Journal of Automation, Electronics and Electrical Engineering

COMPARATIVE ANALYSIS OF DATA TRANSMISSION TECHNOLOGIES IN INDUSTRIAL SYSTEMS OF THE INTERNET OF THINGS (IOT)

Zbigniew ŁUKASIK[1], **Anton USHAKOV**[2]

[1] Uniwersytet Technologiczno-Humanistyczny, Wydział Transportu, Elektrotechniki i Informatyki, Malczewskiego 29, 26-600 Radom, Polska, z.lukasik@uthrad.pl
[2] Uniwersytet Technologiczno-Humanistyczny, Wydział Transportu, Elektrotechniki i Informatyki, Malczewskiego 29, 26-600 Radom, Polska, a.ushakov@uthrad.pl

DOI: https://doi.org/10.24136/jaeee.2020.004

Abstract – This article provides a comparative analysis of modern data transmission technologies that can be used in modern automation and telemechanics systems for data exchange with various sensors and other security and access control systems. The authors describe the most common types of transmission networks and offer options for their application in relation to the requirements of specific customers. The main emphasis is on open source solutions that can be used in research projects on an unlicensed basis.

Key words – Internet of Things (IoT), Zigbee, WIFI, BLE, Ethernet

INTRODUCTION

IoT devices are becoming more and more common among ordinary users in households and in the small and medium-sized business environment. There are many prerequisites for this.

Among the main ones are the following:

• Significant reduction in the average cost of off-the-shelf hardware platforms. If back in the early 2010s, prices for IoT solutions even for households (i.e. without special requirements for reliability and durability of operation) started from several hundred US dollars, now due to the fact that new players from among large transnational companies such as IKEA, Philips, Xiaomi, etc., the cost of such ready-made solutions has decreased by an order of magnitude, i.e. up to tens of dollars.

• The emergence of a large number of chip makers from among relatively small fabless manufacturers (especially those originating from China). So, if back in the 2000s all small automation was carried out mainly on low-performance 8-bit solutions of the AVR and PIC platforms (for example, the Arduino platform), then the 2010s gave us many different solutions on completely different 32 and 64-bit hardware platforms. These are ESP8266 / ESP32 from Espressif Systems (based on Tensilica Xtensa chips), and Onion Omega 2+ from Onion (based on MIPS chips), and STM32 platform from STMicroelectronics, and many fabless chip developers on the ARM platform (Allwinner, Amlogic, Broadcom, Rockchip, etc.). At the beginning of 2020, solutions based on the completely open source RISC-V architecture began to appear in the open access, which, after the appearance of convenient SDKs for developers, will also be able to enter the competitive race. All of this has dramatically reduced prices and allowed developers to not really care about the cost of hardware and focus all their efforts on improving the software.

• The emergence of convenient and free tools for rapid development (SDK). Back in the 2000s, most powerful development tools (such as, for example, the IAR Embedded Workbench) were produced by large software companies only for the needs of enterprises and other large businesses and their cost was hundreds and thousands of US dollars. But in the 2010s, in the wake of the popularity of the Arduino platform with their ArduinoIDE, most of the major market players introduced free and often open source solutions for small businesses and households. Moreover, this was done by both major players in the hardware market (such as STMicroelectronics with their STM32CubeIDE) and third-party software developers (for example, PlatformIO). It has also drastically lowered the barriers to entry and has allowed many non-company enthusiast developers to be attracted to the IoT.

• Significant reduction in the cost of tariffs for data transmission in mobile networks. If earlier the developers of IoT solutions were limited only to Ethernet and WIFI networks within households or large industrial facilities, now, with the development of 4th generation LTE and NB-

IOT cellular networks and the introduction of eSIM electronic SIM cards, it has become possible for a relatively small fee (about 10 dollars per year) to equip each IoT device with its own dedicated channel to the Internet and at the same time not depend on the infrastructure of the household / enterprise, since the device will transmit and receive data wherever there is a signal from a cellular operator.

All of the above made it possible to attract a huge number of developers, system administrators and other enthusiasts to the creation and deployment of IoT networks. As a result, at the moment we have a huge number of different technologies that allow data transmission in IoT networks and therefore it is required to analyze the entire main range of existing hardware and software solutions, describe their advantages and disadvantages and determine the most beneficial areas for their application. This is what this article will be devoted to.

I. MQTT STANDART FOR SMART HOME IOT SYSTEMS

Before talking about the standards for transferring data to IoT networks, it is necessary to say a few words about in what logical form this data will be transferred. It is clear that each standard has its own unique means of transmission and coding, but if we do not have a unified format in which data is presented at the highest application layer, then we will not be able to process this data unified and therefore talk about some kind of a single IoT platform will be impossible. For this there is the Application layer protocol MQTT of the conceptual model «**Internet protocol suite**».

MQTT is an OASIS standard for IoT connectivity. It is a publish/subscribe, extremely simple and lightweight messaging protocol, designed for constrained devices and low-bandwidth, high-latency or unreliable networks. The design principles are to minimize network bandwidth and device resource requirements whilst also attempting to ensure reliability and some degree of assurance of delivery. These principles also turn out to make the protocol ideal of the “Internet of Things” world of connected devices, and for mobile applications where bandwidth and battery power are at a premium.[16]

MQTT was invented by Dr Andy Stanford-Clark of IBM, and Arlen Nipper of Arcom (now Eurotech), in 1999[5].

For the operation of the MQTT network, a broker is required. A broker is a server that routes published messages to subscribers.

Clients (subscribers) connect to the server and send data to it or receive data from it in the form of messages.

If you need to use multiple servers, then a bridge is required. Bridge is a connection between two MQTT brokers.

The most famous and widespread server is Mosquitto is an Open Source MQTT server. We will use it in our research.

In order to view or publish messages to us from a personal computer, we need a client program. In this case, we will use software MQTT.fx.

An example of the operation of this program is shown in Figure 1.

MQTT messages can be presented in a hierarchical manner.

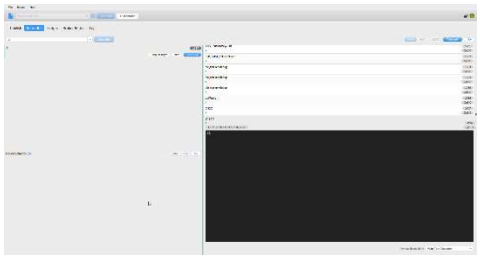

Fig.1. MQTT.fx program (author's photo)

For example, the message about the network status of our sensor module can be represented as follows:
{"uptime":909160,"version":"v0.9.5","freemem":39336,"rssi":25,"SSID":"CHEBNET_IOT","ip":"192.168.6.72","mac":"80:7D:3A:3E:85:7B","wifiprt":0,"modules":"IRHADiscovery"}

And the message about the status of the sensors connected to it can be presented in the following form
{"battery":69,"illuminance":45,"illuminance_lux":367,"linkquality":68,"pressure":998,"soil_moisture":98,"temperature_ds":23.5,"voltage":2900}

If we have devices in the network that need to be controlled (for example, switches), then we can give them a signal to turn on / off and receive a status response, i.e. have a feedback system.

All of the above makes MQTT a very flexible protocol that we can adapt to the needs of a particular customer.

II. RS485

One of the oldest ways to connect peripherals to computers is various serial communication standards. The most common standard for industrial automation devices today is the RS485 standard. It is used by industrial networks Modbus, Profibus DP, ARCNET, BitBus, WorldFip, LON, Interbus and many non-standard networks. This is due to the fact that according to all the main indicators, this interface is the best of all possible at the current level of technology development.

Its main advantages are:

- two-way data exchange using just one twisted pair of wires;
- work with several transceivers connected to the same line, that is, the ability to organize a network;
- long communication line length;
- sufficiently high transmission speed.

Fig.2 RS-485 – USB converter (author's photo)

The maximum line length of the RS485 interface depends on the set network baud rate. So, the maximum length of the communication line (1200 m) is possible at low transmission rates (less than 100 kbps).

At the same time, the implementation of this interface for their devices is available even for beginners. There is a huge number of ready-made hardware solutions (Fig. 2) and already written software libraries for working with this interface.

One of the broadest uses of this standard is as an extension cable when connecting a transmitter-receiver of low-speed radio links (for example, LoRa) located on the roof of buildings and digital signal processors located in the user's home / office. As we know, high frequency antenna cables are very susceptible to interference (especially in urban environments). It is therefore very important to locate the transmitter / receiver as close to the antenna as possible. And the receiver itself and the digital signal processor can be easily connected with just a two-core cable at a distance of up to 1200 meters.

The main disadvantages of this interface are its low data transfer rate (compared to modern network standards) and the need for wires (compared to wireless standards).

III. ETHERNET

Another of the oldest and most widely accepted wired connection standards is Ethernet. Ethernet is a family of computer networking technologies commonly used in local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN). It was commercially introduced in 1980 and first standardized in 1983 as IEEE 802.3. Ethernet has since been refined to support higher bit rates, a greater number of nodes, and longer link distances, but retains much backward compatibility. [12]

It makes no sense to describe in detail what Ethernet is in such a short article, so we just note that this standard, which uses twisted pair for data transmission, is cheap to implement, provides high speeds (up to 2.5 Gbps) and a sufficient transmission distance without repeaters (by 100 meters of 24-gauge unshielded twisted-pair cable and 150 meters or longer with high quality cabling).

For a long time, the main problem with the implementation of Ethernet for industrial automation was the need to place additional wires to power end devices, since early standards did not describe the possibility of powering devices directly over twisted pair.

Power over Ethernet, or PoE, describes any of several standards or ad hoc systems that pass electric power along with data on twisted pair Ethernet cabling. This allows a single cable to provide both data connection and electric power to devices such as Wireless Access Points (WAPs), Internet Protocol (IP) cameras, and Voice over Internet Protocol (VoIP) phones.[19]

There are several common techniques for transmitting power over Ethernet cabling. Three of them have been standardized by Institute of Electrical and Electronics Engineers (IEEE) standard IEEE 802.3 since 2003. These standards are known as alternative A, alternative B, and 4PPoE. For 10BASE-T and 100BASE-TX, only two of the four signal pairs in typical Cat 5 cable are used. Alternative B separates the data and the power conductors, making troubleshooting easier. It also makes full use of all four twisted pairs in a typical Cat 5 cable. The positive voltage runs along pins 4 and 5, and the negative along pins 7 and 8.

Alternative A transports power on the same wires as data for 10 and 100 Mbit/s Ethernet variants. This is similar to the phantom power technique commonly used for powering condenser microphones. Power is transmitted on the data conductors by applying a common voltage to each pair. Because twisted-pair Ethernet uses differential signaling, this does not interfere with data transmission. The common-mode voltage is easily extracted using the center tap of the standard Ethernet pulse transformer. For Gigabit Ethernet and faster, both alternatives A and B transport power on wire pairs also used for data since all four pairs are used for data transmission at these speeds.

4PPoE provides power using all four pairs of a twisted-pair cable. This enables higher power for applications like Pan–Tilt–Zoom (PTZ) cameras, high-performance WAPs, or even charging laptop batteries.

In addition to standardizing existing practice for spare-pair (Alternative B), common-mode data pair power (Alternative A) and 4-pair transmission (4PPoE), the IEEE PoE standards provide for signaling between the power sourcing equipment (PSE) and powered device (PD). This signaling allows the presence of a conformant device to be detected by the power source, and allows the device and source to negotiate the amount of power required or available.

The original IEEE 802.3af-2003 PoE standard provides up to 15.4 W of DC power (minimum 44 V DC and 350 mA) on each port. Only 12.95 W is assured to be available at the powered device as some power dissipates in the cable. The updated IEEE 802.3at-2009 PoE standard also known as PoE+ or PoE plus, provides up to 25.5 W of power for Type 2 devices. The 2009 standard prohibits a powered device from using all four pairs for power. Both of these standards have since been incorporated into the IEEE 802.3-2012 publication.

The IEEE 802.3bu-2016 amendment introduced single-pair Power over Data Lines (PoDL) for the single-pair Ethernet standards 100BASE-T1 and 1000BASE-T1 intended for automotive and industrial applications. On the two-pair or four-pair standards power is transmitted only between pairs, so that within each pair there is no voltage present other than that representing the transmitted data. With single-pair Ethernet, power is transmitted in parallel to the data. PoDL defines 10 power classes, ranging from .5 to 50 W (at PD).

IV. RF

Ultra high frequency (UHF) is the ITU designation for radio frequencies in the range between 300 megahertz (MHz) and 3 gigahertz (GHz), also known as the decimetre band as the wavelengths range from one meter to one tenth of a meter (one decimeter). Radio waves with frequencies above the UHF band fall into the super-high frequency (SHF) or microwave frequency range. Lower frequency signals fall into the VHF (very high frequency) or lower bands. UHF radio waves propagate mainly by line of sight; they are blocked by hills and large buildings although the transmission through building walls is strong enough for indoor reception.

Fig.3 General scheme of the author's radio system (author's photo)

They are used for television broadcasting, cell phones, satellite communication including GPS, personal radio services including Wi-Fi and Bluetooth, walkie-talkies, cordless phones, and numerous other applications.

430–440 MHz: Amateur radio (70 cm band)

863–868 MHz: Used for licence-exempt wireless systems.

An example of such systems is the 868Mhz radio transmission system from Anton Ushakov's doctoral dissertation (Fig.3), which will collect data on the status of each container from the module (Fig.4) with sensors installed on it.

Then this system will transfer them by radio to an intermediate server-computer station, the only one on a rolling stock, where this data will be logged onto a flash memory carrier.

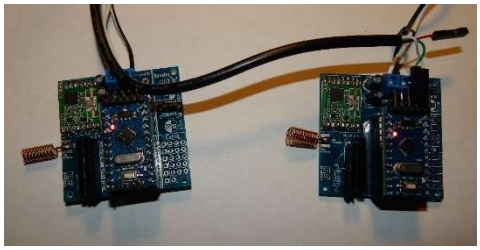

Fig.4 Modules of the author's radio system (author's photo)

The advantage of RF is the relative cheapness of the components, the unlicensed basis and the difficulty for hacking. The main disadvantage of this technology is the lack of ready-made standards and the need to develop our own data exchange protocols.

V. LoRa

LoRa (Long Range) is a low-power wide-area network (LPWAN) protocol developed by Semtech. It is based on spread spectrum modulation techniques derived from chirp spread spectrum (CSS) technology. It was developed by Cycleo of Grenoble, France and acquired by Semtech, the founding member of the LoRa Alliance.

LoRa uses license-free sub-gigahertz radio frequency bands like 433 MHz, 868 MHz (Europe), 915 MHz (Australia and North America), 865 MHz to 867 MHz (India) and 923 MHz (Asia). LoRa enables long-range transmissions (more than 10 km in rural areas) with low power consumption. The technology covers the physical layer, while other technologies and protocols such as LoRaWAN (Long Range Wide Area Network) cover the upper layers. It can achieve data rate from 0.3 kbps to 27 kbps depending upon the spreading factor.[4]

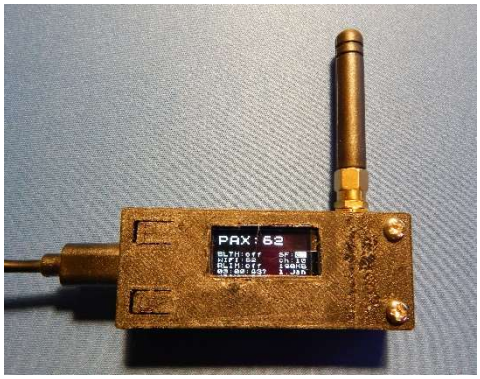

Fig.5 LoRa module (author's photo)

Since LoRa defines the lower physical layer, the upper networking layers were lacking. LoRaWAN is one of several protocols that were developed to define the upper layers of the network. LoRaWAN is a cloud-based medium access control (MAC) layer protocol but acts mainly as a network layer protocol for managing communication between LPWAN gateways and end-node devices as a routing protocol, maintained by the LoRa Alliance.[11]

LoRaWAN defines the communication protocol and system architecture for the network, while the LoRa physical layer enables the long-range communication link. [18]

LoRaWAN is also responsible for managing the communication frequencies, data rate, and power for all devices. Devices in the network are asynchronous and transmit when they have data available to send. Data transmitted by an end-node device is received by multiple gateways, which forward the data packets to a centralized network server. The network server filters duplicate

packets, performs security checks, and manages the network. Data is then forwarded to application servers. The technology shows high reliability for the moderate load, however, it has some performance issues related to sending acknowledgements. [10]

An example of a LoRaWAN module counting the number of users of wireless devices in nearby premises can be seen in Figure 5.

VI. Z-WAVE

Z-Wave is a wireless communications protocol used primarily for home automation. It is a mesh network using low-energy radio waves to communicate from appliance to appliance, allowing for wireless control of residential appliances and other devices, such as lighting control, security systems, thermostats, windows, locks, swimming pools and garage door openers. Like other protocols and systems aimed at the home and office automation market, a Z-Wave system can be controlled via the Internet from a smart phone, tablet or computer, and locally through a smart speaker, wireless keyfob, or wall-mounted panel with a Z-Wave gateway or central control device serving as both the hub controller and portal to the outside. Z-Wave provides the application layer interoperability between home control systems of different manufacturers that are a part of its alliance.[15]

Fig.6 Z-wave network receiver-transmitter (author's photo)

Z-Wave is designed to provide reliable, low-latency transmission of small data packets at data rates up to 100kbit/s. The throughput is 40kbit/s (9.6kbit/s using old chips) and suitable for control and sensor applications, unlike Wi-Fi and other IEEE 802.11-based wireless LAN systems that are designed primarily for high data rates. Communication distance between two nodes is about 30 meters (40 meters with 500 series chip), and with message ability to hop up to four times between nodes, it gives enough coverage for most residential houses. Modulation is frequency-shift keying (FSK) with Manchester encoding.[17]

Z-Wave uses the Part 15 unlicensed industrial, scientific, and medical (ISM) band. It operates at 868.42 MHz in Europe, at 908.42 MHz in North America and uses other frequencies in other countries depending on their regulations. This band competes with some cordless telephones and other consumer electronics devices, but avoids interference with Wi-Fi, Bluetooth and other systems that operate on the crowded 2.4 GHz band. The lower layers, MAC and PHY, are described by ITU-T G.9959 and fully backwards compatible. In 2012, the International Telecommunication Union (ITU) included the Z-Wave PHY and MAC layers as an option in its G.9959 standard for wireless devices under 1 GHz. Data rates include 9600 bps and 40 kbps, with output power at 1 mW or 0 dBm. The Z-Wave transceiver chips are supplied by Silicon Labs.

Fig.7 Z-wave to MQTT system interface (author's photo)

For smart home wireless networking, there are numerous technologies competing to become the standard of choice. Wi-Fi consumes a lot of power, and Bluetooth is limited in signal range and number of devices. Other network standards competing with Z-Wave include Wi-Fi HaLow, Bluetooth 5, Insteon, Thread and ZigBee. Z-Wave has a long open-air operating range at 90 meter (outdoor) and 24+ meter(indoor). Insteon can theoretically address a large number of devices at 17.7 million (compared to ZigBee's 65,000 and Z-Wave's 232).

There are a large number of ready-made transceivers (Fig.6) on sale that connect to the USB port and work with a computer as part of the serial port emulation.

There are also open source systems that allow you to receive and transmit data in the Z-Wave using the MQTT protocol. One of the most famous is the system Z-Wave2MQTT (Fig.7).

VII. WIFI

Wi-Fi is a family of wireless network protocols, based on the IEEE 802.11 family of standards, which are commonly used for local area networking of devices and Internet access. Wi-Fi is a trademark of the non-profit Wi-Fi Alliance, which restricts the use of the term Wi-Fi Certified to products that successfully complete interoperability certification testing.

Wi-Fi uses multiple parts of the IEEE 802 protocol family and is designed to interwork seamlessly with its wired sibling Ethernet. Compatible devices can network through wireless access points to each other as well as to wired devices and the Internet. The different versions of Wi-Fi are specified by various IEEE 802.11 protocol standards, with the different radio technologies determining radio bands, and the maximum ranges, and speeds that may be achieved.

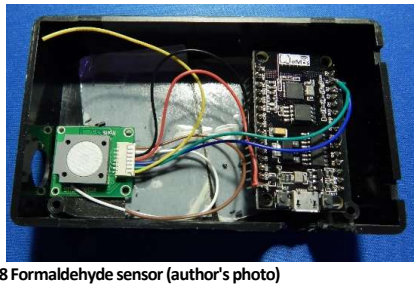

Fig.8 Formaldehyde sensor (author's photo)

Wi-Fi most commonly uses the 2.4 gigahertz (120 mm) UHF and 5 gigahertz (60 mm) SHF ISM radio bands; these bands are subdivided into multiple channels. Channels can be shared between networks but only one transmitter can locally transmit on a channel at any moment in time.[14]

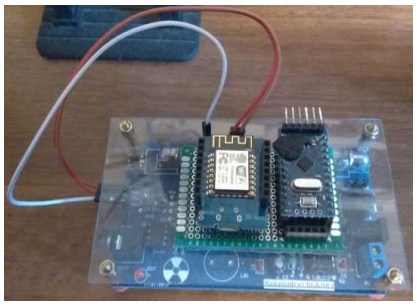

Fig.9 Radiation sensor (author's photo)

Wi-Fi's wavebands have relatively high absorption and work best for line-of-sight use. Many common obstructions such as walls, pillars, home appliances, etc. may greatly reduce range, but this also helps minimize interference between different networks in crowded environments.

An access point (or hotspot) often has a range of about 20 meters (66 feet) indoors while some modern access points claim up to a 150-metre (490-foot) range outdoors. Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometers using many overlapping access points with roaming permitted between them. Over time the speed and spectral efficiency of Wi-Fi have increased. As of 2020, at close range, some versions of Wi-Fi, running on suitable hardware, can achieve speeds of over 1 Gbit/s (gigabit per second).[8]

An example of such WIFI systems the author's system uses the widespread WIFI and Ethernet protocols for data transfer.

In consist of several components of the Internet of Things system, namely:

- A central server running under the Linux operating system with one of the widely used "Smart Home" open systems in the world;
- Modules of environmental sensors that use WIFI or ZigBee networks to transmit to the server the necessary environmental parameters inside and outside the wagon (temperature, atmospheric pressure, humidity, amount of particulate matter (PM10, PM2.5) and hazardous gases (formaldehyde, carbon monoxide, excess carbon dioxide);
- State sensors that track movements inside and outside the container platform (motion and presence sensors), possible drops and movement of the load (vibration sensors), as well as container opening sensors (reed sensors).

Each sensor (Fig. 8,9) in system is a separate module that can operate both autonomously and as part of a common Smart Wagon system.

This allows to make the modular system in order to increase fault tolerance and flexibly adapt to the needs of specific customers.

VIII. BLUETOOTH LOW ENERGY (BLE)

Bluetooth Low Energy (Bluetooth LE, colloquially BLE, formerly marketed as Bluetooth Smart) is a wireless personal area network technology designed and marketed by the Bluetooth Special Interest Group (Bluetooth SIG) aimed at novel applications in the healthcare, fitness, beacons, security, and home entertainment industries. It is independent of Bluetooth BR/EDR and has no compatibility, but BR/EDR and LE can coexist. The original specification was developed by Nokia in 2006 under the name Wibree, which was integrated into Bluetooth 4.0 in December 2009 as Bluetooth Low Energy.

Bluetooth Low Energy technology operates in the same spectrum range (the 2.400–2.4835 GHz ISM band) as classic Bluetooth technology, but uses a different set of channels. Instead of the classic Bluetooth seventy-nine 1-MHz channels, Bluetooth Low Energy has forty 2-MHz channels. Within a channel, data is transmitted using Gaussian frequency shift modulation, similar to classic Bluetooth's Basic Rate scheme. The bit rate is 1 Mbit/s (with an option of 2 Mbit/s in Bluetooth 5), and the maximum transmit power is 10 mW (100 mW in Bluetooth 5). [2]

BLE devices are detected through a procedure based on broadcasting advertising packets. This is done using 3 separate channels (frequencies), in order to reduce interference. The advertising device sends a packet on at least one of these three channels, with a repetition period called the advertising interval. For reducing the chance of multiple consecutive collisions, a random delay of up to 10 milliseconds is added to each advertising interval. The scanner listens to the channel for a duration called the scan window, which is periodically repeated every scan interval.

The discovery latency is therefore determined by a probabilistic process and depends on the three parameters (viz., the advertising interval, the scan interval and the scan window). The discovery scheme of BLE adopts a periodic-interval based technique, for which upper bounds on the discovery latency can be inferred for most parametrizations. While the discovery latencies of BLE can be approximated by models for purely periodic interval-based protocols, the random delay added to each advertising interval and the three-channel discovery can cause deviations from these predictions, or potentially lead to unbounded latencies for certain parametrizations.

Fig.10 BLE temperature and humidity sensor

The main advantage of BLE sensors is their low cost. So, the most popular BLE temperature and humidity sensor (Fig.10), ready-made, costs less than $ 3 piece, which allows them to be widely used to control temperature conditions in rooms.

The main disadvantage is the small size of the coating (up to 20 meters), which requires the mandatory presence in the system of BLE-Wifi gateways.

IX. ZIGBEE

Zigbee is an IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create personal area networks with small, low-power digital radios, such as for home automation, medical device data collection, and other low-power low-bandwidth needs, designed for small scale projects which need wireless connection. Hence, Zigbee is a low-power, low data rate, and close proximity (i.e., personal area) wireless ad hoc network.[9]

The technology defined by the Zigbee specification is intended to be simpler and less expensive than other wireless personal area networks (WPANs), such as Bluetooth or more general wireless networking such as Wi-Fi. Applications include wireless light switches, home energy monitors, traffic management systems, and other consumer and industrial equipment that requires short-range low-rate wireless data transfer.

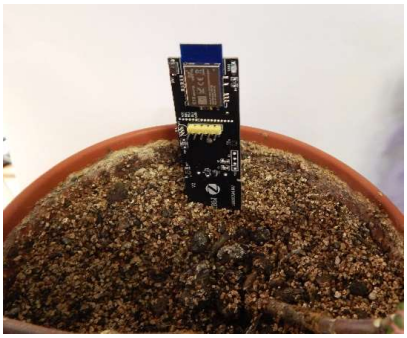

Fig.11 Zigbee Soil moisture sensor (author's photo)

Its low power consumption limits transmission distances to 10–100 meters line-of-sight, depending on power output and environmental characteristics. Zigbee devices can transmit data over long distances by passing data through a mesh network of intermediate devices to reach more distant ones. Zigbee is typically used in low data rate applications that require long battery life and secure networking (Zigbee networks are secured by 128bit symmetric encryption keys.) Zigbee has a defined rate of 250 kbit/s, best suited for intermittent data transmissions from a sensor or input device.[13]

Zigbee was conceived in 1998, standardized in 2003, and revised in 2006. The name refers to the waggle dance of honey bees after their return to the beehive.

There are three classes of Zigbee devices:

Zigbee coordinator (ZC) (Fig.13): The most capable device, the coordinator forms the root of the network tree and may bridge to other networks. There is precisely one Zigbee coordinator in each network since it is the device that started the network originally (the Zigbee LightLink specification also allows operation without a Zigbee coordinator, making it more usable for off-the-shelf home products). It stores information about the network, including acting as the trust center and repository for security keys.

Fig.12 Zigbee2MQTT interface (author's photo)

Zigbee router (ZR): As well as running an application function, a router can act as an intermediate router, passing data on from other devices.

Zigbee end device (ZED): Contains just enough functionality to talk to the parent node (either the coordinator or a router); it cannot relay data from other devices. This relationship allows the node to be asleep a significant amount of the time thereby giving long battery life. A ZED requires the least amount of memory and thus can be less expensive to manufacture than a ZR or ZC.

The current Zigbee protocols support beacon-enabled and non-beacon-enabled networks. In non-beacon-enabled networks, an unslotted CSMA/CA channel access mechanism is used. In this type of network, Zigbee routers typically have their receivers continuously active, requiring additional power. However, this allows for heterogeneous networks in which some devices receive continuously while others transmit when necessary. The typical example of a heterogeneous network is a wireless light switch: The Zigbee node at the lamp may constantly receive since it is reliably powered by the mains supply to the lamp, while a battery-powered light switch would remain asleep until the switch is thrown. In which case, the switch wakes up, sends a command to the lamp, receives an acknowledgment, and returns to sleep.

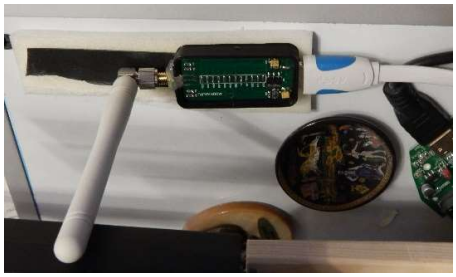

Fig.13 CC2538 Zigbee coordinator (author's photo

Fig.14 Zigbee relay module (author's photo)

In such a network the lamp node will be at least a Zigbee router, if not the Zigbee coordinator; the switch node is typically a Zigbee end device. In beacon-enabled networks, Zigbee routers transmit periodic beacons to confirm their presence to other network nodes. Nodes may sleep between beacons, thus extending their battery life. Beacon intervals depend on data rate; they may range from 15.36 milliseconds to 251.65824 seconds at 250 kbit/s, from 24 milliseconds to 393.216 seconds at 40 kbit/s and from 48 milliseconds to 786.432 seconds at 20 kbit/s. Long beacon intervals require precise timing, which can be expensive to implement in low-cost products.

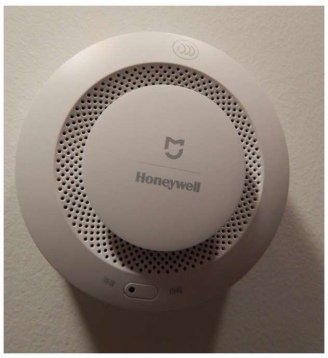

Fig.15 Zigbee smoke detector (author's photo)

In general, the Zigbee protocols minimize the time the radio is on, so as to reduce power use. In beaconing networks, nodes only need to be active while a beacon is being transmitted. In non-beacon-enabled networks, power consumption is decidedly asymmetrical: Some devices are always active while others spend most of their time sleeping.

The main advantage of the Zigbee is its wide distribution among enthusiasts.

There are a large number of open source projects that allow you to connect both branded and self-soldered Zigbee sensors to smart home systems using the MQTT protocol.

Soil moisture sensors (Fig.11) and a relay module (Fig.14) can be cited as examples of s self-soldered Zigbee module by the authors.

Also, on sale there is a huge number of ready-made Zigbee modules (Fig.15) from world-famous manufacturers of security systems.

The most popular system for communicating Zigbee devices via the MQTT protocol is Zigbee2MQTT. (Fig.12)

X. NARROWBAND IOT AND LTE

Long-Term Evolution (LTE) is a standard for wireless broadband communication for mobile devices and data terminals, based on the GSM/EDGE and UMTS/HSPA technologies. It increases the capacity and speed using a different radio interface together with core network improvements. LTE is the upgrade path for carriers with both GSM/UMTS networks and CDMA2000 networks. The different LTE frequencies and bands used in different countries mean that only multi-band phones are able to use LTE in all countries where it is supported.[1]

The LTE specification provides downlink peak rates of 300 Mbit/s, uplink peak rates of 75 Mbit/s and QoS provisions permitting a transfer latency of less than 5 ms in the radio access network. LTE has the ability to manage fast-moving mobiles and supports multi-cast and broadcast streams. LTE supports scalable carrier bandwidths, from 1.4 MHz to 20 MHz and supports both frequency division duplexing (FDD) and time-division duplexing (TDD). The IP-based network architecture, called the Evolved Packet Core (EPC) designed to replace the GPRS Core Network, supports seamless handovers for both voice and data to cell towers with older network technology such as GSM, UMTS and CDMA2000. The simpler architecture results in lower operating costs (for example, each E-UTRA cell will support up to four times the data and voice capacity supported by HSPA).[3]

Narrowband Internet of Things (NB-IoT) is a Low Power Wide Area Network (LPWAN) radio technology standard developed by 3GPP to enable a wide range of cellular devices and services. The specification was frozen in 3GPP Release 13 (LTE Advanced Pro), in June 2016. Other 3GPP IoT technologies include eMTC (enhanced Machine-Type Communication) and EC-GSM-IoT. [6]

NB-IoT focuses specifically on indoor coverage, low cost, long battery life, and high connection density. NB-IoT uses a subset of the LTE standard, but limits the bandwidth to a single narrow-band of 200kHz. It uses OFDM modulation for downlink communication and SC-FDMA for uplink

communications. IoT applications which require more frequent communications will be better served by NB-IoT, which has no duty cycle limitations operating on the licensed spectrum. [7]

XI. Conclusion

As a conclusion, it should be noted that all of the above systems are currently widely used in industrial automation devices.

It is impossible to single out some kind of unconditional leader, since each of the technologies has its own special niche, where it is widely spread.

There is certainly healthy competition in this market, but it is mainly reflected in the confrontation of similar standards (NARROWBAND IOT vs LTE, Z-Wave vs ZigBee, BLE vs WIFI).

It is impossible to fully cover all the features and benefits of each technology within the framework of one small review article, so separate articles should be devoted to these issues.

For example, if we start comparing the most popular standards of the Internet of Things, then Z-Wave has better interoperability than ZigBee, but ZigBee has a faster data transmission rate. Zigbee operates on the busy Wi-Fi standard frequency of 2.4 GHz, while Z-Wave operates at 908 MHz in the US, which has reduced noise and a greater coverage area. The Z-Wave MAC/PHY is globally standardized by the International Telecommunications Union as ITU 9959 radio, and the Z-Wave Interoperability, Security (S2), Middleware and Z-Wave over IP specifications were all released into the public domain in 2016. Zigbee is much more common in the home automation segment and is supported by more manufacturers.

As we can see, the topic is very complex and multifaceted, so the authors will try to sanctify it in more detail in their future articles.

ANALIZA PORÓWNAWCZA TECHNOLOGII TRANSMISJI DANYCH W PRZEMYSŁOWYCH SYSTEMACH INTERNETU RZECZY (IOT)

W artykule dokonano analizy porównawczej nowoczesnych technologii transmisji danych, które mogą znaleźć zastosowanie w nowoczesnych systemach automatyki i telemechaniki do wymiany danych z różnymi czujnikami i innymi systemami bezpieczeństwa i kontroli dostępu. Autorzy opisują najczęściej spotykane typy sieci przesyłowych i proponują możliwości ich zastosowania w odniesieniu do wymagań konkretnych klientów. Główny nacisk kładzie się na rozwiązania open source, które mogą być wykorzystywane w projektach badawczych bez licencji.

Słowa kluczowe: Internet of Things (IoT), Zigbee, WIFI, BLE, Ethernet

BIBLIOGRAPHY

[1] "An Introduction to LTE". 3GPP LTE Encyclopedia. Retrieved 5 December 2020
[2] "Bluetooth Smart or Version 4.0+ of the Bluetooth specification". bluetooth.com. Retrieved 5 December 2020.
[3] "Long Term Evolution (LTE): A Technical Overview" (PDF). Motorola. Retrieved 5 December 2020
[4] "LoRaWAN Specification" (PDF). lora-alliance.org. Retrieved 5 December 2020.
[5] "MQTT FAQ". MQTT.org. Retrieved 2020-11-17. // https://mqtt.org/faq/
[6] "NarrowBand – Internet of Things (NB-IoT)". https://www.gsma.com/iot/narrow-band-internet-of-things-nb-iot/ // Retrieved 5 December 2020
[7] "Standardization of NB-IOT completed". 3gpp.org. 3GPP. June 22, 2016. p. 1. Retrieved 5 December 2020
[8] "Wi-Fi Alliance® introduces Wi-Fi 6". Wi-Fi Alliance. 3 October 2018. Retrieved 5 December 2020
[9] "ZigBee Specification FAQ". ZigBee.org. Zigbee Alliance. Archived from the original on June 27, 2013. Retrieved 5 December 2020.
[10] Adelantado, Ferran; Vilajosana, Xavier; Tuset-Peiro, Pere; Martinez, Borja; Melia-Segui, Joan; Watteyne, Thomas (2017). "Understanding the Limits of LoRaWAN". IEEE Communications Magazine. 55 (9): 34–40. doi:10.1109/mcom.2017.1600613. hdl:10609/93072. ISSN 0163-6804. S2CID 2798291.
[11] Bankov, D.; Khorov, E.; Lyakhov, A. (November 2016). "On the Limits of LoRaWAN Channel Access". 2016 International Conference on Engineering and Telecommunication (EnT): 10–14. doi:10.1109/ent.2016.011. ISBN 978-1-5090-4553-2. S2CID 44799707.
[12] Charles E. Spurgeon (2000). Ethernet: the definitive guide. OReilly Media. ISBN 978-1-56592-660-8.
[13] Gislason, Drew; "ZigBee Wireless Networking" EE Times Retrieved 5 December 2020.
[14] Lemstra, Wolter; Hayes, Vic; Groenewegen, John (2010). The Innovation Journey of Wi-Fi: The Road to Global Success. Cambridge University Press. p. 121. ISBN 978-0-521-19971-1.
[15] Lou Frenzel, "What's The Difference Between ZigBee And Z-Wave?" Electronic Design, March 29, 2012.
[16] MQTT 5.0 specification". OASIS. Retrieved 2020-11-17. // https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html
[17] Oliver Kaven, "Zensys' Z-Wave Technology," PC Magazine, January 8, 2005.
[18] Ramon Sanchez-Iborra; Jesus Sanchez-Gomez; Juan Ballesta-Viñas; Maria-Dolores Cano; Antonio F. Skarmeta (2018). "Performance Evaluation of LoRa Considering Scenario Conditions". Sensors. 18 (3): 772. doi:10.3390/s18030772. PMC 5876541. PMID 29510524.
[19] Urs von Burg (2001). The triumph of Ethernet: technological communities and the battle for the LAN standard. Stanford University Press. pp. 175–176, 255–256. ISBN 978-0-8047-4095-1.