EMJ MS
EUROPEAN MULTIDISCIPLINARY JOURNAL OF MODERN SCIENCE
https://emjms.academicjournal.io/index.php/ Volume:5

Wireless Network Protocols as a Solution for WBAN

Nurshod Akhmedov, Khalimjon Khujamatov, Malika Kudratxonova
Data communication networks and systems department Tashkent University of Information Technologies named after Muhammad al-Khwarizmi Tashkent, Uzbekistan

Jaxongir Aripov
First Deputy General Director of Uzbektelecom JSC Tashkent, Uzbekistan

Abstract: The development of sensor technologies and IoT opens up opportunities for the development of industries, including healthcare. Wireless body area networks are the backbone of smart health, which are designed to collect data from wearable sensors and transmit it to receiving nodes. Wireless body area networks place stringent demands on data transmission technologies. In this article, we conducted a comparative analysis of technologies such as Wi-Fi, Z-wave, ZigBee and Bluetooth to determine the optimal technology for transmitting data in wireless body area networks.

Keywords: Body area network, Wi-Fi, ZigBee, Z-wave, Bluetooth.

I. Introduction (*Heading 1*)

Nowadays very difficult for anyone to go long without digital devices. Today, even our body is becoming digital, allowing us to control the parameters and indicators of the body, wherever we are: in the car, office or on a walk. Since for the implementation of such projects, the bodies are equipped with sensors, and they, in turn, are combined into a network, we need a universal way with which all sensors and wearable devices will “communicate” with each other and with us. Unfortunately, there is no such “universal language” today. Instead, we see several competing and virtually incompatible wireless standards for wireless body area networks (WBAN). Each of them is fighting for the title of the main technology of WBAN. These standards include not only well-known Wi-Fi and Bluetooth, but also specialized protocols - Z-Wave and ZigBee. All of them have advantages and disadvantages that are not obvious at first glance. But the choice of the standard around which the entire wearable network will be built must be made even before you decide on the use of wearable sensors.

II. Wi-Fi as a sollution for WBAN

A. Advantages of Wi-Fi

Wi-Fi is a powerful and reliable wireless solution that has been successfully used to build local area networks for many years. 802.11 has become the de facto global communications standard because it offers many flexible features and is continually enhanced by the Institute of Electrical and Electronics Engineers (IEEE) [1].

Designed to quickly exchange significant amounts of data over short distances, Wi-Fi does its job well. Basic parameters, such as coverage range or data rate, differ between different 802.11 options. But in most cases, a regular home wireless router is sufficient to provide network coverage for a small apartment. In larger buildings, you can increase the number of access points or signal repeaters to increase coverage [2].

Wi-Fi can easily transfer high definition video streams, and its theoretical bandwidth limit is

much higher than the average user needs. Some older versions of the 802.11 standard are limited to 11 Mbps or 54 Mbps, but the now widely used 802.11n is capable of transmitting tens and hundreds of megabits per second, and the newer 802.11ac is even more. These numbers certainly look great compared to other popular home automation solutions [3]. Their bandwidth values are expressed in Kbps, not Mbps.

In addition, one of the main benefits of Wi-Fi is the ubiquity of 802.11 infrastructure as given in figure 1. The fact that this standard is being integrated into new laptops, smartphones and tablets is of great importance in terms of implementing smart home and Internet of Things control applications.

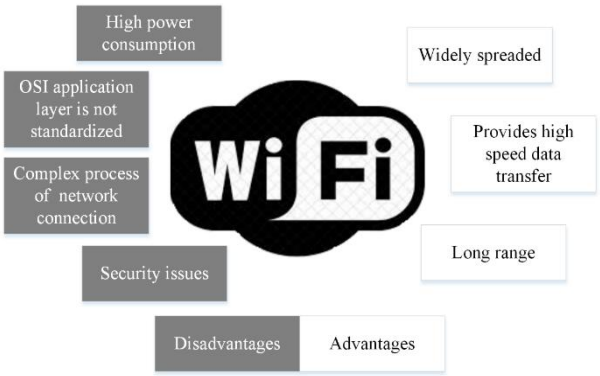

Fig. 1. Wi-Fi advantages and disadvantages.

B. Disadvantages of Wi-Fi

The benefits listed above are well known. Thanks to them, Wi-Fi has entered our everyday life and has become an everyday technology for wireless Internet access. But when it comes to home automation, high speed Internet access and the ability to quickly transfer huge amounts of information are not parameters that you will pay any attention to. Moreover, the capabilities of Wi-Fi in this regard are excessive for the vast majority of smart software solutions for home or office automation. These solutions work in an environment where typical devices transmit simple control commands (such as “on / off”), state change signals, or minuscule amounts of data (such as measurements from a sensor) [4].

Excess bandwidth itself is not a problem, but maintaining it comes with significant power consumption. As a high-speed wireless standard, Wi-Fi is a waste of power for the Internet of Things. Obviously, power consumption doesn't matter much if any device is connected to a permanent power source - a regular electrical outlet, lamp holder, etc. But it becomes a huge problem for those solutions that need to operate from autonomous power supplies without wires. It's almost impossible to build a responsive Wi-Fi device that is battery-powered or battery-powered that can last long enough. For example, it makes no sense to create an autonomous sensor for motion, smoke, door open / close based on Wi-Fi: its battery will be quickly discharged. In other words, despite the widespread and impressive data transfer rates and, Wi-Fi simply cannot effectively support the most important component of the world of smart homes - autonomous wireless sensors and actuators. And without them, home automation loses its practical meaning [5].

Another major limitation arises from the topology of the Wi-Fi network. The dependence of all traffic on the central router has a serious drawback: as soon as the router fails, the individual nodes on the network stop communicating with each other. This leads to the failure of the entire automation network [6]. Of course, you can expect a Wi-Fi router to be stable most of the time. Often it does. But as soon as it "freezes" or breaks down, huge problems immediately arise: the entire smart home will stop working. Do not forget that

replacing a failed wireless router will most likely require rebuilding and configuring the network from scratch.

Wi-Fi can be found in every new smartphone or laptop, which in theory makes them candidates for smart home controllers. However, in the case of Wi-Fi, this potential cannot be fully realized. Although a smartphone and a Wi-Fi smart home device use the same "communication language," this communication is not direct. It is always done through a central network access point. This is why Wi-Fi devices cannot use some important functions, such as detecting nearby devices [7].

Considering that virtually every consumer has a Wi-Fi enabled smartphone, it can be assumed that adding new smart devices to a Wi-Fi network will be a breeze. Unfortunately, this is not so. Before adding a smart home device to a Wi-Fi network, you need to tell it the network password. It's easy to do if you want to connect your laptop or smartphone. But the task becomes more difficult if your device has neither a keyboard nor a screen. Is it possible to entrust this work to a smartphone, because it also "speaks" the Wi-Fi language? Why not use it to tell the device a password? Not a bad idea, but the problem is that your smart device needs to be connected to the network first. And that brings us back to where we started. Manufacturers use a variety of techniques to make the customization process more manageable. But each such method has certain disadvantages and introduces additional complexity for users. In most cases, to add smart devices to a Wi-Fi network, you need to install a special mobile application or desktop utility, then put each added device into pairing mode, enter the Wi-Fi password through the application, and then add the device to the home automation system. Some vendors have gone as far as adding microUSB ports to their smart Wi-Fi devices solely for initial connection and setup purposes. While this solves the installation problem, you will hardly enjoy using the USB ports to add smart smoke or motion detectors installed in tight spaces to your network [8].

Compatibility is the most important issue in home automation. What does Wi-Fi offer in this regard? Unfortunately, not much. The Wi-Fi standard does not define the application layer of the OSI network model. This means that if device manufacturers have not agreed that their products will interact with each other, then machine-to-machine communication between such devices is almost impossible. Oftentimes, Wi-Fi technologists mistakenly attribute full interoperability just because it enables communication between users [9]. However, such a connection is possible only because people intervene in the process of interaction. For example, setting up a Skype connection is what you might call adding a conditional application layer to Wi-Fi. Smart devices cannot cope with this task on their own precisely for the reason that Wi-Fi itself does not provide any compatibility in the world of connected devices [10].

It should be noted that the Wi-Fi Alliance is aware of the shortcomings of Wi-Fi and is making efforts to address them. In 2016, a new standard was introduced - IEEE 802.11ah. He promised to free Wi-Fi from many of the limitations that 802.11 technologies face in the resource-demanding smart home and Internet of Things market. Some analysts were cautiously optimistic about 802.11ah, but the market as a whole was skeptical about the prospects of the new standard. For example, research company ABI Research predicts that by 2020 only 11 million 802.11ah chipsets will be shipped. For the IoT market, this is a drop in the ocean.

Why is the market so pessimistic about the 802.11ah standard? There are several reasons. Yes, it eliminates some of the serious flaws of previous 802.11 standards by extending coverage and adding lower power consumption to devices. But some of the problems remained unresolved - compatibility between individual devices; a router as a single point of

failure for the entire network; complex process of adding smart devices to the network; and the lack of additional security features such as key management [11]. In addition, being a completely new radio standard, it is incompatible with all wireless routers already found in millions of households and offices around the world. In other words, one of the biggest benefits of Wi-Fi is disappearing.

Thus, Wi-Fi should almost never be seen as the foundation of a smart home. The exception is those rare cases where only a reliable connection to the cloud is required, and you do not plan to implement smart devices based on other standards [12].

III. Zee-wave as a sollution for WBAN

Z-Wave covers all layers of the OSI network model, from physical to application. This guarantees a high level of compatibility between home automation equipment from different suppliers. Z-Wave is a well-debugged protocol focused on the exchange of short commands and messages between devices, which minimizes the congestion of the radio channel and reduces the likelihood of data loss.

Z-Wave uses the concept of a mesh network topology. The protocol is designed in such a way that the nodes of the network acting as relayers have the ability to forward a message through themselves until it reaches the addressee. This approach not only significantly expands the range of the wireless network, but also increases its reliability. In case of movement / deactivation / failure of any node, the network will not be paralyzed, but will continue to work as usual: messages will start automatically being sent through the relaying network nodes, bypassing the failed one [13].

Each Z-Wave logical network can support up to 232 devices. If you need to connect more devices, it is possible to combine networks. Several Z-Wave networks can easily coexist on the same territory without interfering with each other. This is achieved by minimizing the size of the transmitted packet and the mandatory requirement for the minimum load on the radio channel, which obliges the device to be in the transmission state no more than 1% of the time [14]. However, the nodes of different networks cannot “see” each other and, accordingly, cannot communicate with each other in any way. Communication between networks is carried out through devices that act as network bridges [15].

Devices on the same network can exchange information with each other, even when they are out of line of sight. In this case, the device uses intermediate nodes (other devices on the same network, except those that are powered by batteries and operate in a "sleep" mode most of the time to save battery power) to transmit information to another device when it is out of range the first device. The optimal and alternative available routes that can be used to transfer a message between two devices through intermediate nodes are predetermined [16].

Each Z-Wave network has a main controller (from which, in fact, the construction of the network begins), which is entrusted with the duties of adding new devices to the network and removing old ones, drawing up routing maps, ensuring secure connection, providing the ability to create automation scripts and other functions on the organization and control of the network. The network can also contain one or more secondary controllers, which for normal operation request information about the network topology from the primary controller. Usually the main controller is the one from which the network construction began. But over time, this function can be transferred to one of the secondary controllers. Often new Z-Wave devices can be added to the network using a QR code or pin code. This fast and secure procedure occurs once during the installation of a new device, after which the device is considered to belong to this network.

A distinctive feature of the Z-Wave ecosystem from the very beginning was that it

purposefully developed as a closed proprietary protocol protected by numerous patents of the management company (first - Zensys, then - Sigma Designs, now - Silicon Labs). All available protocol functions are implemented in the program code of the technology owner and are delivered to equipment manufacturers in a compiled form after signing a license agreement.

On the one hand, the closed nature of the technology is a disadvantage, since without knowledge of proprietary specifications, third-party developers cannot, at their discretion, use the protocol to develop software for controlling Z-Wave devices. This made it harder for Z-Wave to enter the corporate market. However, the owners of smart homes from such "closeness" were in big gain. The Z-Wave brand is the only one on the home automation market that can guarantee backward compatibility of used devices regardless of manufacturer, price, functional tasks, chip generations, specific device, etc.

Gradually, starting in 2012, wishing to make life easier for developers and expand the boundaries of its protocol, Sigma Designs opened part of the Z-Wave specification. But to maintain device backward compatibility, it continued to control manufacturers through stringent certification requirements.

The lower layers (physical and channel) of the Z-Wave protocol became open back in 2012 and since then are described by the International Telecommunication Union ITU-T G.9959 standard. They are directly responsible for wireless data transmission, describing in detail the frequencies used, coding and addressing methods [17].

In 2016, Sigma Designs released the official specification of the Z-Wave protocol to the public. In particular, command classes (describing how each individual command is formed and how to interpret a data packet) and device classes (describing the specification of existing devices and how these devices, depending on their type, perceive different commands) have been published. A description of the latest encryption specifications in Z-Wave, called Security 2 (S2), has been published. In addition, a description of Z / IP (Z-Wave over IP), a software add-on for transmitting Z-Wave packets over TCP / IP, has been published. This made it much easier to develop third-party web applications for Z-Wave.

The network and transport layers still remain closed, which provide unprecedented industry stability for large Z-Wave networks and are responsible, among other things, for routing messages in the smart home network, relaying them and acknowledging receipt.

A. Advantages of Z-Wave

Developers of Z-Wave were many years ahead of their time, and the mesh topology has long had unique functionality that gives this protocol a significant competitive advantage as given in figure 2. Now only Z-Wave does not have a mesh topology. But mesh networks have not lost their relevance, remaining to this day the optimal solution for home automation. Unlike many competitors, Z-Wave has been around for many years, and the developers have polished the message routing process to perfection. Of all the home automation solutions on the market, Z-Wave devices are arguably the most energy efficient, reliable, secure, and economical in terms of airtime.

In order to neutralize transmission delays and not overload the network, it is allowed to use up to 4 intermediate nodes for transit data transmission. Taking into account the fact that the range in the line of sight of modern Z-Wave modules is about 40 meters (and the new generation of Z-Wave devices on 700 series chipsets increases this value to 100 m), the final signal transmission range in one network Z-Wave is sufficient for most large home automation projects.

A huge unique advantage of Z-Wave technology is the ability to almost instantly self-medicate the network when a node stops responding. This is achieved through the use of the Explorer Frame procedure, which starts automatically. It takes no more than a second to determine all possible "working" routes and, accordingly, restore the Z-Wave network to work. Moreover, with the advent of the Explorer Frame procedure in the Z-Wave network, it became possible to fully use portable devices, the performance of which in older implementations was severely limited.

Another feature that improves the resiliency and performance of a Z-Wave network is associations between devices. Thanks to this function, one device can send a command to a nearby device, bypassing the central controller. For example, a siren can be triggered by a motion sensor instantly, without waiting for a command from the controller. After completing the action, the device will send an execution report to the controller. This not only speeds up the actuation of actuators, but also increases the reliability of critical network nodes. For example, a “sensor-actuator” link will work even if the controller is out of order. Yes, the user will no longer receive notifications from the controller about device triggers. But thanks to the associations, these devices themselves will continue to work together. To do this, they must be located close to each other, i.e. no routing is required to pass the command. In addition, they must be able to work together (eg leakage sensor and automatic ball valve).

Another advantage of Z-Wave is security. Here it is implemented at the highest level. Z-Wave technology uses the same encryption technologies as online banking systems. A new security standard known as Security 2 (or S2) became mandatory for certification of all Z-Wave smart devices after April 2, 2017. It improves encryption standards for exchanging data between nodes, and also sets new procedures for connecting new devices to the smart home network using PIN codes or QR codes that are unique for each device. A new layer of authentication protection ensures that hackers cannot take control of devices while they are connected to the network. S2 is the most advanced security system available on the home automation market. The tremendous attention that Z-Wave developers have paid to improving security has already borne fruit - over the past couple of years, Z-Wave has significantly strengthened its position in the smart security systems market, becoming, for example, the undisputed leader for such an indicative segment as smart door locks [18].

Fig.2. Z-Wave advantages and disadvantages.

Z-Wave operates in the unlicensed portion of the 800-900 MHz band dedicated to short-range devices. A distinctive feature of these frequencies is the ability to confidently overcome various obstacles, including floors and walls. After all, as you know, the longer the wavelength, the better it overcomes obstacles [19]. This is largely the reason for the impressive range of Z-Wave devices for the home automation market (while they are also the most energy efficient). This part of the range is also characterized by a small amount of interference from other devices operating at the same frequencies. Considering that other

competing home automation technologies are forced to huddle in the ultra-popular 2.4 GHz band, which is used by a huge number of devices around the world, even as far from wireless communications as conventional microwave ovens, there is practically no interference in the Z-Wave operating range (and as a result - low latency), becomes another competitive advantage of this home automation protocol.

B. Disadvantages of Z-Wave

There are not many bottlenecks left to Z-Wave worthy of mention: over the years, the technology has managed to fine-tune it. Perhaps one of the disadvantages stems from the advantage: this is the frequency range. The choice of the low-frequency, stable and most free range for short-range devices, and not the more popular and loaded (2.4 GHz), turned out to be a forward-looking and correct decision that saved Z-Wave smart home users from serious problems with interference in heavily loaded Wi-Fi frequencies -Fi ". But everything has a price. Historically, different countries have allocated different frequencies for small-action devices. For example, for all of Europe (CEPT countries), as well as China and a number of other Asian countries, this is 868.42 MHz. But in the USA and Mexico, these frequencies are occupied by GSM technology, therefore Z-Wave solutions there operate at 908.42 MHz. Russia, which signed the CEPT agreement, but never ratified it, went its own way and chose an operating range of 869.0 MHz for Z-Wave. What does this mean from the point of view of the average user? You need to be very careful when buying a new product in another country and connecting it to your home automation network. For example, a device designed for the US market will not be compatible with devices in the “Russian” range. Therefore, for use in Russia, it is best to buy Z-Wave devices in trusted Russian stores.

In addition, as we noted earlier, Z-Wave has developed as a closed technology for a long time. This allowed the developers to guarantee excellent compatibility, security, fault tolerance, and so on. But this "closed" is more expensive in device development. Therefore, Z-Wave solutions cannot be called the most budgetary option for a smart home. Another thing is that the ratio of price / quality, where the Z-Wave technology left competitors almost no chance.

IV. ZigBee as a sollution for WBAN

The ZigBee protocol suite defines only the upper layers of the OSI model - network, transport, and application. It is built on top of the IEEE 802.15.4 standard, which defines the lower layers of a wireless network targeting end-devices (rather than users like Wi-Fi), and is characterized by low power consumption and low data rates. The IEEE 802.15.4 standard is supported by several chip vendors and is used not only for ZigBee, but several dozen other protocols as well. This standard defines the unlicensed frequencies of 2.4 GHz (worldwide), 915 MHz (for America and Australia) and 868 MHz (for Europe) as the operating range. The maximum data rate is 250 kbps in the 2.4 GHz band, 40 kbps in the 915 MHz band and only 20 kbps in the 868 MHz band. Therefore, almost all ZigBee devices only operate on the 2.4 GHz frequency [20].

Unlike Z-Wave, which uses source routing to deliver packets to individual nodes on the network, ZigBee uses destination routing. Thus, three classes of devices are involved in the implementation of the ZigBee mesh network: a coordinator (the “brain” of the network, which forms it and coordinates its work), a router (constantly active, therefore it must be connected to a constant power system; responsible for connecting and maintaining up to 32 end devices, so their location needs to be optimized, and the number must be sufficient to serve all devices on the network; also a key element in broadcasting and dynamic routing of packets in the network) and end devices (they are in sleep mode most of the time to save

power batteries, can receive and send packets, but do not participate in their retransmission) [21]. Thus, ZigBee offers a slightly different approach to organizing a mesh network from a technical point of view, but, like in the case of Z-Wave, it is able to provide a self-healing network and can quickly reroute data packets to ensure their delivery, if any node is down or not responding as given in figure 3.

A. Advantages of ZigBee

ZigBee is a mature home automation technology. At the moment, the Zigbee Alliance has hundreds of members, and there are thousands of different solutions on the market with declared Zigbee support. High market penetration is definitely the technology's strength, as users have a choice.

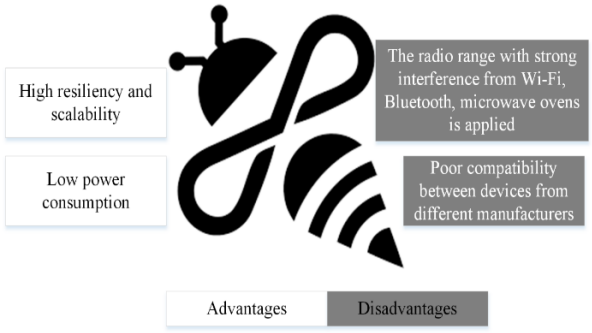

Fig. 3 ZigBee advantages and disadvantages.

ZigBee is an open wireless communication standard that primarily looks attractive from the point of view of developers and manufacturers. This allows them to be more flexible in choosing the functionality they need, as well as to bring new products to market at a lower cost. So, for example, thanks to this, ZigBee had some success in the corporate market. In particular, some cable TV networks and telecommunications companies have used ZigBee in their set-top boxes and satellite transceivers, and utilities have added support for this protocol to smart electricity and water meters to improve the ability to monitor, control and manage service consumption for their users.

The main trump card of Zigbee is its focus on budget consumers. This is greatly facilitated not only by the openness of the standard, but by the Zigbee Alliance's soft approach to certification of new products, allowing manufacturers to use only the functionality they need in their solutions. Thus, the Zigbee network is a relatively cheap way to implement wireless home automation.

As we already noted, power consumption can be attributed to the strengths of solutions with support for Zigbee. Despite the fact that the achievements of Zigbee in this aspect are not as impressive as those of the main competitors (Z-Wave and even Bluetooth), individual Zigbee devices can last up to 2 years without having to replace the battery. Overall, this is a good indicator for today's home automation market [22].

ZigBee has good scalability. Capable of supporting up to 65,000 nodes, this standard can theoretically provide huge coverage despite the relatively small range of individual modules (10-20 meters indoors). True, these figures should be treated with a grain of salt. For example, networks with a four-digit number of nodes face significant challenges in maintaining uptime even in a lab environment. Communication delays tend to occur even for much smaller deployments (only a few hundred devices). This is not surprising, given the fact that ZigBee operates in a supercharged 2.4 MHz band, and the maximum data transfer rate is 250 Kbps.

B. Disadvantages of ZigBee

ZigBee does not cope well with cases where there is strong interference from other devices in the network coverage area. ZigBee combined with a protocol such as Wi-Fi or Bluetooth cannot always effectively deal with interference found in the dense 2.4 GHz frequency band. The workload of the 2.4 GHz band is growing every year, which can only worsen the situation in the near future. The IEEE 802.15.4 standard states that one of the advantages of ZigBee is that it is under the control of the IEEE, which defines the physical layer of the ZigBee protocol stack, limiting the data rate to 250Kbps. Therefore, in order to meet the needs of the market, the ZigBee Alliance must enter into lengthy negotiations with the IEEE. Since the IEEE pursues its own goals, the outcome of these negotiations is unpredictable. Organizations like the Z-Wave Alliance are in a much better position as they have complete control over their practices. The Z-Wave Alliance defines each layer of the OSI model. Therefore, all decisions regarding any aspect of communication are in the hands of one organization.

ZigBee offers a wide range of measures to ensure adequate communication between smart devices in security matters. With three keys used to manage security and 128-bit AES used to encrypt and authenticate data, end users don't have to worry, but that's only at first glance. However, in some cases, there have been news about security issues found on ZigBee-enabled devices. An example is the Black Hat conference in the US in 2015, which talked about how Cognosec ZigBee products can exploit some vulnerabilities and mainly focused on insecure key pair generation when a new device is connected to the network.

The ZigBee Alliance has made a statement that the Hask method described in the Cognes report is known and applies to any ZigBee system that uses public key exchange when connecting to a network. So what is this date? why is this vulnerability still not fixed if it exists for a long time? Quite simply, some security issues in ZigBee networks have nothing to do with the protocol itself. In its report, Sognoses acknowledges that the features provided by the ZigBee standard can be considered very advanced and robust, despite the potential for exploiting ZigBee vulnerabilities. However, the Zigbee Alliance does not require device manufacturers to follow all the specifications, and instead they are given the freedom to choose the mechanisms needed to make specific decisions. As a result, vendors often introduce the minimum security features required for certification, and such "pruned" programs often leave the entire network vulnerable.

Despite the aforementioned shortcomings, ZigBee is still an effective technology. Theoretically, ZigBee should do a great job with many home automation tasks, as well as a key role in the smart home. But often ZigBee devices from different manufacturers do not fit together [23].

ZigBee has a leading position in the global Internet market due to its very loose certification policy, which makes it interested in supporting its devices. In order to facilitate the integration of ZigBee products with manufacturers and create a basis for interoperability between different solutions from different vendors, the ZigBee Alliance has created a set of standardized specifications (profiles), such as a home automation profile, a remote control profile or a Light link profile, communication schemes between smart devices belonging to to a specific product category.

The Zigbee Alliance Certification Program ensures that a particular product conforms to the relevant profile and that devices with the same profile can communicate with each other, even if they are from different vendors. But device manufacturers are given the freedom to choose, and they themselves choose how and when they will use the developed profiles in their

products. Large enterprises and manufacturers immediately enjoy this freedom and create their own patents. This is why interactions in the ZigBee ecosystem no longer look like a well-coordinated mechanism, but rather a lot of incompatible profile changes with the wild west world and the vast majority of incompatible ZigBee products.

When it comes to large brands, for example, if you choose two ZigBee lines from different manufacturers in a store, they will not be able to directly interact with each other. Large companies always create their own Zigbee solutions and they can interoperate with other devices under the same product brand. There are whole isolated ZigBee ecosystems of various brands such as Philips Hue, Xiaomi, and the combination of controllers of the same brand with sensors and other actuators directly out of the box does not work. For example, in order for the Xiaomi smart Home Controller to be able to control Philips Hue lamps, you will need to buy a more expensive Philips controller. Controllers communicate with each other via an IP-based API, but not with other goods.

If you take Zigbee as the basis for smart home automation, you will have to independently check the compatibility of all selected solutions from different brands. The failed certification program of the ZigBee Alliance consortium, unfortunately, cannot provide any guarantee of compliance.

The main disadvantage of ZigBee is poor communication, and this cancels out some of the advantages of this technology.

V. Bluetooth as a sollution for WBAN

Bluetooth covers all layers of the basic OSI model, from the application layer like Z-Wave to the physical layer. Generally speaking, Bluetooth's development and licensing oversight body, the Bluetooth Special Interest Group (SIG), has the same unique privilege as the Z-Wave Alliance. It is a privilege to make changes to the standard directly and independently as given in figure 4.

Bluetooth low energy, like other low frequency and low power communication standards, is designed for data transmission with short active battery life and small packets. Therefore, the main difference from the classic Bluetooth we use is that Bluetooth low energy devices connect to each other only when they need to send or receive data.

At the application level, interaction between solutions from different manufacturers is ensured by defining profiles (specifications for the operation of low-power devices and specific applications). This principle was borrowed from the original specification of classic Bluetooth. In this way, manufacturers can embed the profiles they need into their devices, ensuring it is compatible with other Bluetooth Smart products that support the same specification. We also note that the ability to implant several profiles into solutions allows manufacturers to flexibly adjust the functionality of their products. However, solutions from different manufacturers will be able to fully communicate only if they have at least one common profile.

A. Advantages of Bluetooth

For a technology focused on low energy consumption, Bluetooth Low Energy has a rather impressive data transfer rate - up to 1 Mbps (for the new fifth version of Bluetooth, this value has been increased to 2 Mbps). The faster the speed, the more information can be transmitted per unit of time. This means that the Bluetooth transmitter will quickly release the radio air, thereby reducing the likelihood of collisions. This is extremely important when operating in an overloaded frequency band such as 2.4 GHz [24].

With support for sleeping nodes (devices that spend most of the time inactive, periodically

"wake up" for a short time just to quickly complete their task, and then also quickly return to sleep) Bluetooth Smart provides a decent, although not the best in the industry value battery life, allowing certain sensors and switches to operate for over a year on tiny coin batteries. With regard to such a critically important parameter for the home automation market as device response time, here again Bluetooth BLE demonstrates results at the level of leading technologies [25].

Plus, Bluetooth Smart has an interesting feature that the other technologies we've reviewed don't have. These are the so-called beacons. Using Bluetooth proximity detection, beacons can force smartphones to perform certain actions when the user is near them. Beacons enable you to implement a wide range of unique applications, from location-based push notifications to precise positioning services. Most importantly, adding a few lines of code to the software stack is all it takes to equip a Bluetooth-enabled smart device with beacon functionality.

The biggest advantage of Bluetooth is its features based on the ability to determine the proximity of Bluetooth devices, as well as the fact that a smart device and a smartphone can directly communicate with each other. Of all the wireless technologies used in the IoT, almost all smartphones, tablets and laptops on the market only support Bluetooth and Wi-Fi. But besides being incompatible with most internet apps, Wi-Fi handles all communications through a central hotspot, and Bluetooth provides a direct connection between phone and device. For users, this is a huge benefit. Because the smart home network of smart devices only needs special software to make the gadget "remote display", and this topology makes it much easier to add new devices to the existing network. With иluetooth, the whole procedure is intuitive and safe and can be very simple [26].

B. Disadvantages of Bluetooth

Bluetooth uses the same 2.4GHz band as most other radio technologies. Using the 2.4 GHz band in Windows, which has built-in Bluetooth anti-interference controls, is a definite disadvantage. True, in addition to constant noise, the 2.4 GHz band has another big drawback, which is that when radio waves pass through walls and other obstacles, through the human body, the signal at this frequency is lost much faster than at frequencies below 1 GHz [27].

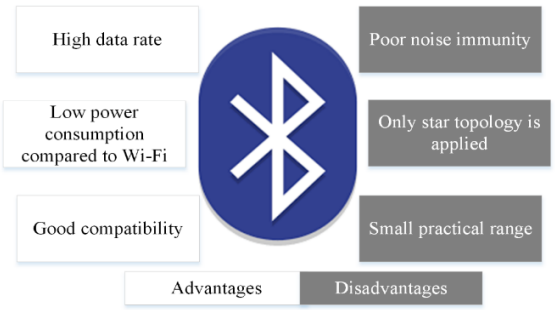

Fig 4. Bluetooth low energy advantages and disadvantages.

Therefore, the range of Bluetooth low energy technologies is not its advantage. Despite the "distance up to 100 meters", which theoretically can be achieved with Bluetooth 4 [28]. If the two devices are closed, you can calculate the distance up to 10 meters. The confusion also arises due to the fact that this number depends not only on the obstacles and obstacles that will be in the signal propagation path, but also on the manufacturer's settings, since with Bluetooth Smart they have the ability to adjust the device's signal level within certain limits, increasing the power and increasing power consumption [29].

The reason why Bluetooth is Smart, specifically designed to address the challenges of the rapidly growing Internet market, is almost never seen as an option for building complex Internet applications as well as complex home automation networks. Designed to support simple star networks in relation to business. This is not about offices or industrial plants, but rather about creating a dynamic, flexible and reliable touch-controlled environment that we want to see in our smart homes. The mesh network is an important topology for many applications, such as those that require extended range or peer-to-peer communication between devices, and so it's not surprising that all of the most popular protocols in the low-bandwidth Z-Wave and ZigBee categories route messages over networks [30-31].

Conclusion

Recently, a lot of multi-protocol controllers have appeared on the market, combining several wireless smart home technologies at once. So manufacturers are trying to reconcile competing protocols and give users more freedom to build smart home networks. The most popular combination is to support Z-Wave, Zigbee and Bluetooth Smart simultaneously in one device. They, for example, can be found in the popular controllers VeraPlus, Vera Secure, a number of Zipato controllers, Smart Things and some other manufacturers.

In general, a universal controller is a good solution to the problem of the “zoo” of smart home protocols. But the catch is that by ensuring that different wireless technologies work together within a single smart home, such controllers do not solve the problem of incompatibility between devices within the framework of the same protocol. It is important to remember this when choosing “periphery” - sensors and actuators, without which no smart home is possible in principle.

As we have already found out, one of the main reasons for poor intra-protocol compatibility is the lack of standardization at the application layer of the OSI network model. And not declared, but real standardization. And it depends primarily on how rigidly the industry groups behind a particular protocol determine the conditions for certification of finished devices.

Today the undisputed leader in the compatibility of devices from different manufacturers within the same protocol is Z-Wave technology. The industry consortium Z-Wave Alliance offers a clear certification program for smart home gadgets and closely monitors the implementation of its conditions. Z-Wave covers all layers of the OSI model. But unlike, for example, Bluetooth Smart (which also supports all these layers), the Z-Wave protocol was originally developed as a highly resilient mesh technology. In addition, Z-Wave is the only popular technology that does not use the overloaded 2.4 GHz frequency range. All these advantages allowed the Z-Wave Alliance to create, without exaggeration, the world's most developed ecosystem of smart home devices (more than 100 million implementations and over 2.5 thousand product names from more than 700 international manufacturers).

Zigbee and Bluetooth Smart also have chances for development. In the first case, the developers try to solve the problem of inter-protocol compatibility by implementing the Dotdot add-on. But given the huge installed base of legacy Zigbee devices and the soft certification policy of the Zigbee Alliance, one can hardly hope for a quick breakthrough in terms of smooth operation of Zigbee gadgets from different manufacturers. In addition, the Thread protocol is considered a potential competitor to Zigbee, which, however, still remains a “dark horse” in the smart home market.

In the case of Bluetooth Low Energy, the prospects for this protocol largely depend on how successful attempts to implement mesh network topology become in it. One way or another, both Bluetooth, Zigbee and Thread are tightly tied to the noisy 2.4 GHz radio band. And this

shortcoming is unlikely to be eliminated in the foreseeable future.

The wireless smart home market is changing rapidly. Only the requirements for power consumption of devices, digital security, network resiliency, the ability of devices to withstand radio interference, ease of connection, and the mutual compatibility of products of the same communication standard remain unchanged. When choosing the basis for a smart home, you need to carefully weigh all these factors.

References

1. I.Kh Siddikov., Kh.A. Sattarov., Kh.E. Khujamatov. Research of the Influence of Nonlinear Primary Magnetization Curves of Magnetic Circuits of Electromagnetic Transducers of the Three-phases Current // Universal Journal of Electrical and Electronic Engineering. Horizon Research Publishing Corporation, USA. 2016, Vol.4(1), pp. 29 – 32. DOI: 10.13189/ujeee.2016.040104
2. I.Kh. Siddikov., Kh.A. Sattarov., Kh.E. Khujamatov., O.R. Dekhkonov. Modeling the processes in magnetic circuits of electromagnetic transdusers // International Conference on Information Science and Communications Technologies ICISCT 2016, 2nd, 3rd and 4th of November 2016, Tashkent, Uzbekistan. (Scopus) DOI: 10.1109/ICISCT.2016.7777393
3. I.Kh. Siddikov., Kh.A. Sattarov., Kh.E. Khujamatov. Modeling of the Transformation Elements of Power Sources Control // 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.2017.8188581
4. Siddikov I.Kh. Sattarov Kh.A. Khujamatov Kh.E. Dexkhonov O.R. Agzamova M.R. Modeling of Magnet Circuits of Electromagnetic Transducers of the Three-Phases Current//2018 XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE-2018), October 2-6, 2018, Novosibirsk. –p.p. 419-422 (Scopus) DOI: 10.1109/APEIE.2018.8545714
5. I.Kh Siddikov., Kh.A. Sattarov., Kh.E. Khujamatov. Modeling and research circuits of intelligent sensors and measurement systems with distributed parameters and values// “Chemical technology control and management” International scientific and technical journal, Tashkent 4-5/2018/ pp. 50-55. https://doi.org/10.34920/2018.4-5.50-54
6. Muradova A.A. Khujamatov Kh.E. Results of Calculations of Parameters of Reliability of Restored Devices of the Multiservice Communication Network // International Conference on Information Science and Communications Technologies ICISCT 2019, Tashkent, Uzbekistan - 2019. (Scopus) DOI: 10.1109/ICISCT47635.2019.9011932
7. Khujamatov Kh.E. Khasanov D.T., Reypnazarov E.N. Modeling and Research of Automatic Sun Tracking System on the bases of IoT and Arduino UNO // International Conference on Information Science and Communications Technologies ICISCT 2019, Tashkent, Uzbekistan - 2019. (Scopus) DOI: 10.1109/ICISCT47635.2019.9011913
8. Khujamatov Kh.E. Khasanov D.T., Reypnazarov E.N. Research and Modelling Adaptive Management of Hybrid Power Supply Systems for Object Telecommunications based on IoT // International Conference on Information Science and Communications Technologies ICISCT 2019, Tashkent, Uzbekistan - 2019. (Scopus) DOI: 10.1109/ICISCT47635.2019.9011831

9. Khalim Khujamatov, Khaleel Ahmad, Ernazar Reypnazarov, Doston Khasanov. Markov Chain Based Modeling Bandwith States of the Wireless Sensor Networks of Monitoring System//International Journal of Advanced Science and Technology, Vol. 29, No.4, (2020), pp. 4889 – 4903. (Scopus) http://sersc.org/journals/index.php/IJAST/article/view/24920
10. I.Kh.Siddikov., Kh.E.Khujamatov., D.T.Khasanov., E.R.Reypnazarov. Modeling of monitoring systems of solar power stations for telecommunication facilities based on wireless nets// "Chemical technology. Control and management" International scientific and technical journal, 2020, №3 (93) pp.20-28. https://uzjournals.edu.uz/ijctcm/vol2020/iss3/4
11. Halim Khujamatov, Reypnazarov Ernazar, Hasanov Doston, Nurullaev Elaman, Sobirov Shahzod. Evaluation of characteristics of wireless sensor networks with analytical modeling // Bulletin of TUIT: Management and Communication Technologies Bulletin of TUIT: Management and Communication Technologies, Volume 3, December 2020. https://uzjournals.edu.uz/tuitmct/vol4/iss1/4
12. Kh. Khujamatov, D. Khasanov, E. Reypnazarov, N. Akhmedov. Networking and Computing in Internet of Things and Cyber-Physical Systems // The 14th IEEE International Conference Application of Information and Communication Technologies, 07-09 October 2020, Tashkent, Uzbekistan (Scopus). DOI: 10.1109/AICT50176.2020.9368793
13. Sobiya Arsheen, Abdul Wahid, Khaleel Ahmad, Kh. Khujamatov. Flying Ad hoc Network Expedited by DTN Scenario: Reliable and Cost-effective MAC Protocols Perspective // The 14th IEEE International Conference Application of Information and Communication Technologies, 07-09 October 2020, Tashkent, Uzbekistan (Scopus). DOI: 10.1109/AICT50176.2020.9368575
14. Halim Khujamatov, Ernazar Reypnazarov, Nurshod Akhmedov, Doston Khasanov. Blockchain for 5G Healthcare architecture // 2020 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan – 2020. (Scopus). DOI: 10.1109/ICISCT50599.2020.9351398
15. Halim Khujamatov, Ernazar Reypnazarov, Nurshod Akhmedov, Doston Khasanov. IoT based Centralized Double Stage Education // 2020 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan – 2020. (Scopus) DOI: 10.1109/ICISCT50599.2020.9351410
16. Halim Khujamatov, Ernazar Reypnazarov, Nurshod Akhmedov, Doston Khasanov. Industry Digitalization Consepts with 5G-based IoT // 2020 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan – 2020. (Scopus) DOI: 10.1109/ICISCT50599.2020.9351468
17. Halim Khujamatov, Temur Toshtemirov. Wireless sensor networks based Agriculture 4.0: challenges and apportions // 2020 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan – 2020. (Scopus) DOI: 10.1109/ICISCT50599.2020.9351411
18. Ilkhom Siddikov, Khalim Khujamatov, Doston Khasanov, Ernazar Reypnazarov. IoT and Intelligent Wireless Sensor Network for Remote Monitoring Systems of Solar Power Stations // 11th World Conference "Intelligent System for Industrial Automation" (WCIS-2020). (Scopus) https://doi.org/10.1007/978-3-030-68004-6_24

19. Afsar Kamal, Khaleel Ahmad, Rosilah Hassan, Khujamatov Khalim. NTRU Algorithm: Nth Degree Truncated Polynomial Ring Units // Functional Encryption (Springer book chapter), (Scopus) https://doi.org/10.1007/978-3-030-60890-3_6
20. Khalim Khujamatov, Doston Khasanov, Ernazar Reypnazarov, Nurshod Akhmedov. IoT, IIoT, and Cyber-Physical Systems Integration // Emergence of Cyber Physical System and IoT in Smart Automation and Robotics (Springer book chapter). https://doi.org/10.1007/978-3-030-66222-6_3
21. Khalimjon Khujamatov, Doston Khasanov, Ernazar Reypnazarov, Nurshod Akhmedov. Existing Technologies and Solutions in 5G-Enabled IoT for Industrial Automation // Blockchain for 5G-Enabled IoT Robotics (Springer book chapter). https://doi.org/10.1007/978-3-030-67490-8_8 (accepted)
22. Khujamatov Khalimjon Ergashevich, Khasanov Doston Turayevich, Fayzullaev Bayram Artikbayevich, Reypnazarov Ernazar Nurjamiyevich. WSN-BASED RESEARCH THE MONITORING SYSTEMS FOR THE SOLAR POWER STATIONS OF TELECOMMUNICATION OBJECTS // IIUM Engineering Journal, Vol. 22, No. 2, 2021. https://doi.org/10.31436/iiumej.v22i2.1464
23. Khairol Amali Bin Ahmad, Halim Khujamatov, Nurshod Akhmedov, Mohd Yazid Bajuri, Mohammad Nazir Ahmad, Ali Ahmadian, Emerging trends and evolutions for smart city healthcare systems, Sustainable Cities and Society, Volume 80, 2022, 103695, ISSN 2210-6707, ttps://doi.org/10.1016/j.scs.2022.103695.
24. 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 Jan 26;5:131.
25. Ilkhom Siddikov, Doston Khasanov, Halim Khujamatov, Ernazar Reypnazarov. Communication Architecture of Solar Energy Monitoring Systems for Telecommunication Objects // 2021 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan – 2021. (Scopus)
26. Khalimjon Khujamatov, Amir Lazarev, Nurshod Akhmedov. Intelligent iot Sensors: Types, Functions and Classification // 2021 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan – 2021. (Scopus)
27. Ilkhom Siddikov, Khalim Khujamatov, Ernazar Reypnazarov, Doston Khasanov. CRN and 5G based IoT: Applications, Challenges and Opportunities // 2021 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan – 2021. (Scopus)
28. Halim Khujamatov, Ilkhom Siddikov, Ernazar Reypnazar. Research of Probability-Time Characteristics of the Wireless Sensor Networks for Remote Monitoring Systems // 2021 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan – 2021. (Scopus)
29. Nurshod Akhmedov, Halim Khujamatov, Amir Lazarev, Madiyar Seidullayev. Application of LPWAN technologies for the implementation of iot projects in the Republic of Uzbekistan // 2021 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan – 2021. (Scopus)

30. Akhmedov Nurshod, Khalim Khujamatov, Amir Lazarev. Remote monitoring system architectures in healthcare // 2021 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan – 2021. (Scopus)
31. Khalimjon Khujamatov, Amir Lazarev Nurshod Akhmedov, Ernazar Reypnazarov, Aybek Bekturdiev. Methods for automatic identification of vehicles in the its system // 2021 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan – 2021. (Scopus)