BEEHIVE SECURITY SYSTEM AGAINST UNAUTHORIZED MANIPULATION

Martin Milota
Master Degree Programme (2nd year), FEEC BUT
E-mail: xmilot03@stud.feec.vutbr.cz

Supervised by: Petr Dejdar
E-mail: xdejda00@stud.feec.vutbr.cz

Abstract: The paper deals with the design of beehive security system against unauthorized manipulation. This system uses LoRaWAN wireless communication technology for data transmission. The device records the movement of the beehive using an accelerometer and then locates the beehive using a GPS module. This low-energy system works via a battery-powered ESP32 microcontroller and is located on a beehive.

Keywords: ESP32 microcontroller, GPS localization, Internet of Things, LoRaWAN network, LPWAN technologies, securing beehives

1 INTRODUCTION

Beekeeping is very widespread in the Czech Republic, and this is associated with a high rate of beehive theft. That is why sufficient hive security is a very important part of beekeeping. This is a security that uses modern wireless transmission technology in IoT. The introduction of the article explains the general issues of IoT and ESP32 microcontroller. For security design the article describes a suitable LoRaWAN transmission technology. The last chapter of the article is devoted to the final design of the security device and the test connection of part of the solution.

2 INTERNET OF THINGS

IoT (Internet of Things) can be defined as a network of physical objects that are interconnected, can communicate with each other, share and analyze data that provide a wealth of information for planning, decision making and management, which illustrates fig. 1. These physical objects are devices of various types and sizes such as vehicles, smartphones, toys, home appliances, industrial systems, medical instruments, buildings and more. IoT is not the only technology, but a combination of different hardware and software technologies. At present, we can already find many practical applications in many areas, such as security of property, agriculture, smart cities, houses and so on [1].

2.1 IoT TECHNOLOGIES

IoT applications have specific requirements, such as long range, low data rate, low power consumption and low cost. Frequently used technologies with short signals, such as ZigBee and Bluetooth, are not adapted to scenarios that require long-distance transmission and are therefore not suitable for such applications. Also, solutions that are based on mobile communication, such as 2G, 3G and 4G, provide a lot of coverage, but consume an excessive amount of device power. That is why these specific requirements of IoT applications have led to the emergence of new wireless communication technologies based on LPWAN (Low-Power Wide Area Network) [2].

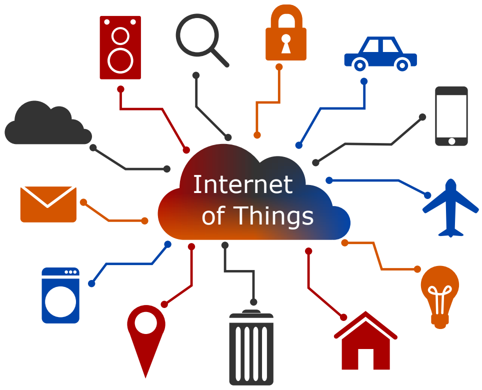

Figure 1: Internet of Things.

3 MICROCONTROLLER ESP32

There are currently many different microcontrollers available in the market for IoT solutions. Such microcontrollers include, for example, the best-known Arduino, but also Xbee or WhizFi. However, most of these microcontrollers have a high weight or high cost and very few of them are open soruce. And this is the advantage of the device from Espressif Systems, which offers the ESP32 microcontroller with integrated 2.4 GHz Wi-Fi, Bluetooth and BLE (Bluetooth Low Energy) technology. The ESP32 system is designed and optimized for the best performance and size, with many advanced low-power chip features for a variety of applications. It is mainly focused on mobile applications, small electronics and IoT applications [3], [4].

4 LORAWAN

The LoRaWAN network has been designed for IoT applications to connect thousands of devices, modules and sensors. It operates in the unlicensed ISM (Industrial, Scientific and Medical) communication band and consists of two different layers. The physical layer of the standard is formed by LoRa modulation and above it is the MAC layer, the operation of which is ensured by the open-source standard LoRaWAN [5], [6].

LoRaWAN networks are formed by a star topology. The basic elements of the network are the end devices that send data to the LoRaWAN gateways. Then, these gateways send the data to the application servers. The operation of such a network can be seen in fig. 2. The end devices communicate with the LoRaWAN gateways wirelessly using the LoRa physical layer. The gateways communicate with application servers via the Internet using 3G / 4G mobile networks, Ethernet or other similar transport communication technology. All measured data thus reaches directly into the data storage, to which the user has access via a dedicated API (Application Programming Interface) or an administrative console running on the application server [7].

5 SECURITY SYSTEM DESIGN

The LoRaWAN network will be used to transfer data from the device to the server, where the data will be further processed. A simplified block diagram of the resulting security system can be seen in fig. 3. It consists of a LOLIN32 ESP-WROOM-32 microcontroller, to which the LoRa module SX1276 is connected for communication via the SPI bus. Next, the GPS module GY-NEO6MV2 connected via the UART bus, which is used to locate the beehive, and the module with the accelerometer and

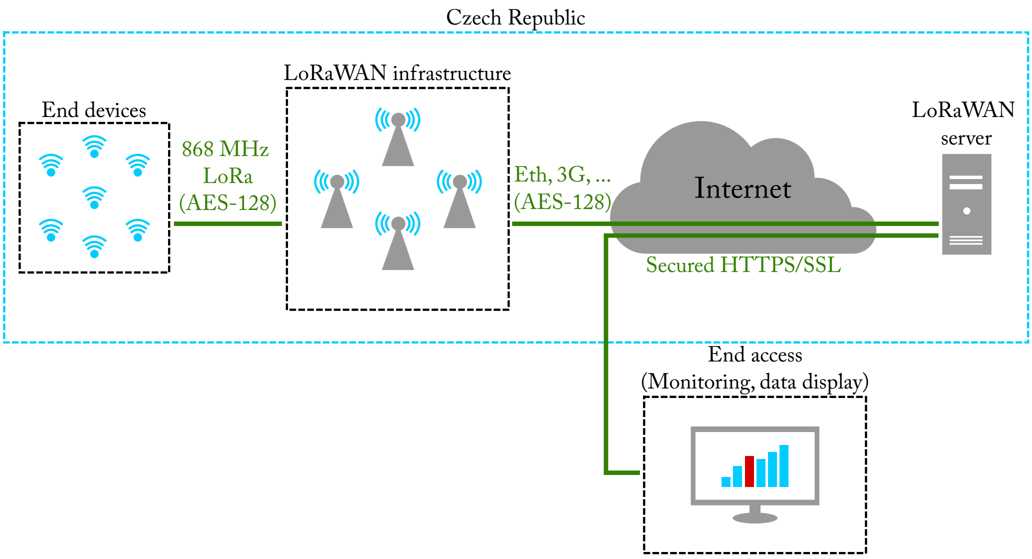

Figure 2: A network using the LoRaWAN protocol [7].

gyroscope GY-521 to record the movement of the beehive connected via the I^2C bus.

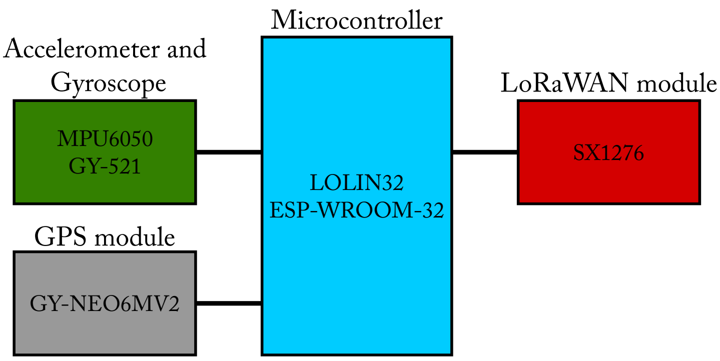

Figure 3: Simplified block diagram of a security system.

The system will be powered via the JST-PH-2 connector using a rechargeable and replaceable LiPol (Lithium Polymer) battery with a capacity of 5000 mAh, which should ensure uninterrupted operation for several months. The microcontroller itself offers 5 possible modes, where in addition to the active mode, the Deep-sleep Mode will be used most of the time with a consumption of 20 µA and will not be awakened until motion is detected by the accelerometer and gyroscope. The location of the device is also enabled by the LoRaWAN technology itself, but in the case of securing beehives, it is assumed that the device will be used outside the built-up area and the necessary network for precise positioning is not yet built in the Czech Republic. That is why the option was chosen to connect a GPS module to the device, which will achieve the required accuracy for locating the beehive. This module will be completely inactive during the operation of the device, a possible solution using MOSFET transistors to save battery power. It will only be activated if the microcontroller is woken to active mode. The LoRa module SX1276 also offers a sleep mode in which it consumes approximately 0.2 µA. After detecting the movement and localization, the command will wake the LoRa module and the data will be sent via the LoRaWAN network to the LoRaWAN server, where it will be further processed. The user will be sent an email about the beehive theft and it will be possible to track his current location using the GPS coordinates latitude and longitude.

6 CONCLUSION

This article focused on the design of a security system for beehives. In the introduction, the concept of IoT and the introduction of the selected ESP32 microcontroller were explained. The following chapter describes the LoRaWAN technology and the last chapter was devoted to the final design of a device for securing beehives. A test connection of a part of the design for functional testing was carried out. This connection consisted of the ESP32 microcontroller itself and a module with an accelerometer and a gyroscope to record the handling of the beehive.

Next, the device will be connected to the LoRaWAN network. A suitable box will be produced for placing the device in the hive, connecting a GPS module to track the position of the hive. The device will then be practically tested to see if it meets the basic requirements for securing beehives.

REFERENCES

[1] PATEL, K. K.; PATEL, M. S. *Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges.* International Journal of Engineering Science and Computing, 2016, vol. 6, no. 5, s. 6122–6131. ISSN 2321-3361.

[2] MEKKI, K.; BAJIC, E.; CHAXEL F.; MEYER F. *A comparative study of LPWAN technologies for large-scale IoTdeployment.* The Korean Institute of Communications and Information Sciences, 2019, vol. 5, no. 1, s. 1–7.

[3] MAIER, A.; SHARP, A.; VAGAPOV, Y. *Comparative analysis and practical implementation of the ESP32 microcontroller module for the internet of things.* Internet Technologies and Applications (ITA), Wrexham, 2017, s. 143–148.

[4] PURBA, J.; WAHYUDIN, D. *Bluetooth Low Energy (BLE) Based Power Window System.* IOP Conference Series: Materials Science and Engineering, Bandung, Indonesia, 2017, vol. 384.

[5] DE CARVALHO SILVA, J.; RODRIGUES, J. J. P. C.; ALBERTI, A. M.;SOLIC, P.; AQUINO, A. L. L. *LoRaWAN — A low power WAN protocol for Internet of Things: A review and opportunities.* 2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech),Split, 2017, s. 1–6.

[6] DAVCEV, D.; MITRESKI, K.; TRAJKOVIC, S.; NIKOLOVSKI, V.; KOTELI, N. *IoT agriculture system based on LoRaWAN.* 2018 14th IEEE International Workshop on Factory Communication Systems (WFCS), Imperia, 2018, s. 1–4.

[7] MAŠEK, P.; ŠTÚSEK, M.; FUJDIAK, R.; MLÝNEK P.; HOŠEK J. *Komunikační systémy pro IoT.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2019