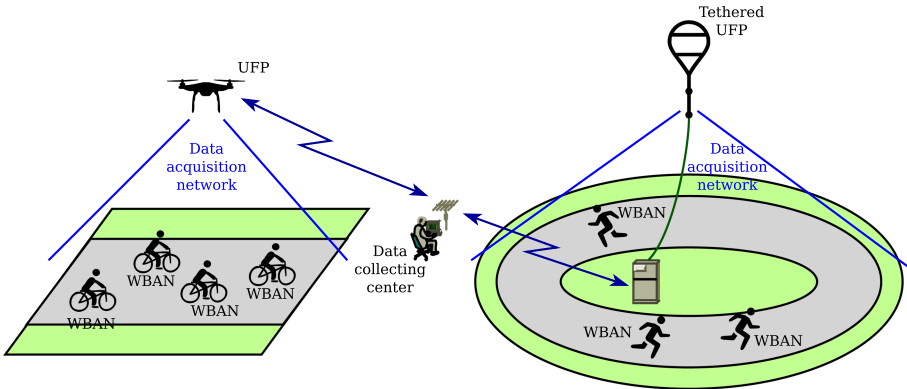


Fig. 1. WBAN data acquisition network based on UFP.

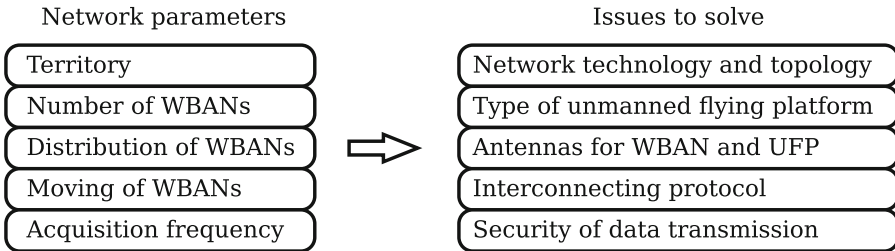


Fig. 2. Network parameters and issues to solve.

3 Issues to Solve

3.1 Network Technology and Topology

The choice of radiotransmitting technology and topology of the deploying DAN primarily depends on such factors as the size and topography of the area where the data acquisition network needs to be deployed. In the case of some sporting events, such as marathon or cycling, or military sports games, the area of the event can be quite large and the use of distributed acquisition wireless networks based on the widely used Wi-Fi technology will require additional deployment costs due to the limited communication range and significant energy consumption of the acquisition nodes. Using cellular technologies based on a single base station can be convenient, but will require a deployment license. Thus, it is advisable to use medium and long range technologies that have low power consumption and operate in unlicensed frequency bands, such as LoRa, DECT-ULE or Bluetooth LE [5, 17, 26]. Since the very idea of collecting information from a WBAN does not imply the exchange of a large amount of information, the requirements for the data transfer rate in such networks are insignificant.

After determining the technology, you need to select the topology of the data acquisition network. Depending on the network coverage area, either a

star-shaped network with one acquisition node or a distributed multinode network should be used (Fig. 3). The height of the UFP with the acquisition node will depend on the maximum working distance of the radio link, which determines the maximum distance from the acquisition node to the most distant WBAN from which information is to be read.

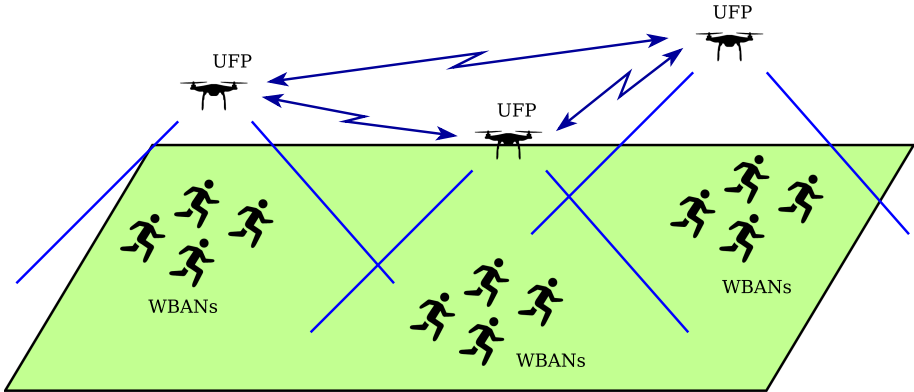


Fig. 3. Distributed multinode data acquisition network

3.2 Type of UFP

Unmanned flying platforms are classified according to several criteria.

By design, there are UFPs heavier than air, which include aircraft and multi-rotor platforms, and platforms lighter than air—balloon type [2].

To solve the presented issue, it seems efficient to use multi-rotor or balloon UFPs, which can hover for a while at a given point. At the same time, aerostatic platforms will be convenient in situations where a long-term placement of the acquisition node is required without the need for a quick change of position. Multi-rotor UFPs are more versatile and allow moving the acquisition node at a sufficiently high speed, which can be a determining factor in the expected active movement of the served WBANs along a certain route. Such systems have a limited run time and place increased demands on the power supply.

According to the height of placement, two types of flying platforms are usually distinguished: operating at heights of up to a few kilometers, the so-called LAPs—low-altitude platforms, and HAPs—high-altitude platforms, operating in the altitude range from 17 to 21 km [2]. To collect information from WBANs, it is more convenient to use platforms operating at low altitudes up to hundreds of meters.

According to the method of communication with the ground, the platforms are divided into tethered, in which communication is provided via the connecting cable [21, 22], and autonomous, using a radio channel.

The choice of communication method depends on the number, location and speed of WBAN's movement. Tethered platforms are useful when there is a lot of information being transferred. In such cases, the UFP, in addition to the functions of the acquisition node, can perform the functions of a video surveillance system. Tethered systems traditionally have greater run time, since they can be powered from a stationary power source located on the ground. However, tethered platforms are not mobile and have a limited working height. The radio channel allows the use of highly mobile acquisition nodes, but it is important to choose the right data transmission technology. In the case of using one radio technology to connect the acquisition node with the data collection center and WBAN networks, it is necessary to take measures to minimize the mutual influence of communication channels. When operating at different frequencies, this problem goes away, but at the same time it requires the use of several transceiver devices, which accordingly leads to an increase in the size, weight and energy consumption of the acquisition node.

3.3 Antennas for WBAN and UFP

Antennas used by WBAN are primarily limited by the linear dimensions of the wearable controller module. The use of efficient large aperture antennas will result in inconvenience for the user to wear the WBAN. It should be additionally taken into account that the location of the antenna relative to the acquisition node is not known in advance, therefore it is advisable to use omnidirectional antennas in a compact design, such as linear and helical monopole antennas and a planar antennas [4, 18, 25, 27, 28].

The antennas placed on the UFP have smaller size restrictions, since the linear dimensions of the UFP, which have sufficient carrying capacity and duration of operation to perform the functions of a data acquisition node, already exceed the linear dimensions of the microwave antennas. On UFPs, the best option would be to use efficient antennas with a large aperture. Considering that the UFP is always located above the WBAN (Fig. 1), antenna structure should have a directional pattern towards the ground. Among the effective antennas of this type are dipoles [3, 6] and biquadrats [15]. The advantage of these antennas is their flat design, which is convenient for placement on the bottom of the UFP.

It is important to note that the directional pattern of the antenna determines the UFP coverage area. Therefore, when deploying a data acquisition network and designing UFP, this issue must be paid special attention. In particular, it is possible to change the directional pattern using reflector.

3.4 Interconnecting Protocol

For interaction between acquisition nodes and WBAN networks, you can use existing protocols or develop your own exchange protocol. It should be noted that collecting information from WBAN sensor networks involves the transmission of data in a previously known format. Earlier it was noted that the acquisition network usually has a simple structure that does not require the use

of complex routing and addressing protocols. Thus, it seems optimal to use a specially developed data transfer protocol that works directly on top of the link layer protocol, which will provide a minimum amount of service information, in contrast to the case with the deployment of a network based on standard TCP/IP protocols.

The WBAN readings acquisition network is generally represented as a dynamic redundant system formed by N WBAN controllers, M mobile UFP nodes and L stationary nodes that form a network from the WBAN to the data collection center. Information transfer is carried out along a chain in three stages: from WBAN to UFP, from UFP to stationary nodes and further from stationary nodes to DCC. At each of these stages, data can be transmitted using various technologies. From the point of view of organizing the data collection, the most interesting is the interaction between WBAN and UFP, which occurs actually at the data collection stage.

The number of WBANs served by one UFP at a collection stage can vary, and the number of UFPs operating simultaneously at a single territory can also change, as shown in Fig. 3. Accordingly, the network must provide a mechanism for registering WBAN to UFP. The entire UFP operation time is divided into cycles, each of which consists of two periods: the W_{reg} time window (registration channel), during which WBANs register with the UFP, and the W_{data} window (data channel), during which the UFP polls the registered WBANs. In the W_{reg} window, the predefined transmission parameters are necessarily used, which are the same for all WBANs and UFPs. Depending on the technology used, it can be a separate frequency channel, CDMA code or chirp spreading factor. In the W_{data} window, work is carried out with parameters that are separate for each UFP. This allows multiple UFPs to operate simultaneously in the same area without interfering with each other.

During the W_{reg} WBANs are registered with the UFP based on channel time contention, treating the registration channel as a common shared medium. As a method of accessing the medium, it is optimal to use the traditional CSMA/CA algorithm based on checking the channel before data transmission. The start of the registration window is determined by the UFP through a Registration Request (RReq) packet containing the UFP identifier and data channel settings. In order to avoid collisions during registration, WBANs that receive an RReq and want to transmit information to the UFP, at a random interval, send a Registration Reply (RRep) packet with the WBAN identifier, the size of the information to be transmitted in bytes and the urgency of the data. After receiving the RRep, the UFP sends the next RReq, which indicates the identifier of the previously registered WBAN. If the RRep packet was not received by the UFP, for example, due to a collision, then the next RReq indicates the identifier of the last registered WBAN. Thus, the WBAN that failed to register is aware of this and can try to register again. In total, the UFP sends N_{req} RReqs during the registration window. Accordingly, during the time W_{reg} , $N_{reg} \leq N_{req}$ WBAN can be registered. WBAN, registered to UFP, switch their transceivers to data channel settings.

The duration of one stage of registration is estimated by the formula

$$T_{reg} = \frac{(L_{RReq} + L_{RRep})}{B} + t_{proc}, \tag{2}$$

L_{RReq} —size of Registration Request from UFP in bits; L_{RRep} —size of Registration Reply from WBAN in bits; B —channel data rate in bps; t_{proc} —time of processing RReq by WBAN and RRep by UFP in seconds.

Accordingly, the duration of the W_{reg} window is

$$T_{W_{reg}} = N_{req} \cdot T_{reg}. \tag{3}$$

An example of the acquisition system operation in the registration window is shown in Fig. 4. The scenario is considered with $N_{req} = 8$. Taking into account three errors of reception and transmission, $N_{reg} = 5$ WBAN out of k possible were registered on the UFP.

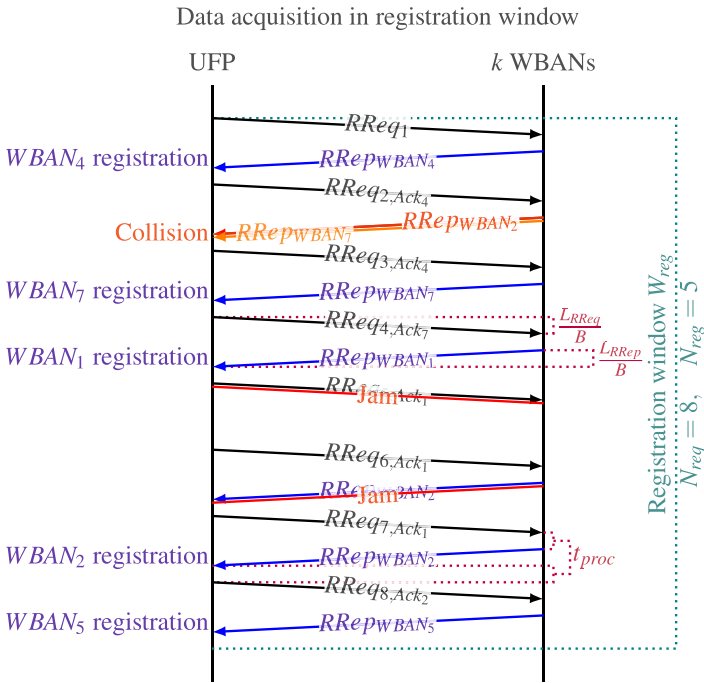


Fig. 4. An example of the registration window W_{reg}

After receiving requests from all registered WBANs, the UFP generates a polling sequence of N_{reg} length, taking into account the urgency indicators received from the WBAN. Further, during the next data channel W_{data} the UFP polls the selected WBANs on a priority basis, sending Data Request (DReq)

packets with the identifier of the polled WBAN, for example, $WBAN_1$. The $WBAN_1$, which receives a DReq with its ID, responds with a Data Reply (DRep) packet. The UFP checks the DRep by comparing the IDs and, if necessary, the checksum, and then replies with the next DReq packet, in which it acknowledges data reception and requests readings for the next WBAN in the sequence, for example, $WBAN_2$. If the DRep packet was transmitted with an error or lost, the UFP repeats request data by the DReq with ID of $WBAN_1$. If after 2 repeated requests it was not possible to receive data from $WBAN_1$, it is marked as unavailable and is no longer polled until the next registration request is received from it. The DCC is notified of an unsuccessful attempt to receive data from $WBAN_1$.

The polling time of one WBAN node during the W_{data} window is estimated by the formula

$$T_{WBAN} = \frac{(L_{DReq} + L_{DRep})}{B} + t_{proc}, \quad (4)$$

L_{DReq} —size of Data Request from UFP in bits; L_{DRep} —size of Data Reply from WBAN in bits; B —channel data rate in bps; t_{proc} —time of processing DReq by WBAN and DRep by UFP in seconds.

The duration of the W_{data} window depends on the number of N_{rpt} repeated requests and is equal to

$$T_{W_{data}} = (N_{reg} + N_{rpt}) \cdot T_{WBAN} + \left(\frac{L_{DReq}}{B} + 0.5t_{proc} \right), \quad (5)$$

where the second summand takes into account the confirmation of the final data packet.

An example of the acquisition system operation in a data transmission window is shown in Fig. 5. The scenario with $N_{reg} = 5$ is considered, corresponding to the previously considered registration example in Fig. 4. We will assume that, in accordance with the urgency indicators, the UFP has formed a polling sequence: $WBAN_1$, $WBAN_7$, $WBAN_2$, $WBAN_4$, $WBAN_5$. Due to two transmission errors, $N_{rpt} = 2$ repeated requests were made.

To increase the survivability of the system and prevent the loss of data of a higher category of urgency or importance in the event of a discharge of the $WBAN_i$ power supply, data transmission is provided to the neighboring WBANs and further to the WBAN in the UFP visibility zone for organizing urgent transmission. Transit WBANs do not process the data received from $WBAN_i$, but simply transmit them in the usual order to the UFP, indicating the maximum urgency.

At the end of the data transmission window, UFP and WBAN switch back to registration mode and the cycle repeats.

The suggested protocol packet format is shown in Fig. 6.

At the beginning of the packet there is address information containing the receiver's identifier and the sender's identifier. The content of the data block depends on the direction of transmission. In general, the UFP sends a data transmission command and a list of requested readings to the WBAN nodes, and the WBAN responds with sensor readings. If each WBAN in the acquisition

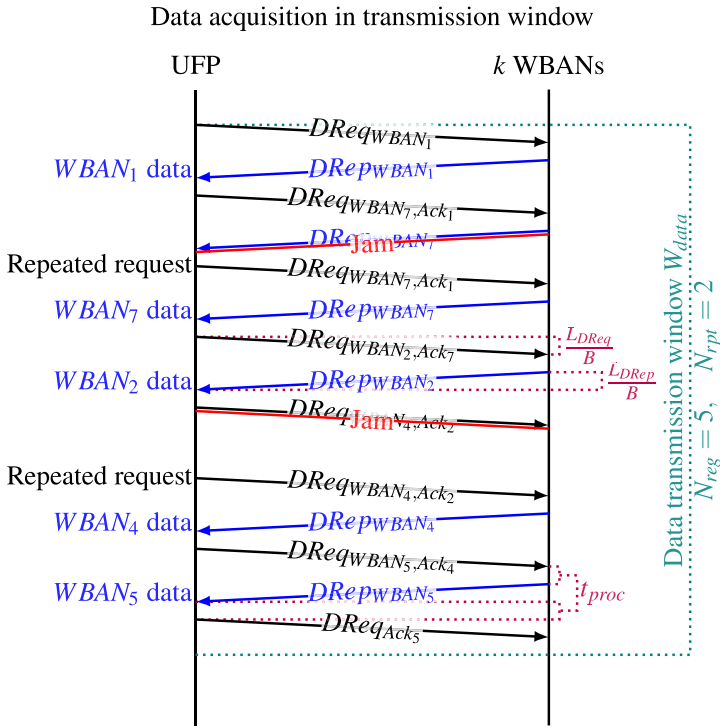


Fig. 5. An example of the data transmission window W_{data}

Receiver Address/ID	Sender Address/ID	Data	Checksum (Hash)
---------------------	-------------------	------	-----------------

Fig. 6. Protocol packet format for data acquisition network

network contains several sensors, then their readings should be separated from each other. In the case when all WBANs contain the same set of sensors, the order of the readings can be foreseen and only the readings themselves can be transmitted. A more universal option is a separate data block for each readings, consisting of three fields: the header, the block length in bytes and the readings themselves. The sizes of the header and length fields are selected based on the number of possible values. Considering that the number of sensors traditionally used in WBAN is limited, it seems optimal to use 1 byte for the header and field length, as shown in Fig. 7.

This method allows to transmit only the necessary readings and optimize the load on the acquisition network. Also, the specified format of data blocks allows them to be used for negotiating encryption keys in cases where it is necessary.

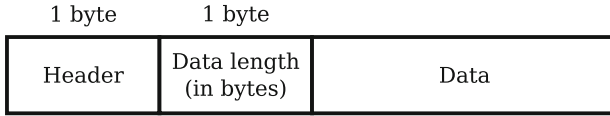


Fig. 7. Data block format for data acquisition network

3.5 Security of Data Transmission

To ensure the secure interaction of the acquisition network nodes and WBANs, it is necessary to solve the problems of mutual identification of the acquisition nodes and the WBAN, as well as to define methods of encryption and integrity checking, which together will provide protection against data interception and substitution by third-party devices.

It is proposed to use various identification methods as device identifiers. The main criterion for choosing a method is the uniqueness of the identifiers used. Ideally, identifiers should be globally unique for maximum flexibility and security. For example, the MAC addresses of the controllers, numeric DOI [1] or the CID and Ecode identification systems [20]. Also there is a developed technique for generating unique hardware identifiers based on degraded NAND [10] or NOR [23,24] flash memory.

For encryption and checking the integrity of the transmitted data, it seems optimal to use the classic combination of symmetric cipher for data exchange, asymmetric encryption for exchange of symmetric encryption keys and hash functions for checking integrity. The choice of specific algorithms depends on the requirements for the acquisition network and the equipment used. For example, when using controllers with low computational capabilities, you should use fast algorithms that do not require productive hardware resources. Also a number of microcontrollers have built-in hardware mechanisms for quickly calculating cryptographic functions, which reduces the time spent on encryption.

4 Conclusion

The article proposes a general model of data acquisition network for collecting information from wireless wearable networks based on unmanned flying platforms. The main conceptual approaches to solving problems of network design and their features are considered. It is planned to continue work within the framework of the tasks considered.

References

1. Albahri, M., Kirichek, R., Muthanna, A., Ateya, A., Borodin, A.: Combating counterfeit for IoT system based on DOA. In: 2018 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), p. 8631257 (2018)

2. Alsamhi, S., Rajput, N.: An intelligent HAP for broadband wireless communications: developments, QoS and applications. *Int. J. Electron. Electr. Eng.* **3**(2), 134–143 (2015)
3. Bath, A., Thakur, A., Sharma, J., Prasad, B.: Analyzing the different parameters of dipole antenna. *Int. J. Electr. Electron. Eng.* **1**(1), 11–15 (2014)
4. Chandran, A.R., Conway, G.A., Scanlon, W.G.: Compact slot-loaded patch antenna for 868 MHz wireless body area networks. In: 2008 Loughborough Antennas and Propagation Conference, LAPC, pp. 433–436 (2008)
5. Das, K., Havinga, P.: Evaluation of DECT-ULE for robust communication in dense wireless sensor networks. In: 2012 3rd IEEE International Conference on the Internet of Things, pp. 183–190. Wuxi (2012)
6. Dw, E.F., Pratama, H., Ihsan, N., Rahmatia, S., Wulandari, P.: Design and performance investigation of dipole antenna using aluminum and iron at 644 MHz - 736 MHz. In: International Conference on Engineering, Technologies and Applied Sciences, Kuala Lumpur, Malaysia, January 2017
7. Ghamari, M., Janko, B., Sherratt, R., Harwin, W., Piechockic, R., Soltanpur, C.: A survey on wireless body area networks for eHealthcare systems in residential environments. *Sensors* **16**, 831 (2016)
8. Ha, I., Cho, Y.: Unmanned aerial vehicles-based health monitoring system for prevention of disaster in activities of the mountain. *Int. J. Control Autom.* **9**(9), 353–362 (2016)
9. IEEE: IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks. IEEE Std 802.15.6-2012 (2012)
10. Jakobsson, M., Johansson, K.A.: Unspoofable device identity using NAND flash memory. *SecurityWeek* (2010). <http://www.securityweek.com/unspoofable-device-identity-using-nand-flash-memory>
11. Kirichek, R.: The model of data delivery from the wireless body area network to the cloud server with the use of unmanned aerial vehicles. In: Proceedings 30th European Conference on Modelling and Simulation (ECMS), pp. 603–606 (2016)
12. Kirichek, R., Pirmagomedov, R., Glushakov, R., Koucheryavy, A.: Live substance in cyberspace - Biodriver system. In: 18th International Conference on Advanced Communication Technology (ICACT) 2016, pp. 274–278 (2016)
13. Koucheryavy, A., Salim, A.: Cluster-based perimeter-coverage technique for heterogeneous wireless sensor networks. In: 2009 International Conference on Ultra Modern Telecommunications and Workshops St. Petersburg, p. 5345452 (2009)
14. Koucheryavy, A., Vladyko, A., Kirichek, R.: State of the art and research challenges for public flying ubiquitous sensor networks. *Lect. Notes Comput. Sci.* **9247**, 299–308 (2015)
15. Li, R., Traille, A., Laskar, J., Tentzeris, M.M.: Bandwidth and gain improvement of a circularly polarized dual-rhombic loop antenna. *IEEE Antennas Wirel. Propag. Lett.* **5**, 84–87 (2007)
16. Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D., Jamalipour, A.: Wireless body area networks: a survey. *IEEE Commun. Surveys Tutorials* **16**(3), 1658–1686 (2014)
17. Olatinwo, D.D., Abu-Mahfouz, A., Hancke, G.: A survey on LPWAN technologies in WBAN for remote health-care monitoring. *Sensors* **19**(23), 5268 (2019)
18. Salim, M., Pourziad, A.: A novel reconfigurable spiral-shaped monopole antenna for biomedical applications. *Progress Electromagnet. Res. Lett.* **57**, 79–84 (2015)
19. Schmidt, R., Norgall, T., Morsdorf, J., Bernhard, J., Grun, T.: Body area network BAN - a key infrastructure element for patient-centered medical applications. *Biomedizinische Technik/Biomed. Eng.* **47**(s1a), 365–368 (2002)

20. Soldatos, J., Yuming, G.: Internet of things. EU-China joint white paper on internet-of-things identification. Technical report, European Research Cluster on the Internet of Things (2014)
21. Vishnevskiy, V., Shirvanyan, A., Tumchenok, D.: Mathematical model of the dynamics of operation of the tethered high-altitude telecommunication platform in the turbulent atmosphere. In: 2019 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2019, p. 8706784 (2019)
22. Vishnevskiy, V., Efrosinin, D., Krishnamoorthy, A.: Principles of construction of mobile and stationary tethered high-altitude unmanned telecommunication platforms of long-term operation. *Commun. Comput. Inf. Sci.* **919**, 561–569 (2018)
23. Vladimirov, S., Kirichek, R.: The IoT identification procedure based on the degraded flash memory sector. In: Galinina, O., Andreev, S., Balandin, S., Koucheryavy, Y. (eds.) NEW2AN/ruSMART/NsCC -2017. LNCS, vol. 10531, pp. 66–74. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-67380-6_6
24. Vladimirov, S., Pirmagomedov, R., Kirichek, R., Koucheryavy, A.: Unique degradation of flash memory as an identifier of ICT device. *IEEE Access* **7**, 107626–107634 (2019)
25. Wang, J.C., Lim, E.G., Leach, M., Wang, Z., Man, K.L., Huang, Y.: Conformal wearable antennas for WBAN applications. In: Proceedings of the International MultiConference of Engineers and Computer Scientists 2016, vol. II, IMECS 2016, 16–18 March 2016, Hong Kong, pp. 651–654 (2016)
26. Wu, F., Wu, T., Yuce, M.R.: An internet-of-things (IoT) network system for connected safety and health monitoring applications. *Sensors* **19**(1), 21 (2019)
27. Xue, D., Garner, B., Li, Y.: Electrically-small folded cylindrical helix antenna for wireless body area networks. In: 2016 Texas Symposium on Wireless and Microwave Circuits and Systems (WMCS), Waco, TX, pp. 1–4 (2016)
28. Xue, S., Yi, Z., Xie, L., Wan, G., Ding, T.: A displacement sensor based on a normal mode helical antenna. *Sensors* **19**(17), 3767 (2019)