2019 International Science and Technology Conference "EastConf"

Development and Research Self-Organizing Network Based on Protocol IEEE 802.11 Wi-Fi

Antipova L.A.
Dept.of Computer Science, Engineering and Security
Altay State Technical University
Barnaul, Russia
e-mail: aa.antipova@bk.ru

Borisov A.P.
Dept.of Computer Science, Engineering and Security
Altay State Technical University
Barnaul, Russia
e-mail: boralp@mail.ru

***Abstract*—The article describes how to organize a channel for data transfer using the IEEE 802.11 Wi-Fi standard defined by the mesh topology. As the end nodes of the network, fairly common modules based on the ESP8266EX microprocessor are used, which differ from their competitors not only by the ease of downloading the program code and further use, but also at a relatively affordable price. Theoretical, practical indicators of communication range, the question of the security of the self-organizing network obtained and possible applications are analyzed. Theoretical calculations of the communication range were confirmed experimentally, showing an excellent result in the percentage of received packets. The results obtained completely satisfy the definition of the topology used. Based on the definition of the 802.11s standard, an increase in the network when connecting points can occur at any time, which increases the distance between the sender and the receiver. Development can be used to exchange messages in narrowly specialized industries, educational purposes, and also apply universally.**

Keywords*—*network, Wi-Fi, mesh, Wemos D1 mini, wireless communication channel, protection, hacking.

I. Introduction

To date, it seems difficult to challenge the importance of wireless technologies for building networks of various scales, including Wi-Fi [1]. If before the creation of an effectively protected transmission channel without wires was not possible, especially on a sufficiently large scale, now the concept of mesh with the use of modern equipment solves this problem [2].

Mesh-networks Wi-Fi - a fully-connected network, where each point can establish both wireless and wire connection to any other; including using such integration of various technologies, they represent a lot of interesting solutions [3].

The topology of such networks is based on a decentralized scheme for organizing communication between active nodes of the network. Access nodes not only realize themselves as subscribers, but also act as routers (repeaters) for other nodes on the same network. Due to this, it becomes possible to create large coverage areas of the network with interchangeable active nodes, as well as the possibility of scaling (in this case new nodes are added to the network automatically) [4].

In data collection systems, their measurement and systematization in the industrial sector, one of the most important tasks was and still is the exchange of information at short distances, the mobility of the devices (equipment) used, the cost of installation and installation [5]. As a consequence, at the moment the most active work is being done to create and implement new short-range radio communication devices. They are most intensively used both in the above systems, and in many other applications [6].

This work consecrates one of these solutions: building your own dynamic network for data exchange. The relevance of this topic, as well as the type of network itself, is confirmed by the rapid development of microelectronics, including for use in IoT [7], and thus the emergence of a variety of devices capable of operating autonomously for a long time, and, most importantly, the independence and stability of the received network.

The main results of studies of mesh networks based on wireless Wi-Fi technology are presented in the works of Guss S.V. [8], Vishnevsky V.M. [9,10,12] and others. These works examine the ways of networking, in particular the structure of the package of the protocol 802.11s, gives a brief overview of examples of existing mesh networks of general use in the world, based on the principles of self-organization, and also discusses the creation and deployment of a private mesh network, problems arising with this and the methods of their solutions [8].

The purpose of the work is the development of a Wi-Fi communication channel based on a mesh network.

The tasks of the work include:

- development of the hardware and software complex for the implementation of the mesh network;

- investigation of the complex for range, noise immunity and resistance to burglary.

II. Main Principles of 802.11s Standard

IEEE 802.11s, which allows the creation of managed networks, is part of the IEEE 802.11 standard. In this implementation, one of the basic principles is that access points form a fault-tolerant network (since single points of failure are excluded). This architecture assumes an excellent

978-1-7281-1931-1/19/$31.00 ©2019 IEEE

coverage of the network, and the connection of access points is possible, both with the help of a cable, and without such physical connections. In practice, mesh networks consist of nodes developed by different manufacturers, so, most often, they have to be configured each separately, but the route of transmitted data packets between the nodes of the test networks is determined already in dynamic mode [9].

In this standard, new protocols are introduced at the physical layer and the MAC sublayer of the link layer supporting broadcast and multicast transmissions, as well as unicast delivery over a self-configuring system of Wi-Fi access points. To this end, the standard introduces a four-address frame format.

In existing 802.11 networks, client endpoints (STA) are connected to access points (APs) and can only communicate with them. APs have access to other networks (for example, the Internet), but they can not communicate with each other.

In mesh networks, in addition to terminal stations and access points, there are special devices - nodes mesh (Mesh Point - MP), able to interact with each other and support mesh services. One device can combine several functions. So, mesh-network nodes, combined with access points, are called mesh access points (Mesh Access Point, MAP). Portals mesh-network (Mesh Point Portal, MPP), being MP, connect mesh-network with external networks. Thus, the mesh-network from the point of view of other devices and protocols of a higher level is functionally equivalent to a broadcast Ethernet network, all nodes of which are directly connected at the link level.

The difference between the MAP packets of the described standard is the presence of a mesh header at the beginning of the data field. This header is present in the data packets if and only if they are transferred from the mesh node to the mesh node by the connection established between them.

The Mesh header contains four fields (fig. 1). The byte of the mesh flags controls the processing of the mesh header. While only the first two bits are used, they simply determine the size of the extended mesh address. The "Mesh Time To Live" (MTL) field contains the remaining maximum number of steps between nodes that a packet can make in the mesh network. Thus, the packet's lifetime is limited with multi-step forwarding, which helps to combat the formation of cyclic routes. The number of the packet in the sequence (Mesh Sequence Number) suppresses the appearance of duplicate packets in the broadcast and multicast messages. The mesh Address Extension field can include additional addresses (Address 4, Address 5 and Address 6, each with 6 bytes), which allows mesh packets to contain up to 6 addresses [10].

The IEEE 802.11 standard supports two modes of wireless networks: hot spot and ad hoc [11]. In hot spot mode, one of the stations operates as an access point, and data can only be transmitted between the access point and other stations in the network. In ad hoc mode, transmission is possible between any two stations.

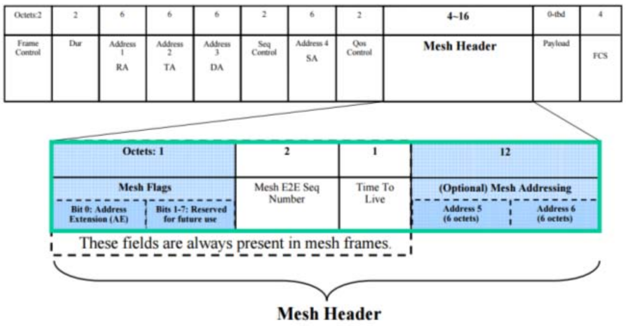

Fig. 1. Format of the MAC-frame with the Mesh-header.

In general, the idea of a mesh-like self-organizing network is as follows: if, for example, you live in an apartment building, and in most apartments there are wireless access points (and at the moment, to a greater extent, this is an indisputable fact) with an exit on the Internet, then such routers can be merged into a mesh network. The advantage can be called even that, if the speed decreases for one of the users, you can use the Internet neighbors.

III. Proposed Solution

In reality, this example is not widely distributed, but still does not lose its relevance. In our case, to replace the routers with direct access to the Internet, Wemos d1 mini became the optimal choice, on the basis of which an independent network for data circulation will be built.

The choice of the experimental device that realizes the network model for testing in practice plays a big role both for the operability of the network itself and the expediency of further development, since it is necessary to take into account not only the ease of flashing (considering the need for repeated loading of the program code) , simplicity in further work with the device, but also its price segment.

WeMos D1 mini is a board with a large amount of program memory and RAM memory (in contrast to its counterparts), is built on the basis of a 32-bit microcontroller with a higher clock speed and is equipped with a built-in Wi-Fi module that can be configured as a client (station, STA), an Access Point (AP), or a client with an access point, which is a particularly important factor for future decentralized mobile network devices [12].

The board is designed to create Internet of Things (IoT) projects and, despite its small size, the microcontroller is able to keep a connection to any other Wi-Fi access point with a reduced power consumption of just 1 mA.

The WeMos D1 mini board can be powered from USB via a USB-microUSB cable, or from an external 5 V power supply (5V and GND terminals), or 3.3V DC (3V3 and GND) terminals. Also, the board can be powered from a 7-24 V power supply by connecting it via WeMos DC Power Shield.

The microcontroller consumes up to:
- 200 mA in the mode of data transfer via WiFi.
- 60 mA in the mode of data reception via WiFi.
- 40 mA in standby mode.

978-1-7281-1931-1/19/$31.00 ©2019 IEEE

When downloading the program code [13], which processes a specific type of received message, data transmission is performed according to the required topology (including its advantages: stability to the loss of individual elements, scalability, the ability to capture a large area) [14].

IV. Theoretical and Experimental Studies

We calculate the theoretical range of information transfer for one device.

The parameter FSL (loss in free space) is determined by the total gain of the system. The total gain of the system is considered as follows:

$$Y = P_t + G_t + G_r - P_{min} - L_t - L_r,$$

where Y is the total system gain (dB), P_t is the transmit power (dBm), G_t is the transmit antenna gain (dBi), G_r is the receive antenna gain (dBi), P_{min} is the receiver sensitivity at this speed (dBm), L_t - loss of signal in the coaxial cable and connectors of the transmission path (dB), L_r - loss of signal in the coaxial cable and the connectors of the receiving path (dB).

FSL is calculated by the formula:

$$FSL = Y - SOM,$$

where SOM (System Operating Margin) is the reserve in the power of radio communication (dB).

The parameter SOM is usually taken equal to 10 dB, since it is considered that 10 - decibel margin for amplification is sufficient for engineering calculation.

As a result, we obtain the communication range formula:

$$D = 10^{\left(\frac{FSL}{20} - \frac{33}{20} - lgF\right)},$$

where D is the communication range in kilometers, F is the center frequency of the channel used [15].

The transmitter power declared by the module manufacturer is 20.5 dBm at 100 mW, the sensitivity is - 93 dBm at a speed of 6 Mbit / s.

Taking into account the gain of 3 dBi (at the receiver and the transmitter they are equal) and the absence of signal loss in the coaxial cable, we find that the theoretical communication range for the two devices with the given data is 62 m, which was confirmed in practice (≈55 m) [16] .

The experiment was also carried out for several devices. When the points were located in two rooms (fig. 2), separated by a concrete adjacent wall, the loss of the packets was not observed.

If one point (for example, the receiver) remains in the room, and the intermediaries with the sender are at a sufficient distance (such that only one intermediary sees the end point - according to Fig. 3), only one packet is lost from five packets. The finding of knots on different storeys also showed a loss of not more than 80% of the packets [17].

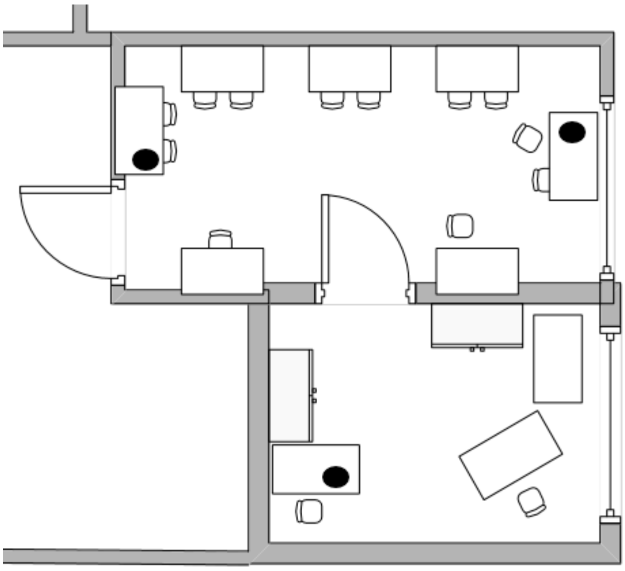

Fig. 2. The layout of the points in the room.

For clarity, we will formulate the result in the Table I.

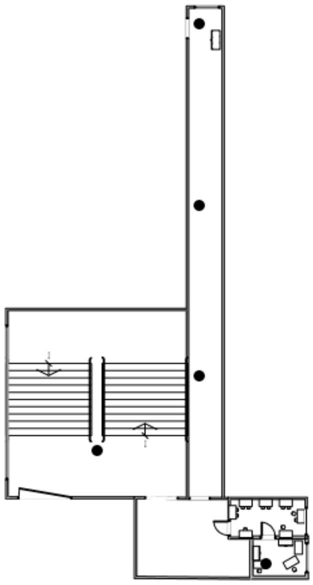

Fig. 3. The layout of points in a complex layout.

TABLE I. Results of the Study

Obstacle	Percentage of received packets
Distance of 3 m, concrete wall	100%
Distance in 80 m between the sender and the receiver	80%
Number of storeys	80%

The results obtained completely satisfy the definition of the topology used [18]. Based on the definition of the 802.11s standard, an increase in the network when connecting points can occur at any time, which increases the distance between the sender and the receiver [19].

Since the network built on the above-described devices is not an ordinary thing, it is an interesting subject for detailed study including transmission safety. For these purposes, it became necessary to intercept and analyze traffic that was being transmitted.

In practice, the built-in WPA / WPA2-PSK encryption is subject to hacking, as on any other device. This was proved by using the main method for this technology: interception of the handshake (handshaking in wireless networks, the exchange of information between the access point and the client at the time of the client's connection to it) and further dictionary attacks, which confirms the need to use more organizational security measures when using system, for example, a well-applied password policy.

V. Conclusions

Thus, the developed network with the described algorithm of processing packages in combination with the software can have extensive practical application, since the devices used are quite common and lie in an affordable price category.

Theoretical calculations of the communication range were confirmed experimentally, showing an excellent result in the percentage of received packets.

The system can be widely used [20]: for exchanging messages in narrowly specialized industries, for educational purposes (more detailed study of the principle of mesh networks operation), in temperature monitoring systems [21], and for meteorological observations [22], and also everywhere.

Acknowledgment

The authors are deeply grateful to the leadership of Altai State Technical University. of I.I. Polzunov (AltSTU) for providing financial support in the publication of this article and to the students of the same university for their help in creating separate components of the experimental information and measuring system used in the studies.

References

[1] L.A. Antipov, A.P. Borisov, “Analysis of communication standards in the concept of Internet of Things”, Modern technologies in the world scientific space: a collection of articles of the International Scientific and Practical Conference, vol. 4, Ufa: AETERNA, 2016, pp. 35-39.

[2] T. Rappaport, “Wireless Communications: Principles and Practice”, USA: Prentice Hall, 2002.

[3] P. Roshan, D. Lieri, “Basics of building wireless local area networks of the 802.11 standard”, M.: Vil'yams, 2004.

[4] V.M. Artyushenko, V.A. Korchagin, “Self-organizing mesh-networks for private use”, Electrotechnical complexes and systems, 2010, vol. 6, № 2, pp. 18-24.

[5] G. Semyuel, “Internet of Things”, Moscow: Al'pina Pablisher, 2016, p. 188.

[6] E.P. Zaramenskikh, “Internet of Things”, Research and field of application, Moscow: Infra-M, 2016, P. 188.

[7] L.A. Antipova, V.B. Yeremin, A.P. Borisov, “The concept of Internet of Things”, Modern problems and perspective directions of innovative development of a science: the collection of articles of the International scientifically - practical conference, vol. 8, Ufa: AETERNA, 2016, pp. 21-23.

[8] S.V. Guss, “Self-organizing mesh-networks for private use”, Mathematical structures and modeling, 2016, № 4(40), pp. 102-115.

[9] V. Vishnevskiy, “Mesh networks of the IEEE 802.11s standard: Routing protocols”, The first mile, 2009, №1, pp. 16-21.

[10] V. Vishnevskiy, “Mesh-network standard IEEE 802.11s - technology and implementation“, The first mile, 2008, №2-3, pp. 26-31.

[11] A.I. Kolybel'nikov, “Overview of wireless network technologies”, Proceedings of MIPT, 2012, vol.4, № 2, pp. 3-29.

[12] V.M. Vishnevskiy, “Simulation of wireless networks with decentralized control”, Automation and telemechanics, 1999, № 6, pp. 88–99.

[13] L.A. Antipova, A.P. Borisov, “A program for transferring data over a Wi-Fi channel using the mesh topology”, Certificate of state registration of the computer program, №2017662654, fr. 13.11.17.

[14] A.I. Lyakhov, A.A. Safonov, A.N. Yurgenson, “Algorithms for the multicast secure transfer task in wireless mesh networks”, Computing and network resources, 2011, № 3, pp. 53-63.

[15] L.A. Antipova, A.P. Borisov, “Application of the IEEE 801.11 standard for creating a mesh network and its use in the educational process for students”, Use of digital teaching aids and robotics in general and vocational education: experience, problems, prospects, Barnaul: Izd-vo Alt. Un-ta, 2017, pp. 10-13.

[16] L.A. Antipova, A.P. Borisov, “Investigation of the signal propagation range in the Wi-Fi network of the Mesh topology”, Measurement, control, informatization: materials of the XVIII International Scientific and Technical Conference, Barnaul: AltGTU, 2017, pp. 6-9.

[17] A.Y. Mizgirev, A.P. Borisov, “Creation of a device for simulation of data encryption in WI-FI networks”, Traditional and innovative science: history, current state, perspectives: a collection of articles of the International Scientific and Practical Conference, vol. 3, Ufa: AETERNA, 2016, pp. 84-86.

[18] A.A. Pavlov, I.O. Dat'yev, “Routing protocols in wireless networks”, Proceedings of the Kola Science Center of the Russian Academy of Sciences, 2014, № 5(24), pp. 64-75.

[19] S. Pakhomov, “Network Packet Analyzers”, ComputerPress, 2006, №4, pp. 17-19.

[20] M.I. Mel'nikov, A.S. Kovtun, “Self-organizing network of operational interaction for the needs of the population and special services”, Reports of Tomsk State University of Control Systems and Radioelectronics, 2014, № 2(32), pp. 281-286.

[21] M. Hussein, A. Yakunin, L. Suchkova, “A Comparison of Data Compression Methods for Solving Problems of Temperature Monitoring”, VII Scientific Conference with International Participation “Information-Measuring Equipment and Technologies”, IME&T 2016, Tomsk, Russia, May 25-28, 2016, MATEC Web of Conferences, vol. 79, DOI: 10.1051/matecconf/20167901076.

[22] A.G. Yakunin, H.M. Hussein, “Hardware-software and algorithmic provision of multipoint systems for long-term monitoring of dynamic processes”, IOP Publishing IOP Conf. Series: Journal of Physics: Conf. Series 881, 2017, 012028, DOI: 10.1088/1742-6596/881/1/012028.

978-1-7281-1931-1/19/$31.00 ©2019 IEEE