



České
vysoké
učení technické
v Praze

F3

Fakulta elektrotechnická
Katedra telekomunikační techniky

Bezdrátová senzorová síť pro přístupový systém

Tomáš Hyhlík

Vedoucí: Ing. Bc. Marek Neruda, Ph.D
Školitel–specialista: Ing. Bc. Lukáš Vojtěch, Ph.D
Obor: Elektronika a komunikace
Studijní program: Elektronika
Říjen 2019

Poděkování | **Prohlášení**

Abstrakt

todo: edit abstract The Wireless Sensor Network (WSN) plays an important role in the Internet of Things (IoT). It is very suitable for intelligent buildings providing a convenient way to collect sensor data and control electronic devices in the building and its surroundings. This paper proposes an extension of the existing access control system with WSN. Design of sensor nodes and gateway connected to the existing RS485 network is performed. The results of a long-term operation measurement in one university floor show the maximum number of sensor nodes simultaneously transmitting data in RS485 network is up to hundreds or thousands in dependence on used RS485 data rate and used reserve of data rate which prevent from malfunction of the access control system. The results prove the WSN can be effectively used in an existing RS485 infrastructure.

Klíčová slova: Access control system, LoRa, LPWAN, WSN.

Vedoucí: Ing. Bc. Marek Neruda, Ph.D

Abstract

The Wireless Sensor Network (WSN) plays an important role in the Internet of Things (IoT). It is very suitable for intelligent buildings providing a convenient way to collect sensor data and control electronic devices in the building and its surroundings. This paper proposes an extension of the existing access control system with WSN. Design of sensor nodes and gateway connected to the existing RS485 network is performed. The results of a long-term operation measurement in one university floor show the maximum number of sensor nodes simultaneously transmitting data in RS485 network is up to hundreds or thousands in dependence on used RS485 data rate and used reserve of data rate which prevent from malfunction of the access control system. The results prove the WSN can be effectively used in an existing RS485 infrastructure.

Keywords: Access control system, LoRa, LPWAN, WSN.

Title translation: Wireless sensor network for access control system

Obsah

0.1 Seznam zkratek	1
1 Úvod	2
Část I Theoretical part	
2 Architektury přístupových systémů	6
3 Výběr bezdrátové technologie pro senzorovou síť	8
3.1 Kandidátní bezdrátové technologie	8
3.1.1 IQRF	8
3.2 Wireless M-bus	8
3.3 Zigbee.....	9
3.4 Bluetooth.....	9
3.5 LoRa.....	9
3.6 Sigfox ??	10
3.7 Z-Wave ??	10
3.8 Thread	10
3.9 RPMA ??.....	10

3.9.1 Wireless Sensor Network Design	10
--	----

Část II **Practical part**

4 Realizace zařízení	14
4.0.1 General System Design	14
4.0.2 Specific System Design for Testing Proposes	14
4.1 Výběr přenosové technologie ..	17
4.2 Výběr komponent	17
4.2.1 Microcontroller	17
4.2.2 LoRa transceiver	18
4.2.3 RS485 transceiver	18
4.3 Implementace LoRaWAN sítě ..	19
4.4 Implementace komunikačního protokolu v síti IMA_RS485 pro komunikaci s control panelem ..	19
4.4.1 Syntaxe příkazů	21
4.4.2 Adresace zařízení v síti ..	21
4.4.3 Statusy	21

4.4.4 Přidávání LoRaWAN zařízení do systému	22	5 Měření výsledky a diskuse	33
4.4.5 Odesílání dat z koncových zařízení	23	6 Závěr	36
4.4.6 Potvrzení	23	Literatura	37
4.4.7 Dotaz na příznaky	23		
4.5 Komunikace přes USB	24		
4.5.1 Log aplikace	24		
4.5.2 Konfigurace systému	25		
4.6 Koncová zařízení	28		
4.6.1 Zpracování dat jednotlivých typů koncových zařízení	28		
4.6.2 Přidávání koncových zařízení ze serveru K4	30		
4.7 Využití non-volatile paměti gatewaye	30		
4.8 Zapojení	30		
4.9 Naprogramování	31		
4.9.1 Zdrojové soubory projektu ..	31		
4.9.2 Nahrání programu do MCU .	32		

Obrázky

2.1 Příklad architektury přístupového systému [10]	6
3.1 LoRa spread factor options [24] .	10
4.1 IMA access control system architecture with WSN extension .	15
4.2 Location of sensor nodes and CKP devices on the university floor	16
4.3 Gateway block diagram, RFM95w [3], RS485 transceiver [7], NUCLEO-L073RZ [1]	16
4.4 Vývojový kit NUCLEO-L073RZ [1]	18
4.5 LoRa transceiver RFM95w [3] ..	18
4.6 RS485 transceiver [7]	19
4.7 foto zapojení	31
5.1 Measured data rate in [bps] in RS485 network during long-term operation test	34

Tabulky

4.1 The STM32L073RZ features [1].	17
4.2 Fyzické vlastnosti IMA_RS485 sítě	20
4.3 Syntaxe příkazu pro komunikaci v síti IMA_RS485	21
4.4 Příklad sekvence příkazů odesílaných mezi zařízením typu master a zařízením typu slave během předávání seznamu LoRaWAN device address koncových zařízení	22
4.5 Příklad dat příkazu "průchod" odeslaného z gatewaye na zarizení typu master, obsahující data z koncových zařízení	23
4.6 Nastavení USB terminálu	24
4.7 Defaultní konfigurace systému ..	28
4.8 Typy koncových zařízení	28
4.9 Pinout připojení externích periférií k procesoru	31
5.1 Packet length frequency analysis	34

0.1 Seznam zkratek

AI	Artifical Intelligence
AppSKey	Application Session Key
CPU	Central Processing Unit
CR	Carriage Return
CRC	Cyclic Redundancy Check
HW	HardWare
IoT	Internet of Things
ISM	Industrial, scientific and medical
LAN	Local Area Network
LF	Line Feed
LPWAN	Low Power Wide Area Network
LPWSN	Low Power Wireless Sensor Network
MCU	Micro Controller Unit
NwkSKey	Network Session Key
RF	Radio Frequency
WSN	Wireless Sensor Network
SF	Spreading Factor

Kapitola 1

Úvod

The demands and use cases of Internet of Things (IoT) applications including security, asset tracking, agriculture, smart metering, smart cities, and smart homes as well as the growth of IoT wireless technologies, which require long range, low power consumption, low data rate and low cost are recently increased.

Short-range IoT applications like smart homes are broadly based on Zigbee or Bluetooth technologies that use the 2.4 GHz ISM band [1], [2]. Long-range IoT applications are typically based on a special kind of wireless technology called Low Power Wide Area Network (LPWAN) [14]. Many LPWAN wireless communication technologies appeared during its evolution with unlicensed ISM band, e.g., LoRa and SigFox and licensed band, e.g., NarrowBand-Internet of Things (NB-IoT) and Long Term Evolution-Machine Type Communication (LTE-M). The LPWAN technologies aim to have range up to 10–15 km in rural areas and 2–5 km in urban areas [15] and can have one of the following topologies: star (centralized), star of stars (decentralized) and mesh (distributed) [11]. Very low power consumption should allow sensor nodes a very long battery life, even greater than 10 years. The low cost of hardware (HW) is achieved by fully integrated transceivers and minimized number of off-chip components [13].

The industry of IoT is growing because of its enormous potential. Cisco study [12] says IoT will be combined with other technologies such as artificial intelligence (AI), fog computing and blockchain. Such a combination of technologies will provide greater value of investment for companies. IoT applications in smart cities require a scalable network coverage. This can be achieved by interconnection of multiple gateways as proposed in [8], where all gateways are connected to web server accessible via the Internet. It aims to manage urban street lighting and the implementation of smart metering is also considered as a future work. Similar application is proposed in paper [1]

which focuses on assisted real-time automatic meter reading (AMR) in cities, but the scalable range is established by mesh network topology. The IoT applications in a smart buildings concept can be proposed as shown in [2], where nodes exchange data with the cloud via a Wi-Fi router or Bluetooth gateway connected to the Internet. Similar application is proposed in [9] where nodes are controlled by a master node via Zigbee network that is connected to a PC via RS232. Basic smart metering systems can be proposed with a gateway connected to a PC where the data are processed as proposed in [10], [11] and [17]. A long-range metering system can be established by multiple gateways connected to a network server from which data are obtained by the application server [13]. Similar network is proposed in Smart Farm application [16] with the difference that nodes can also be connected to the gateway via RS485 which forms a hybrid wired /wireless system.

This paper proposes to extend the access control system to include a low power Wireless Sensor Network (WSN) which can be used for smart metering applications, smart building applications and the building surroundings which is related to smart city applications. The WSN gateway is connected by the same way as a card reader is connected in the access control system, therefore it also has to support the same protocol. This can lead to complications since the reader is meant to transmit a short packets with user ID when the user's credential is attached to it. The WSN gateway is designed and tested in access control system of one university floor. The results show the infrastructure of access control system can manage up to thousands sensor nodes in dependence on used RS485 data rate.

Část I

Theoretical part

Kapitola 2

Architektury přístupových systémů

Přístupové systémy jsou elektronické systémy řídící přístup uživatelů do omezených prostor v závislosti na jejich prokázané identitě. Obrázek 2.1 zobrazuje typickou architekturu přístupového systému, kde identifikátor (ID Credential) představuje prvek umožňující identifikovat uživatele, např. RFID tag, otisk prstu nebo QR kód.



Obrázek 2.1: Příklad architektury přístupového systému [10]

Čtečka (Reader) slouží ke čtení dat z identifikátoru a v digitální podobě je odesílá k zařízení kontrolní panel (Control Panel). Zámek dveří (Door Lock) řídí fyzický přístup uživatelů do omezených prostor. Kontrolní panel tvoří rozhranní mezi Access Control Server a páry čteček a zámků dveří. kontrolní panely jsou obvykle připojeny k serveru řízení přístupu (Access Control Server) přes TCP/IP síť a páry čtečka a zámků dveří jsou obvykle připojeny ke kontrolnímu panelu přes RS485 síť. Databáze obsahuje všechna

uživatelské ID. Na serveru řízení přístupu je spuštěn Software (SW) spravující databázi a komunikující se všemi zařízeními typu Contril Panel. Čtečka čte uživatelská ID z předložených identifikátorů a přeposílá je na kontrolní panel, který je dále přeposílá na server řízení přístupu. Access Control Software vyhledá obdržený uživatelský identifikátor v databázi a pokud je nalezen, pošle příkaz odpovídajícímu kontrolnímu panelu k přepnutí odpovídajícímu zámku dveří, čímž je uživateli udělen přístup do omezené oblasti [10].

Kapitola 3

Výběr bezdrátové technologie pro senzorovou síť

Navržená senzorová síť je napojena na infrastrukturu zavedeného přístupového systému v budově zákazníka s dosahem po celé budově a jejím okolí. Takto navržená síť umožní v těchto prostorách snímání dat z desítek senzorů. Mezi hlavní kritéria pro vybranou bezdrátovou technologii patří nízká spotřeba energie koncových zařízení, nízká cena, jednoduchost implementace a možnost připojení koncových zařízení třetích stran. Pro jednoduchost implementace vybraná bezdrátová technologie tedy používá bezlicenční pásmo ISM.

3.1 Kandidátní bezdrátové technologie

Níže jsou popsány dostupné bezdrátové technologie vyhovující stanoveným kritériím pro tento projekt.

3.1.1 IQRF

IQRF je subGHz bezdrátová technologie vyvinuta IQRF aliancí [4], která je jediným výrobcem IQRF transceiveru [3] za cenu v rozsahu \$15-20 za kus a k tomu poskytuje nástroje jako je SDK [2] a IDE [1]. Z hlediska kriérů pro tento projekt je u této technologie nevýhodou nízký počet zařízení třetích stran dostupných na trhu. Většinou je tedy tato technologie používána pro realizaci vlastní sítě??

3.2 Wireless M-bus

"Wireless Meter Bus has its origins within the Meter-Bus standards. This is a field bus standard aimed at applications for collecting meter data for gas, electricity, water, etc." [5] It supports a few application modes for differing

applications.

- S1 Unidirectional, data are transmitted only a several times a day.
- S2 Bidirectional version of S1.
- T1 Unidirectional transmission of data with a period of a few seconds of minutes.
- T2 Bidirectional version of T1.
- C1 Unidirectional transmission of bigger amount of data.
- C2 Bidirectional version of C1.

Usually one M-bus device support only a few of these application modes [5] [6] [7] [8].

3.3 Zigbee

Zigbee, developed by zigbee alliance is usually used for mesh sensor networks because of its short range. This technology is standardized since 2003, so there is many available nodes at the market by now [10] [11] [12].

3.4 Bluetooth

Bluetooth has the big advantage, taht it's built in almost every mobile phone, tablet or laptop so there are more options to control the network. The Bluetooth 4.0+ also called BLE (Bluetooth Low Energy) aims to low power wireless sensor networks. It can be used for point-to-point, broadcast or mesh network topology [13] [14] [15] [16].

3.5 LoRa

The name LoRa stands for "Long Range"wireless communication with low data rate and power consumption. The protocol enables to modify SF which affects the communication range and data rate. The 3.1 shows this dependence.

This technology is very attractive for its long range capability and easy to connect nodes. It's complicated to build a full-capacity gateway which is capable of receiving packets at all frequency channels and SF in parallel. The

Spreading Factor (125kHz Lora)	Bit rate(bps)	Range (varies on propagation conditions)	Time on air(ms) (10 bytes payload)	0.1% of Time on air waiting time	1% of Time on air waiting time
SF7	5470	2 km	56 ms	1 min	6s
SF8	3125	4 km	100 ms	1 min 40s	10s
SF9	1760	6 km	200 ms	3 min 20s	20s
SF10	980	8 km	370 ms	6 min 10s	37s
SF11	440	14 km	740 ms	12 min 20s	1 min 14s
SF12	290	20 km	1400 ms	23 min 20s	2min 20s

Obrázek 3.1: LoRa spread factor options [24]

transceiver for this application costs about \$130. Although it's also possible to build single-channel gateway which is way too cheaper, but it can receive packets at only one frequency channel and SF at once [17] [18] [19] [20] [21] [22] [23] [24].

■ 3.6 Sigfox ??

This technology focuses on short message and long range communication applications [25] [26].

■ 3.7 Z-Wave ??

Z-Wave is intended for wireless connectivity for all possible smart home products, controlled by PC, phone, voice, etc. It's based on mesh network topology so every non-battery powered device works as a router to enhance the network range so the more devices are connected in one network, the stronger the network is [27] [28].

■ 3.8 Thread

This technology based on IPv6 was developed for home network controlled by smartphone, tablet or PC [29] [30] [31].

■ 3.9 RPMA ??

The "Random Phase Multiple Access" developed by Ingenu designed for M2M and IoT applications [32] [33] [34]. *"RPMA has been deployed for the Machine Network, but can also be rolled out as a private network installation. It is highly suitable for regions, where the rollout of 3GPP LPWA technologies is lagging, where cellular coverage is generally weak, or where users would like to exert full control over their network deployments."* [33]

■ 3.9.1 Wireless Sensor Network Design

Wireless sensor network design is based on a popular IoT technology LoRa, which is a LPWAN technology using ISM band, 433 MHz, 868 MHz and 915 MHz (depends on the region) and communicates on multiple frequency channels and uses multiple data rates [16]. The LoRaWAN is an open standard network protocol and system architecture specified by [17] and creates a media access control (MAC) layer on the top of the LoRa physical layer, secured by AES-128 encryption. The LoRaWAN nodes communicate directly with the LoRaWAN gateway [18].

Část II

Practical part

Kapitola 4

Realizace zařízení

■ 4.0.1 General System Design

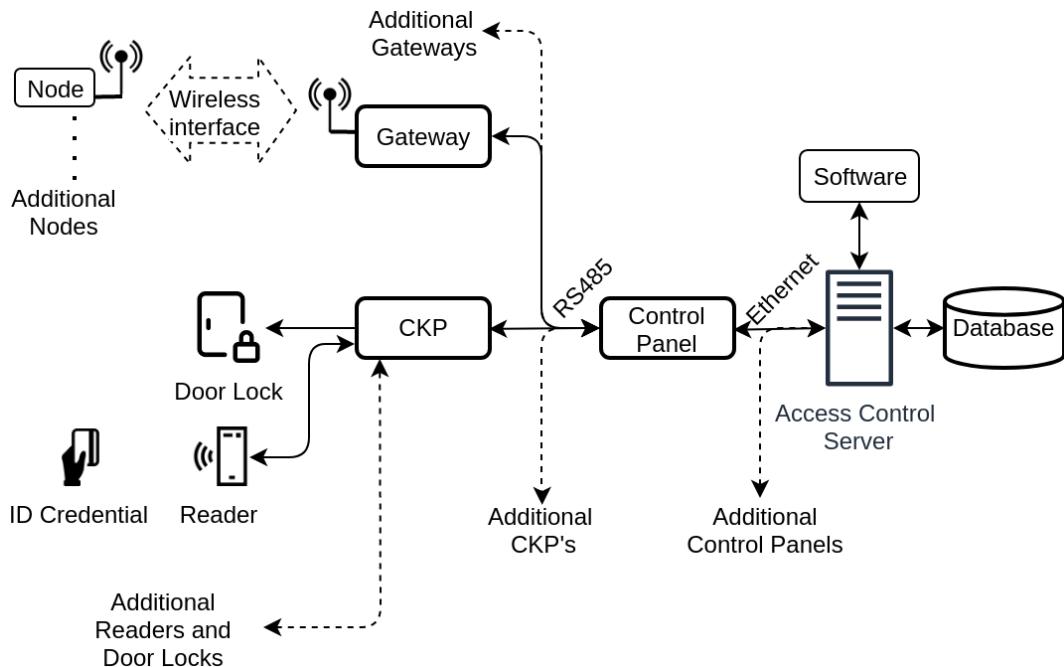
■ Wireless Sensor Network Design

Wireless sensor network design is based on a popular IoT technology LoRa, which is a LPWAN technology using ISM band, 433 MHz, 868 MHz and 915 MHz (depends on the region) and communicates on multiple frequency channels and uses multiple data rates [16]. The LoRaWAN is an open standard network protocol and system architecture specified by [17] and creates a media access control (MAC) layer on the top of the LoRa physical layer, secured by AES-128 encryption. The LoRaWAN nodes communicate directly with the LoRaWAN gateway [18].

■ 4.0.2 Specific System Design for Testing Proposes

■ Tested Access Control System Architecture

The access control system to be extended by WSN is designed by IMA company, but it differs from the general architecture shown in Fig. 2.1 by an added CKP device that creates an interface between the Control Panel and the Reader with the Door Lock. There are several types of CKP devices to connect different types of Readers, Door Locks, barriers and gates, but all of them support the protocol of the IMA company on the RS485 network. The IoT extension of the access control system is done by connecting a WSN Gateway to the Control Panel via the RS485 network, i.e., the same way as CKP device is connected as shown in Fig. 4.1. Therefore the WSN Gateway has to support the same protocol as CKP device in RS485 network to communicate with the Control Panel. It's a collision protocol, where all connected devices follow the rule "listen before talk", collisions are detected by integrity check mechanism applied for all messages. When the device receives a corrupted command, it requests a retry.



Obrázek 4.1: IMA access control system architecture with WSN extension

The Access Control System operates by obtaining a CKP list of valid cards (ID Credentials) from the Access Control Server. The designed Gateway takes it as a list of valid device addresses in the WSN. When the user presents his card to the Reader and the card ID matches one of the valid cards, the CKP device sends the data to the Access Control Server. The same procedure applies to the Gateway. When the Gateway receives data from a Node and the Node address matches one of the valid device address list, the Gateway sends the data to the Access Control Server.

■ Design of Tested Wireless Sensor Network

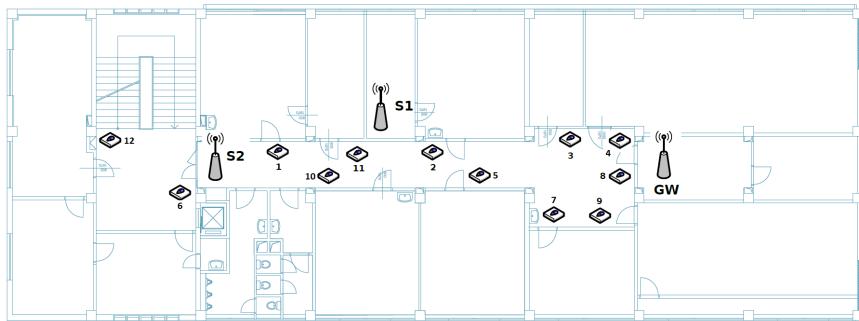
The most important requirements for the WSN Gateway are simplicity, low cost and the ability to use third-party nodes. LoRa with the standardized network protocol LoRaWAN is chosen as wireless communication technology, but only in single-channel mode as used in development projects [19], so it is not fully LoRaWAN compliant. Single-channel Gateway communicates only on one channel and data rate at a time, therefore all devices in WSN are configured for one frequency channel and data rate. The advantage of a single-channel Gateway is about ten times cheaper transceiver and lower CPU performance requirements than standard LoRaWAN Gateway transceiver. Third-party LoRaWAN nodes are fully compatible with any LoRaWAN Gateway, so it can be deployed into this system, but it needs to be configured to communicate at the specified frequency channel and data rate. LoRaWAN protocol uses 4-byte device address for nodes. These 4 bytes and node payload are included in the communication protocol between the Gateway and the

Control Panel via RS485. In the case of lack of space, the node payload is decoded in the Gateway according to node payload documentation provided by manufacturer [20] and only the required data are transmitted to the Control Panel.

In summary, when the Gateway receives an encrypted LoRaWAN packet, it looks for whether the Node device address is in the list of known device addresses. If this is the case, the packet is encoded in the communication protocol of the Gateway and sent to the Control Panel. If there is not enough space in communication protocol of the Gateway, the packet is decrypted and relevant data, i.e., sensor values, are selected.

In this design the opposite direction of communication direction is not implemented, but it can also be used to control actuators, e.g., switch, motor.

To test the proposed system design, the Gateway is built from one NUCLEO-L073RZ development board [1], RFM95w LoRa Shield [3] and RS485 transceiver [7], Fig. 4.3.



Obrázek 4.2: Location of sensor nodes and CKP devices on the university floor



Obrázek 4.3: Gateway block diagram, RFM95w [3], RS485 transceiver [7], NUCLEO-L073RZ [1]

The NUCLEO-L073RZ development board with STM32L073RZ microcontroller is suitable for the development purposes because of its parameters, Tab. 4.1, price and available documentation. LoRa transceiver board RFM95w with SX1276 chip integrated into Dragino LoRa Shield has the same pinout as the NUCLEO-L073RZ development board. RS485 transceiver as an RS485/UART interface enables communication with Control Panel.

Microcontroller architecture	ARM Cortex-M0+ 32-bit RISC
Internal flash memory	192 kB
Internal SRAM memory	20 kB
Internal EEPROM memory	6 kB
CPU frequency	up to 32 MHz
Interfaces	2x SPI, 3x I2C, 4x UART, LIN

Tabulka 4.1: The STM32L073RZ features [1]

4.1 Výběr přenosové technologie

Pro implementaci LPWSN je použita RF technologie LoRa se standardizovaným síťovým protokolem LoRaWAN, ale s požitím pouze jednoho kanálu. Tento způsob řešení se liší od standardu omezením na pouze jeden kanál a SF vysílání. Jedenokanálové řešení bylo zvoleno z toho důvodu, že plnohodnotný LoRa transceiver, který přijímá na všech osmi kanálech je příliš drahý (přibližně desetinásobná cena) a složitý k implementaci, zatímco v tomto projektu je kladen důraz na cenu a jednoduchost řešení.

Vybraná technologie používá topologii typu hvězda, tedy koncová zařízení komunikují přímo s gateway, zbytek času mohou být ve stavu nízké spotřeby, což má pozitivní vliv na životnost baterie. Koncová zařízení od různých výrobců jsou plně kompatibilní s cizí gateway, tudíž není problém je implementovat do tohoto systému. Je pouze třeba je překonfigurovat pro vysílání na jednom použitém kanále a SF.

4.2 Výběr komponent

4.2.1 Microcontroller

Pro toto zařízení je zvolen mikrocontroller STM32L073RZ se zaměřením na nízkou spotřebu, jelikož je levný, má dostačující vlastnosti a je dostupný ve formě vývojového kitu NUCLEO-L073RZ který byl použit pro vývoj zařízení. Mezi hlavní vlastnosti patří [1]:

- Architektura ARM Cortex-M0+ 32-bit RISC
- Interní Flash paměť 192 KB
- Interní SRAM paměť 20 KB
- Interní EEPROM paměť 6 KB
- Až 32 MHz CPU

- 2X SPI, 3x I2C, 4x USART, LIN, ADC

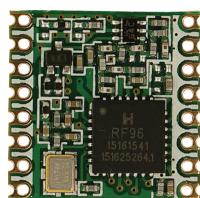
Pořizovací cena kitu přímo na stránce výrobce www.st.com je \$13 [1] [2].



Obrázek 4.4: Vývojový kit NUCLEO-L073RZ [1]

4.2.2 LoRa transceiver

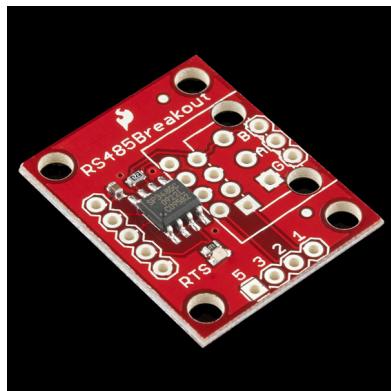
Lora transceiver čip doposud vyrábí pouze Semtech, pro použití v Evropském pásmu je určen typ SX1276. V tomto návrhu je použita deska RFM95w od firmy HopeRF s integrovaným čipem SX1276 [3]. Pro vývoj zařízení byl využit tento transciever v tzv. Dragino LoRa Shield [4], který má stejně jako použitý vývojový kit, pinout kompatibilní s Arduino UNO. Pořizovací cena samotného transceiveru RFM95w je okolo \$7, cena Dragino Shieldu se pohybuje okolo \$22 na ebay.



Obrázek 4.5: LoRa transceiver RFM95w [3]

4.2.3 RS485 transceiver

SparkFun Transceiver Breakout - RS485 převádí rozhranní UART na RS485, pří vstupním napětí 3.3 V. A je dostupný za cenu okolo \$10 [7].



Obrázek 4.6: RS485 transceiver [7]

4.3 Implementace LoRaWAN sítě

Jednokanálové použití technologie LoRa umožňuje použít transceiver navržený pro koncová zařízení, kterým jsou pakety kontinuálně odposlouchávány na jednom nastaveném kanále a SF. Tyto dva parametry jsou nakonfigurovány na všech zařízeních v síti stejně.

Jak je popsáno v sekci ??, použitý protokol pro komunikaci s control panelem přístupového systému firmy IMA zajišťuje posílání dat z koncových zařízení příkazem "průchod", který má kapacitu na data z koncového zařízení pouze 6 B. Systém je proto navržen neobvyklým způsobem. Přijme-li gateway LoRaWAN paket, nejprve zkонтroluje zda zná adresu zařízení, pokud ano, přečte z paměti i typ zařízení, paket dešifruje a dekóduje payload, čímž získá konečné hodnoty senzorů, které pak dále pošle přes RS485 rozhraní na zařízení typu master.

LoRaWAN device address a typ každého zařízení v síti je uložena v EEPROM (non-volatile) paměti gatewaye a jsou nastavována na z access control serveru. Všechna zařízení v síti mají nastavené stejné šifrovací klíče a gateway je má uložené v EEPROM.

Pro tento projekt byla vyvinuta knihovna pro dekódování payloadu na základě dokumentů [8] [9].

4.4 Implementace komunikačního protokolu v síti IMA_RS485 pro komunikaci s control panelem

V tomto projektu je komunikace protokolu IMA_RS485 naprogramována v souborech rs485_protocol.h a rs485_protocol.c. Jedná se o kolizní protokol

■ ■ ■ 4.4. Implementace komunikačního protokolu v síti IMA_RS485 pro komunikaci s control panelem

v síti, kde je připojen jedno zařízení typu master, a jeden nebo více zařízení v typu slave.

Baud rate	9600
Data bits	8
Parity	none
Stop bits	1

Tabulka 4.2: Fyzické vlastnosti IMA_RS485 sítě

■ 4.4. Implementace komunikačního protokolu v síti IMA_RS485 pro komunikaci s control panelem

■ 4.4.1 Syntaxe příkazů

Komunikace v síti probíhá formou příkazů, které mají specifikovanou syntaxi v tabulce 4.3.

popis	adresa příjemce	adresa odesílatele	typ příkazu	délka dat	data	crc
počet bytů	1	1	1	2	délka dat	1

Tabulka 4.3: Syntaxe příkazu pro komunikaci v síti IMA_RS485

Typy příkazu jsou zadefinované konstanty s předponou CKP_CMD_ v souboru ./Inc/rs485_protocol.h. Příkazy odeslané zařízením typu master obsahují navíc synchronizační byte na začátku 0xAA. CRC je pro kontrolu XOR přes všechny předchozí byty v celém příkazu kromě synchronizačního bytu.

■ 4.4.2 Adresace zařízení v síti

Každé zařízení na této sběrnici má svoji adresu, která mu je nastavena externě. Zařízení typu master má adresu 0xFF, adresa pro všechny (broadcast) je 0x00 a zařízení v této síti můžou mít adresu libovolnou (kromě těchto dvou) nesmí zde však být připojena 2 zařízení s nastavenou stejnou adresou.

■ 4.4.3 Statusy

Zařízení typu slave má dva možné statusy v síti IMA_RS485, offline a online. Zařízení typu slave má povoleno odesílat příkaz "průchod" pouze má-li status online. Zařízení typu slave odesílá příkaz obsahující informaci o jeho statusu periodicky s typem příkazu 0x10 a jedním bytem dat označujícím status. Pro status online je tento byte 0x00 a pro status offline 0xEE. Tento příkaz je odesílán s intervalm 10 s, pokud zařízení má status offline a s intervalm 30 s, pokud má zařízení status online. Status zařízení mění pouze zařízení typu master odesláním příkazu s typem 0x41 pro přepnutí na status online a 0x42 pro přepnutí na status offline. Zařízení typu slave svůj status přepne samo pouze v případě, že má status online a zařízení typu master přestane odpovídat na příkaz průchod, jak je popsáno v sekci 4.4.5. Je-li zařízení spuštěno, je ve stavu offline a jelikož nemá povoleno odesílat příkaz "průchod", přijatá data z koncových zařízení jsou zahazována. Zařízení typu slave pouze odpovídá na příkazy od zařízení typu master a čeká na příkaz od zařízení typu master k přepnutí na status online.

■ 4.4.4 Přidávání LoRaWAN zařízení do systému

Pokud zařízení typu master příjme příkaz od zařízení typu slave oznamující že je ve stavu offline, nejprve tomuto zařízení pošle seznam LoRaWAN adres všech známých koncových zařízení a následně toto zařízení přepne do stavu online. Přijímání seznamu adres je realizováno sekvencí příkazů typu 0x8F.

Níže v tabulce 4.4 je příklad sekvence příkazů odesílaných mezi zařízením typu masterem a zařízením typu slavem během předávání seznamu LoRaWAN device address koncových zařízení, kde zařízení typu slave má adresu 0x10 a zařízení typu master standardně 0xFF. Jak již bylo řečeno, příkazy od zařízení typu master lze jednoduše odlišit tím, že vždy začínají bytem 0xAA.

příkaz	data
master: start	AA 10 FF 8F 02 00 00 00 62
slave: ACK	FF 10 06 02 00 8F 00 64
master: data	AA 10 FF 8F 21 00 01 B1 C4 12 00 00 00 00 00 B2 C4 12 00 00 00 00 00 B3 C4 12 00 00 00 00 00 B4 C4 12 00 00 00 00 00 44
slave: ACK	FF 10 06 02 00 8F 01 65
master: data	AA 10 FF 8F 19 00 02 B5 C4 12 00 00 00 00 00 B6 C4 12 00 00 00 00 00 F6 1F 01 26 00 00 00 00 B6
slave: ACK	FF 10 06 02 00 8F 02 66
master: konec	AA 10 FF 8F 04 00 03 FF 2A 57 E5
slave: ACK	FF 10 06 02 00 8F 03 67

Tabulka 4.4: Příklad sekvence příkazů odesílaných mezi zařízením typu master a zařízením typu slave během předávání seznamu LoRaWAN device address koncových zařízení

LoraWAN protokol používá 4-bytové adresy koncových zařízení. Adresy předávány touto sekvencí jsou dlouhé 8-bytové. První 4 byty je tedy LoRaWAN device address, pátý byte je typ zařízení a zbylé 3 byty jsou nevyužity, jejich použití je možné v případě změn či rozšiřování vlastností systému.

První Byte dat je counter paketu začínající od nuly, který označuje číslo odeslaného paketu v sekvenci. Na každý tento paket v sekvenci zařízení typu slave odpovídá ACK příkaz, který se liší od obyčejného ACK příkazu tím, že v datech paketu navíc obsahuje counter pakety v sekvenci. První příkaz této sekvence má délku dat 2 byty, které mají hodnotu 0x00 přičemž první je counter. Další příkazy hned za counter bytem obsahují několik osmibytových adres, jejichž počet je různý. Příkaz ukončující tuto sekvenci příkazů má délku 4 byty, což je tedy counter, 0xFF a 2 byty CRC přes všechny odeslané adresy (nepodstatné, tudíž ho nepoužívám).

■ 4.4.5 Odesílání dat z koncových zařízení

Jak je popsáno v sekci ??, tudíž data z koncových zařízení jsou odesílána příkazem "průchod", jehož typ je 0x10 a kapacita na data z koncového zařízení je pouze 6 B. První byte dat označuje typ průchodu, byl zvolen konstantní byte 0xD0. Dále následuje LoRaWAN adresa koncového zařízení od kterého byl paket přijat. Dále následují 4 byty dat ze senzoru, další 2 byty signalizující čas průchodu, což v tomto projektu není použito a tyto dva byty mají vždy hodnotu 0xFF. A nakonec jsou další 2 byty obsahující data ze senzoru. Příklad příkazu: FF 1F 10 0D 00 D0 F6 1F 01 29 AD 0A 5A 27 FF FF DE 09 E1. Data příkazu jsou níže rozepsána v tabulce 4.5.

typ průchodu	LoRaWAN device address	data (4B)	cas	data (2B)
D0	F6 1F 01 29	AD 0A 5A 27	FF FF	DE 09

Tabulka 4.5: Příklad dat příkazu "průchod" odeslaného z gatewaye na zarizení typu master, obsahující data z koncových zařízení

Zařízení typu master na příkaz "průchod" odpovídá příkazem ACK. Zařízení typu slave na tuto odpověď čeká standardně 3 sekundy, ale tento parametr je nastavitelný. Pokud v tomto timeoutu zařízení typu master neodpoví, zařízení typu slave příkaz "průchod" zopakuje přičemž změní typ příkazu na 0x20. Pokud zařízení typu master ani na třetí opakování neodpoví ACK, zařízení typu slave se přepne do stavu offline a vymaže frontu příkazů "průchod" k odeslání.

■ 4.4.6 Potvrzení

Zařízení typu slave odpovídá na každý příkaz od zařízení typu master ACK. Typ příkazu ACK je 0x06 a data příkazu obsahují jeden byte signalizující typ příkazu na který je právě odpovídáno potvrzením. Zařízení typu master odpovídá ACK se stejným typem příkazu 0x06, ale s žádnými daty příkazu.

■ 4.4.7 Dotaz na příznaky

Zařízení typu master se může zeptat s jak dlouhými adresami zařízení typu slave pracuje s typem příkazu 0x49. Zařízení typu slave na to odpovídá ACK s tím, že v datech příkazu je navíc byte 0x04. Zařízení typu master pak počítá s tím, že zařízení typu slave pracuje se 64-bit adresami (ve skutečnosti ale používá 32-bitové a zbylé 4 byty v příkazu průchod jsou pro data z koncového zařízení).

4.5 Komunikace přes USB

Gateway má implementovanou komunikaci přes USB, což má za účel konfiguraci systému a logování. K připojení přes USB lze použít PC s aplikací terminálu s nastavením viz tabulka 4.6.

Baud rate	115200
Data bits	8
Parity	none
Stop bits	1
Flow control	none

Tabulka 4.6: Nastavení USB terminálu

Při komunikaci jsou data standardně oddělována bytem CR (carriage return) 0x0D, ale je akceptována i sekvence CR LF (Line Feed), tedy 0x0D 0x0A.

4.5.1 Log aplikace

Gateway loguje informace o proběhlých událostech přes USB. Níže je příklad výpisu dat pro případ, že gateway přjala LoRaWAN paket z koncového zařízení v síti.

Nejprve jsou vypsána data týkající se LoRaWAN protokolu, zašifrovaný i dešifrovaný payload, typ zařízení a konečné informace dekódované z payloadu. Řádek začínající předponou "Tx -> RS-485:" obsahuje data odeslané k zařízení typu master přes RS485 síť a následující řádek začínající předponou "Rx -> RS-485:" obsahuje odpověď od zařízení typu master.

```
Rx -> LoRaWAN, pktCntr: 6
RSSI: -51, SNR: 9, length: 22

Message type: Unconfirmed Data Up
Packet rawData: "40F61F0128C0D62508D970CB071595D115BAC68F6663"
Device Address: "F61F0128"
FCnt: 9686
message (encrypted): "D970CB071595D115BA"
MHDR: 40; FCtrl: C0; FPort: 08; MIC: "C68F6663"
adaptive data rate: true; ack: false
message HEX (decrypted): "013566779600FFFFAF"
```

```
Sensor type: RHF1S001
temperature: 23.30 C, humidity: 52 %
period: 300 s, RSSI: -51 dBm, SNR: 9 dB, battery voltage: 3.2 V
Tx -> RS-485: "FF1F100D00D0F61F01281A0934CDFFF09202E"
```

```
Rx -> RS-485: "AA1FFF060000E6"
ACK
```

4.5.2 Konfigurace systému

Konfigurace gatewaye se provádí opět přes USB port. Je do ní vstoupeno odesláním příkazu "config", následuje vypsání současného stavu konfigurace a dále je vypsáno konfigurační menu, kde uživatel vybere jednotlivý bod menu zadáním jeho čísla na začátku řádku. Níže je zobrazen příklad výpisu po vstupu do konfigurace.

```
-----Entering configuration setup-----
```

```
System configuration:
```

```
*** LoRa channel:
channel: 0 (868.1 Mhz)
SF7
```

```
*** RS485 channel:
my address: 10
master address: FF
timeout: 3 s
```

```
*** LoRaWAN keys:
NwSKey: FD 90 0D 8C 70 9F 19 24 18 EC FD D4 28 0C AC 47
AppSKey: 68 9F D0 AC 7A 0F 95 58 B1 19 A0 16 17 F4 16 33
```

```
Config menu:
1 -> Config LoRa channel
2 -> Config RS485 channel
3 -> Config LoRaWAN protocol
4 -> Print all LoRaWAN devices
5 -> Erase all LoRaWAN devices
6 -> Restore to default configuration
7 -> Exit without save
8 -> Save and exit
```

Z konfigurace je možné vystoupit kdykoliv bez uložení změn příkazem "quit". Při vstoupení do konfigurace je pozastavena činnost gatewaye, komunikace s koncovými zařízeními LoRaWAN sítě a komunikace se zařízením typu master v síti RS485 nejsou aktivní. Jsou zde tedy 3 stavy konfigurace, přičemž je možné vždy jednotlivá nastavení přeskakovat odesláním "prázdného příkazu" 0x0D (v terminálu obvykle stačí stisknout Enter). Systém při konfiguraci vždy vypíše jaká data mají být zadána v jakém tvaru a zároveň současnou hodnotu měněného parametru. Zadaná data uživatelem jsou vždy zkонтrolována zda

splňují požadovaný tvar. Pokud ne, uživatel je o tom informován a vyzván k dalšímu pokusu. Po provedení konfigurace následuje vždy návrat zpět do hlavního menu. Pro uložení nové konfigurace je potřeba v menu vybrat "Save and exit", gateway pak následně vypíše které parametry byly změněny a provede restart.

■ Config LoRa channel

Konfigurace LoRa RF kanálu zahrnuje nastavení SF a frekvenční pásmo. Níže je příklad konfigurace.

```
LoRa channel configuration:
Enter SF number (7-12)
(current: 7)
8
SF8 set.

Enter LoRa channel number (0-7)
ch0 is 868.1 Mhz
ch1 is 868.3 Mhz
ch2 is 868.5 Mhz
ch3 is 867.1 Mhz
ch4 is 867.3 Mhz
ch5 is 867.5 Mhz
ch6 is 867.7 Mhz
ch7 is 869.0 Mhz
(current: 0)
1
channel 1 set.
```

■ Config RS485 channel

Konfigurace RS485 kanálu pro komunikaci se zařízením typu master zahrnuje nastavení adresy tohoto zařízení, adresa zařízení typu master a timeout, což je doba čekání na potvrzení od zařízení typu master po odeslání příkazu "průchod". Níže je příklad konfigurace.

```
RS485 channel configuration:
Enter address of this device, FF and 00 are reserved.
(current: 10)
11
Address of this device is set to: 11

Enter master address:
(current: FF)
FE
Master address is set to: FE

Enter timeout (seconds)
```

```
(current: 3)
5
timeout set to: 5 s
```

■ Config LoRaWAN protocol

Konfigurace LoRaWAN protokolu zahrnuje nastavení šifrovacích klíčů NwkSKey a AppSKey. Níže je příklad konfigurace.

```
LoRaWAN protocol configuration:
Enter NwkSKey (16 bytes in HEX)
(current: FD 90 0D 8C 70 9F 19 24 18 EC FD D4 28 0C AC 47)
11111112222222333333344444444
NwSKey set to: 11 11 11 11 22 22 22 22 33 33 33 33 44 44 44 44

Enter AppSKey (16 bytes in HEX)
(current: 68 9F D0 AC 7A 0F 95 58 B1 19 A0 16 17 F4 16 33)
11111112222222333333344444444
AppSKey set to: 11 11 11 11 22 22 22 22 33 33 33 33 44 44 44 44
```

■ Print all LoRaWAN devices

Vypíše všechna LoRaWAN zařízení uložená v paměti. Níže je příklad.

```
number.....0:
Device Address: B1 C4 12 00
Device Type: RH1S001
number.....1:
Device Address: B2 C4 12 00
Device Type: RH1S001
number.....2:
Device Address: B3 C4 12 00
Device Type: RH1S001
number.....3:
Device Address: B4 C4 12 00
Device Type: IMA_tempPress
number.....4:
Device Address: B5 C4 12 00
Device Type: IMA_tempPress
```

■ Restore default configuration

Po zvolení této možnosti je načtena defaultní konfigurace systému, která obsahuje hodnoty viz tabulka 4.7. Tyto defaultní hodnoty jsou nastaveny v programu a slouží především pro testovací účely.

popis	hodnota
RS485 myAddr	0x10
RS485 MasterAddr	0xFF
RS485 timeout	3
LoRa SF	SF7
LoRa channel	0 (868.1 Mhz)
NwSKey	FD 90 0D 8C 70 9F 19 24 18 EC FD D4 28 0C AC 47
AppSKey	68 9F D0 AC 7A 0F 95 58 B1 19 A0 16 17 F4 16 33

Tabulka 4.7: Defaultní konfigurace systému

4.6 Koncová zařízení

Jelikož používaný protokol ke komunikaci se zařízením typu master je omezen na pouhých 6 B na jeden paket, payload koncových zařízení je dekódován v gatewayi a v paketu odeslaném na zařízení typu master jsou pouze vybraná nejdůležitější data, která se vejdu do této velikosti. Prote společně s LoRaWAN device address koncového zařízení je v gatewayi uložen i typ zařízení zadefinován jedním bytem a na základě typu zařízení gateway rozpozná jak dekódovat payload.

Momentálně jsou podporovány dva typy koncových zařízení, dle potřeby je možné rozšířit FW gatewaye o další typy koncových zařízení.

Typ zařízení	Hodnota
RHF1S001	0x00
IMA_tempPress	0x01

Tabulka 4.8: Typy koncových zařízení

4.6.1 Zpracování dat jednotlivých typů koncových zařízení

Níže je popsáno pro jednotlivá podporovaná koncová zařízení jak jsou data uložena v datové struktuře, jak jsou data z této struktury zpracována a zobrazena a nakonec jak vybraná data jsou zapsána do výsledného bufferu o délce 6 B, který je odeslán na zařízení typu master příkazem "průchod".

RHF1S001

Senzor od firmy RisingHF měří teplotu a vlhkost.

```

1  /* RHF1S001 data structure */
2  typedef struct {
3      int16_t temperature;
4      uint8_t humidity;
5      uint16_t period;
6      int8_t rssi ;

```

```

7     int8_t snr;
8     uint8_t battery;
9 } RHF1S001_data_t;
10
11 /* Print the data from the structure */
12 printf("temperature: %d.%d C, ", RHF1S001_data.temperature / 100,
13     RHF1S001_data.temperature % 100);
14 printf("humidity: %d %%\n", RHF1S001_data.humidity);
15 printf("period: %d s, ", (int)RHF1S001_data.period);
16 printf("RSSI: %d dBm, ", RHF1S001_data.rssi);
17 printf("SNR: %d dB, ", RHF1S001_data.snr);
18 printf("battery voltage: %d.%d V\r\n", RHF1S001_data.battery/10,
19     RHF1S001_data.battery % 10);
20
21 /* Put the data into 6B long buffer, that is transmitted to the master */
22 buffer [0] = RHF1S001_data.temperature & 0xFF;
23 buffer [1] = RHF1S001_data.temperature >> 8;
24 buffer [2] = RHF1S001_data.humidity;
25 buffer [3] = RHF1S001_data.rssi;
26 buffer [4] = RHF1S001_data.snr;
27 buffer [5] = RHF1S001_data.battery;

```

IMA_tempPress

Senzor vytvořený ve firmě IMA, měřící teplotu a tlak.

```

1  /* IMA_tempPress data structure */
2  typedef struct {
3      int16_t temperature;
4      uint16_t pressure;
5      int8_t rssi ;
6      int8_t snr;
7  } IMA_tempPress_data_t;
8
9  /* print the data from the structure */
10 printf("temperature: %d.%d C, ", IMA_tempPress_data.temperature / 100,
11     IMA_tempPress_data.temperature % 100);
12 printf("pressure: %d.%d Pa\r\n", IMA_tempPress_data.pressure/10,
13     IMA_tempPress_data.pressure % 10);
14 printf("RSSI: %d dBm, SNR: %d dB\r\n", IMA_tempPress_data.rssi,
15     IMA_tempPress_data.snr);
16
17 /* Put the data into 6B long buffer, that is transmitted to the K4 server */
18 buffer [0] = IMA_tempPress_data.temperature & 0xFF;
19 buffer [1] = IMA_tempPress_data.temperature >> 8;
20 buffer [2] = IMA_tempPress_data.pressure & 0xFF;
21 buffer [3] = IMA_tempPress_data.pressure >> 8;
22 buffer [4] = IMA_tempPress_data.rssi;
23 buffer [5] = IMA_tempPress_data.snr;

```

4.6.2 Přidávání koncových zařízení ze serveru K4

Koncová zařízení síť se nastavují ze serveru K4 v podobě seznamu offline karet s délkou UID 8 B. LoRaWAN device address je dlouhá 4 B, jeden byte je navíc použit pro typ koncového zařízení, zbylé 3 byty jsou nuly. Jelikož typ zařízení je uložen v gatewayi i na K4 serveru. Při odesílání příkazu průchod se tedy už typ zařízení neposílá z důvodu datového omezení tohoto příkazu. Na serveru K4 se UID nastavuje jako dekadické číslo. Níže je příklad vytvoření výsledného čísla obsahující DevAddr a typ zařízení, které se zadává do K4 serveru.

Příklad

Pro případ, kde typ zařízení je 01 a DevAddr AABBCCDD (little endian) výsledné číslo v hexadecimální podobě je 01DDCCBAA. Následně se překládá do decimalní podoby, výsledné číslo k zadání do K4 serveru je tedy 8016149418.

4.7 Využití non-volatile paměti gatewaye

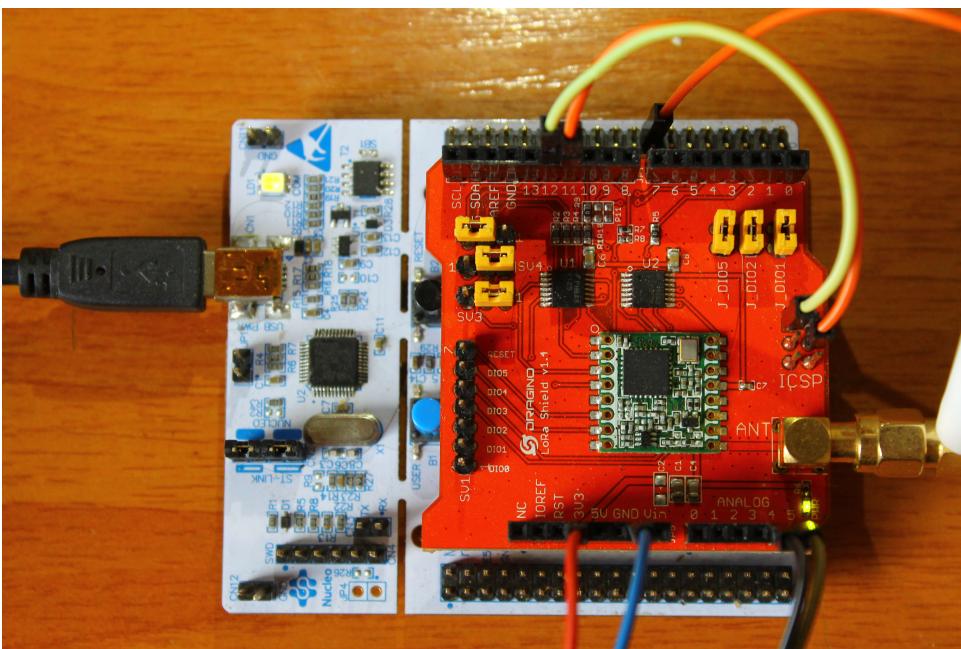
Konfigurace a adresy s typy všech koncových zařízení v LoRaWAN síti jsou uloženy v non-volatile paměti EEPROM gatewaye o kapacitě 6144 B. Paměť je tedy rozdělená tak, že od adresy 0 až po 6080 je prostor pro ukládání LoRaWAN zařízení a od 6080 až po 6144 je prostor pro ukládání konfigurace gatewaye.

Každé LoRaWAN zařízení v síti má v paměti uložené LoRaWAN device address (4 byty), typ zařízení (1 byte) a další 3 byty jsou rezervovány. Jedno koncové zařízení v paměti tedy zabírá 8 B, takže gateway má kapacitu paměti pro až 760 koncových zařízení.

4.8 Zapojení

LoRa shield [4] je nasazen přímo na vývojový kit Nukleo. Kit neobsahuje ISCP konektor, který je součástí pinoutu Arduino UNO a LoRa shield má SPI piny MISO a MOSI přivedeny právě na tento konektor. Musí být tedy propojeny externě viz obrázek 4.7. Jumpery na Dragino LoRa shieldu musí také být stejně jako v obrázku.

Pro komunikaci s LoRa transceiverem je tedy použito SPI1, pro komunikaci přes USB je použito USART2 a pro komunikaci přes RS485 je použito UART1.



Obrázek 4.7: foto zapojení

Periférie	Název pinu	Pin procesoru
RS485 transceiver	RX	PC1
	TX	PC0
	RTS	PB1
LoRa transceiver	CS	PB6
	CLK	PA5
	MISO	PA6
	MOSI	PA7
	RST	PC7
	DIO0	PA10

Tabulka 4.9: Pinout připojení externích periférií k procesoru

4.9 Naprogramování

K naprogramování MCU byla použita HAL knihovna a inicializační nástroj STM32CubeMX poskytnuté výrobcem, tedy ST Microelectronics. Zdrojové soubory programu byly vyvíjeny v textovém editoru VS-Code, ke komplikaci zdrojových souborů byl použit kompilátor arm-none-eabi-gcc a jako pomocný nástroj makefile skript.

4.9.1 Zdrojové soubory projektu

Pro šifrování LoRaWAN paketu byla použita knihovna AES-128, dostupná na githubu [5] a knihovna OpenPANA také dostupná z githubu [6]. Níže je

seznam zdrojových souborů.

Drivers	STM32 Drivers
Inc	Headers
aes.h	AES-128 library for LoRaWAN paket encryption
cmac.h	library for CMAC calculation in LoRaWAN protocol
LinkedList_ByteArray.h ..	Byte array linked list library for stacks
LoRaWAN_paket.h.....	LoRaWAN library for paket data decoding
stm32l0xx_hal_conf.h.....	HAL initialization of peripherals
ByteArray.h.....	Library for Byte array operations
LoRa.h	Library for interfacing LoRa transceiver
main.h	Main file
stm32l0xx_it.h	HAL initialization of peripherals
EEPROM.h.....	Library for eeprom operations
LoRa_sensors.h.....	Library for decoding data from payload
rs485_protocol.h	Library for RS485 IMA protocol
usb.h ...	Library for USB communication and system configuration
Src.....	Sources
aes.c	source file to the aes.h
aes.c	source file to the cmac.h
LinkedList_ByteArray.c	source file to the LinkedList_ByteArray.h
LoRaWAN_paket.c	source file to the LoRaWAN_paket.h
stm32l0xx_hal_msp.c	HAL source file
ByteArray.c	source file to the ByteArray.h
LoRa.c	source file to the LoRa.h
main.c	main source file
stm32l0xx_it.c	HAL source file
EEPROM.c	source file to the EEPROM.h
LoRa_sensors.c	source file to the LoRa_sensors.h
rs485_protocol.c	source file to the rs485_protocol.h
system_stm32l0xx.c	HAL source file
usb.h	source file to the usb.h

4.9.2 Nahrání programu do MCU

Výstupem komplikace je soubor s koncovkou .binary, který je nahrán do MCU. K tomuto nahrání není potřeba žádný speciální SW nebo HW. Stačí kit připojit k PC přes USB, v PC se kit zobrazí jako flash disk. Zkomplikovaný program s koncovkou .binary stačí překopírovat na toto zařízení. Po dobu kopírování souboru bliká na kitu LED1 červená/zelená. Jakmile kopírování skončí, program na kitu je spuštěn, případně je možné kit resetovat černým tlačítkem reset. Pro uvedení Gateweye do provozu je nutné se připojit k zařízení přes USB a nastavit všechny parametry viz sekce 4.5.2.

Kapitola 5

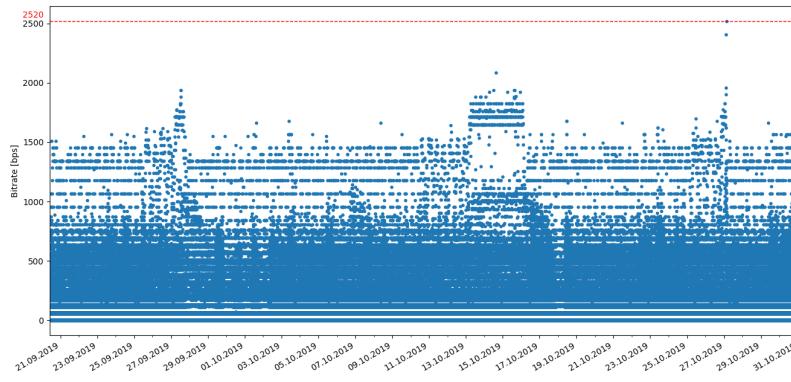
Měření výsledky a diskuse

One floor block of university building is selected to perform the test. It is equipped with twelve CKP devices, each controlling one Door Lock and one Reader. One Gateway is added to the infrastructure, i.e., thirteen devices are connected to one RS485 network. Two temperature/humidity sensor nodes are wirelessly connected to the Gateway. The Gateway and CKP devices are connected via RS485 network as shown in Fig. 2.1. The specific location of CKP devices, Gateway and two sensor nodes on the floor is shown in Fig. 4.2.

The long-term operation test is carried out from 21st September to 31th October, i.e., in the period involving the presence of students and employees in the classrooms and offices on the monitored floor of the university. During this period, the Control Panel received 1 876 978 packets (14 074 522 Bytes) and sent 1 101 556 packets (8 295 219 Bytes) from/to RS485 network. The lengths of all 2 978 534 packets, i.e., 22 369 741 Bytes, are recorded in RS485 network during long-term operation test and the frequency analysis method, i.e., the number of packet lengths in monitored period, is performed. Three packets reach the largest value, i.e., 40 Bytes. Considering the total amount of packets, it is negligible quantity, i.e., 1.3E-04%. However, given the nature of the system, i.e., the system with the primary function of access to a restricted area, the worst-case scenario is considered to be an uncrossable limit. Number of sensor nodes that can be wirelessly connected to the Gateway and does not affect the existing access control system, can be calculated in dependence on used RS485 data rate. The reserve of the data rate is considered in order to protect the access control system from malfunction, e.g., a long waiting for the door to open.

Based on the frequency analysis given in Tab. 5.1 and IMA know-how, 19 Bytes length packets transmit sensor data, and 7 Bytes length packets are general acknowledgement of IMA protocol. At least two packets are required to handle sensor data via RS485 network, i.e., one carrying sensor data and

Packet length	Count
7	2 216 098
8	619 127
9	3
11	58 393
13	58 620
16	1
18	2
19	26 286
23	1
40	3

Tabulka 5.1: Packet length frequency analysis**Obrázek 5.1:** Measured data rate in [bps] in RS485 network during long-term operation test

the other with acknowledgement.

During long term operation test, lengths of transmitted packets (l) are captured with the accuracy of timestamps of a thousandth of a second. Then resampled to one second resolution interval using the sum function to easily represent achieved data as a bit rate in bit per second (bps), Fig. 5.1. Red colored dashed line (with value of 2520 bps) shows one second time interval in which a sum of captured packets is transported in RS485 network. It shows, based on detailed knowledge of the IMA protocol, less than 20% of the RS485 network capacity is used.

To avoid RS485 network congestion the maximum number of sensor nodes S_{MAX} can be calculated as:

$$S_{MAX} = \frac{\frac{v_{485}}{B} - R}{P} \quad (5.1)$$

where:

v_{485} 485 network data rate [bps]
 B bits to Byte
 l_{MAX} maximal packet length
 R reserve of the data rate [%]
 P number of packets to transmit sensor data

Considering above mentioned limits, desired reserves and RS485 data rates, the maximum number of sensor nodes simultaneously transmitting their data on RS485 network is calculated, Tab. ??.

Values for calculation are:

v_{485} = RS485 network data rate
 B = 8
 l_{MAX} = 40
 P = 2

For example, WSN can connect up to 162 sensor nodes that work in RS485 network with a 115200 bps data rate and 10 % reserve, or up to 126 sensor nodes with a 115200 bps data rate and 30 % reserve. The results also show, one floor block of university building, i.e., one RS485 network, can operates dozens of sensors with sufficient reserve protecting the access control system from malfunction.

Kapitola 6

Závěr

In this paper, the conditions of extending an existing access control system running in an industry standardized RS485 network with a wireless sensor network based on LoRaWAN single-channel mode is discussed. Design of wireless sensor network is performed, i.e., the sensor nodes and one single-channel gateway based on LoRaWAN protocol are designed. The gateway represents a type of CKP device connected to the RS485 network, therefore it supports the existing protocol in the RS485 network. A long-term operation measurement is performed in one university floor infrastructure consisting of twelve CKP devices (pairs of card reader and door lock) and one gateway. Frequency analysis of packet lengths is performed and the biggest value of packet length is considered as well as the reserve of the RS485 data rate in order to protect the access control system from malfunction. Maximum number of wireless sensor nodes simultaneously transmitting data RS485 network is calculated in dependence on RS485 data rate and the reserve of data rate, e.g., 81 sensor nodes that work in RS485 network with a 57600 bps data rate and 10 % reserve. This number of sensor nodes significantly exceeds the actual needs of the sensor nodes on one floor block of university building. Therefore we can state that WSN is suitable for smart metering applications.

Literatura

- [1] H. Ali, W. Y. Chew, F. Khan and S. R. Weller, "Design and implementation of an IoT assisted real-time ZigBee mesh WSN based AMR system for deployment in smart cities," *2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE)*, Oshawa, ON, 2017, pp. 264-270. [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8052810> [Accessed: 9-Sep-2019].
- [2] T. Malche and P. Maheshwary, "Internet of Things (IoT) for building smart home system," *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, 2017, pp. 65-70. [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8058258> [Accessed: 9-Sep-2019].
- [3] K. Mekki, E. Bajic, F. Chaxel and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment". *ICT Express*, vol. 5, no. 1, March 2019. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2405959517302953> [Accessed: 9-Sep-2019].
- [4] M. Centenaro, L. Vangelista, A. Zanella and M. Zorzi, "Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios," in *IEEE Wireless Communications*, vol. 23, no. 5, pp. 60-67, October 2016. [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7721743> [Accessed: 9-Sep-2019].
- [5] A. Lavric and A. Ioan Petrariu, "High-Density Low Power Wide Area Networks," *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, Iasi, Romania, 2018, pp. 1-4. [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8678997> [Accessed: 9-Sep-2019].
- [6] A. Kosari and D. D. Wentzloff, "MURS Band for LPWAN Applications," *2019 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet)*, Orlando, FL, USA, 2019, pp. 1-3.

- [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8711814> [Accessed: 9-Sep-2019].
- [7] KRANZ, Maciej. The Internet of Things: 5 Predictions for 2018. CISCO: blog [Online]. Available: <https://blogs.cisco.com/innovation/the-internet-of-things-5-predictions-for-2018> [Accessed: 9-Sep-2019].
- [8] R. F. Fernandes, C. C. Fonseca, D. Brandão, P. Ferrari, A. Flammini and A. Vezzoli, "Flexible Wireless Sensor Network for smart lighting applications," 2014 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) Proceedings, Montevideo, 2014, pp. 434-439. [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6860782> [Accessed: 9-Sep-2019].
- [9] W. Huiyong, W. Jingyang and H. Min, "Building a Smart Home System with WSN and Service Robot," 2013 Fifth International Conference on Measuring Technology and Mechatronics Automation, Hong Kong, 2013, pp. 353-356. [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6493740> [Accessed: 9-Sep-2019].
- [10] Luo Hui, "A meter reading system based on WSN," 2010 International Conference on Optics, Photonics and Energy Engineering (OPEE), Wuhan, 2010, pp. 311-314. [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5508121> [Accessed: 9-Sep-2019].
- [11] M. J. Mudumbe and A. M. Abu-Mahfouz, "Smart water meter system for user-centric consumption measurement," 2015 IEEE 13th International Conference on Industrial Informatics (INDIN), Cambridge, 2015, pp. 993-998. [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7281870> [Accessed: 9-Sep-2019].
- [12] R. K. Kodali, "Radio data infrastructure for remote monitoring system using lora technology," 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, 2017, pp. 467-472. [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8125884> [Accessed: 9-Sep-2019].
- [13] N. Shah and P. S. Sundar, "Smart Electric Meter Using LoRA Protocols and lot applications," 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, 2018, pp. 1178-1180. [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8474749> [Accessed: 9-Sep-2019].
- [14] C. Yoon, M. Huh, S. Kang, J. Park and C. Lee, "Implement smart farm with IoT technology," 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon-si Gangwon-do, Korea (South), 2018, pp. 749-752. [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8323908> [Accessed: 9-Sep-2019].

- [15] Know about Access Control Systems and Their Types with Features. *Electronics projects focus* [Online]. Available: <https://www.elprocus.com/understanding-about-types-of-access-control-systems/> [Accessed: 9-Sep-2019].
- [16] D. Singh, O. G. Aliu and M. Kretschmer, "LoRa WanEvaluation for IoT Communications," *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Bangalore, 2018, pp. 163-171. [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8554713> [Accessed: 9-Sep-2019].
- [17] LoRa Alliance, "LoRaWAN 1.1 Specification", version 1.1, October 11, 2017 [Online]. Available: https://lora-alliance.org/sites/default/files/2018-04/lorawantm_specification_-v1.1.pdf [Accessed: 9-Sep-2019].
- [18] A. Zourmand, A. L. Kun Hing, C. Wai Hung and M. AbdulRehman, "Internet of Things (IoT) using LoRa technology," *2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)*, Selangor, Malaysia, 2019, pp. 324-330. [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8825008> [Accessed: 9-Sep-2019].
- [19] N. H. Abd Rahman, Y. Yamada, M. H. Husni and N. H. Abdul Aziz, "Analysis of Propagation Link for Remote Weather Monitoring System through LoRa Gateway," *2018 2nd International Conference on Telematics and Future Generation Networks (TAFGEN)*, Kuching, 2018, pp. 55-60. [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8580479> [Accessed: 9-Sep-2019].
- [20] RisingHF, "Outdoor IP64 Temperature and Humidity LoRaWAN sensor RHF1S001", version 1.2, 2015 [Online]. Available: http://www.objenious.com/wp-content/uploads/2016/10/RHF-DS015880utdoor-IP64-Tempratrure-and-Humidity-LoRaWAN-Sensor-RHF1S001_V1.3.pdf [Accessed: 9-Sep-2019].
- [21] *NUCLEO-L073RZ*. ST Microelectronics [Online]. Available: <https://www.st.com/en/evaluation-tools/nucleo-l073rz.html> [Accessed: 20-Sep-2019].
- [22] *RFM95/96/97/98(W) - Low Power Long Range Transceiver Module*. HopeRF electronic. V1.0. [Online]. Available: http://wiki.dragino.com/index.php?title=Lora_Shield [Accessed: 20-Sep-2019].
- [23] *Lora Shield*. Dragino. [Online]. Available: http://wiki.dragino.com/index.php?title=Lora_Shield [Accessed: 20-Sep-2019].
- [24] *SparkFun Transceiver Breakout - RS-485*. Sparkfun. [Online]. Available: <https://www.sparkfun.com/products/10124> [Accessed: 20-Sep-2019].

- [1] *NUCLEO-L073RZ*. ST Microelectronics [Online]. Available: <https://www.st.com/en/evaluation-tools/nucleo-1073rz.html> [Accessed: 20-Sep-2019].
- [2] *NUCLEO-L073RZ* ARM Mbed. [Online]. Available: <https://os.mbed.com/platforms/ST-Nucleo-L073RZ/> [Accessed: 20-Sep-2019].
- [3] *RFM95/96/97/98(W) - Low Power Long Range Transceiver Module*. HopeRF electronic. V1.0. [Online]. Available: http://wiki.dragino.com/index.php?title=Lora_Shield [Accessed: 20-Sep-2019].
- [4] *Lora Shield*. Dragino. [Online]. Available: http://wiki.dragino.com/index.php?title=Lora_Shield [Accessed: 20-Sep-2019].
- [5] *tiny-AES128-C* bitdust. [Online]. Available: <https://github.com/bitdust/tiny-AES128-C> [Accessed: 20-Sep-2019].
- [6] *openpana*. OpenPANA. [Online]. Available: <https://github.com/OpenPANA/openpana> [Accessed: 20-Sep-2019].
- [7] *SparkFun Transceiver Breakout - RS-485* Sparkfun. [Online]. Available: <https://www.sparkfun.com/products/10124> [Accessed: 20-Sep-2019].
- [8] *LoRaWAN Specification*. LoRa Alliance. v1.1. Sparkfun. [Online]. Available: <https://lora-alliance.org/resource-hub/lorawan™-specification-v11> [Accessed: 20-Sep-2019].
- [9] Robert Miller. *LoRa Security Building a Secure LoRa Solution*. MWR Labs Whitepaper. [Online]. Available: <https://labs.mwrinfosecurity.com/assets/BlogFiles/mwri-LoRa-security-guide-1.2-2016-03-22.pdf> [Accessed: 20-Sep-2019].
- [10] [Online]. Available: <https://www.elprocus.com/understanding-about-types-of-access-control-systems/> [Accessed: 9-Sep-2019].
- [11] [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8678997> [Accessed: 9-Sep-2019].
- [12] [Online]. Available: <https://blogs.cisco.com/innovation/the-internet-of-things-5-predictions-for-2018> [Accessed: 9-Sep-2019].
- [13] [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8711814> [Accessed: 9-Sep-2019].
- [14] [Online]. Available: <https://reader.elsevier.com/reader/sd/pii/S2405959517302953?token=1D12BD2186DD8FA9065DCE9301C63D4D2F67C3557C4677D06FCE5DBB92C96984BFCF132B6DD37ED892EAF> [Accessed: 9-Sep-2019].
- [15] [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7721743> [Accessed: 9-Sep-2019].

- [16] [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8323908> [Accessed: 9-Sep-2019].
- [17] [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8125884> [Accessed: 9-Sep-2019].
- [18] [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5453569> [Accessed: 9-Sep-2019].
- [1] *RF.* IQRF Alliance.
[Online]. Available: <https://www.iqrf.org/technology/rf> [Accessed: 9-Jun-2018].
- [1] *RF.* IQRF Alliance.
[Online]. Available: <https://www.iqrf.org/technology/iqrf-ide> [Accessed: 9-Jun-2018].
- [2] *IQRF SDK.* IQRF Alliance. [Online]. Available: <https://www.iqrf.org/technology/iqrf-sdk> [Accessed: 9-Jun-2018].
- [3] *Transceivers.* IQRF Alliance.
[Online]. Available: <https://www.iqrf.org/products/transceivers> [Accessed: 9-Jun-2018].
- [4] *Three security levels in new IQRF OS 4.0.* IQRF Alliance.
[Online]. Available: <https://www.iqrfalliance.org/news/117-three-security-levels-in-new-iqrf-os-4-0> [Accessed: 9-Jun-2018].
- [5] *Wireless Meter Bus, WM-Bus Technology.* Radio-Electronics. [Online]. Available: <http://www.radio-electronics.com/info/wireless/wireless-m-bus/basics-tutorial.php> [Accessed: 9-Jun-2018].
- [6] *Wireless M-Bus in Industrial Wireless Sensor Networks.* Radiocrafts.
[Online]. Available: <https://radiocrafts.com/technologies/wireless-m-bus-technology-overview/> [Accessed: 9-Jun-2018].
- [7] Radiocrafts: *WirelessM-Bus in Industrial Sensor Networks.*
[Online]. Available: https://radiocrafts.com/uploads/AN024_Using_Wireless_M-BUS_in_Industrial_Sensor_Networks_1_0.pdf [Accessed: 9-Jun-2018].
- [8] Silicon labs: *WIRELESS M-BUS SOFTWARE IMPLEMENTATION.*
[Online]. Available: <https://www.silabs.com/documents/public/application-notes/AN451.pdf> [Accessed: 9-Jun-2018].
- [9] Compass security: *Wireless M-Bus Security Whitepaper Black Hat USA 2013.* June 30th. 2013, v1.01. [Online]. Available: https://www.compass-security.com/fileadmin/Datein/Research/Praesentationen/blackhat_2013_wmbus_security_whitepaper.pdf [Accessed: 9-Jun-2018].

- [10] *Zigbee*. Wikipedia. [Online]. Available: <https://en.wikipedia.org/wiki/Zigbee> [Accessed: 9-Jun-2018].
- [11] Xueqi Fan, Fransisca Susan, William Long, Shangyan Li: *Security Analysis of Zigbee*. May 18, 2017. [Online]. Available: <https://courses.csail.mit.edu/6.857/2017/project/17.pdf> [Accessed: 9-Jun-2018].
- [12] *The Zigbee Alliance*. Zigbee alliance. [Online]. Available: <http://www.zigbee.org/zigbee-for-developers/about-us/> [Accessed: 9-Jun-2018].
- [13] *Bluetooth sensor network*. mikroelektronika. [Online]. Available: <https://www.mikroe.com/blog/bluetooth-sensor-network> [Accessed: 9-Jun-2018].
- [14] *Dispelling Common Bluetooth Misconceptions*. Sans technology institute. [Online]. Available: <https://www.sans.edu/cyber-research/security-laboratory/article/bluetooth> [Accessed: 9-Jun-2018].
- [15] *Bluetooth radio interface, modulation, & channels*. Radioelectronics. [Online]. Available: <http://www.radio-electronics.com/info/wireless/bluetooth/radio-interface-modulation.php> [Accessed: 9-Jun-2018].
- [16] Kianoosh Karami: *BLE Packet*. Punch through. November 07 2016. [Online]. Available: <https://punchthrough.com/blog/posts/maximizing-ble-throughput-part-2-use-larger-att-mtu> [Accessed: 9-Jun-2018].
- [17] *LoRa Wireless for M2M & IoT*. Radioelectronics. [Online]. Available: <http://www.radio-electronics.com/info/wireless/lora/basics-tutorial.php> [Accessed: 9-Jun-2018].
- [18] *LoRa Network: LoRaWAN*. Radioelectronics. [Online]. Available: <http://www.radio-electronics.com/info/wireless/lora/lorawan-network-architecture.php> [Accessed: 9-Jun-2018].
- [19] *Understanding the Limits of LoRaWAN*. IEEE. Communications Magazine. January 2017 [Online]. Available: <https://arxiv.org/pdf/1607.08011.pdf> [Accessed: 9-Jun-2018].
- [20] BRIAN RAY: *Use Cases and Considerations for LoRaWAN*. Link-labs. June 20, 2016. [Online]. Available: <https://www.link-labs.com/blog/use-cases-and-considerations-for-lorawan> [Accessed: 9-Jun-2018].
- [21] *LoRa Physical Layer & RF Interface*. Radioelectronics. [Online]. Available: <http://www.radio-electronics.com/info/wireless/lora/rf-interface-physical-layer.php> [Accessed: 9-Jun-2018].

- [22] Kianoosh Karami: *BLE Packet Punch through*. November 07, 2016. [Online]. Available: <https://punchthrough.com/blog/posts/maximizing-ble-throughput-part-2-use-larger-att-mtu> [Accessed: 9-Jun-2018].
- [23] *Build your own gateway*. The things network. [Online]. Available: <https://www.thethingsnetwork.org/docs/gateways/start/build.html> [Accessed: 9-Jun-2018].
- [24] *LoraWAN in Europe*. Match X. [Online]. Available: <https://matchx.io/community/eu/12-lorawan-in-europe> [Accessed: 9-Jun-2018].
- [25] Ian Poole: *SIGFOX for M2M & IoT*. Radioelektronics. [Online]. Available: <http://www.radio-electronics.com/info/wireless/sigfox/basics-tutorial.php> [Accessed: 9-Jun-2018].
- [26] *SIGFOX for white paper security*. Sigfox. February 2017. [Online]. Available: https://www.sigfox.com/sites/default/files/1701-SIGFOX-White_Paper_Security.pdf [Accessed: 9-Jun-2018].
- [27] *Z-Wave*. Z-wave Alliance. [Online]. Available: <http://www.z-wave.com/about> [Accessed: 9-Jun-2018].
- [28] *Z-Wave*. Wikipedia. [Online]. Available: <https://en.wikipedia.org/wiki/Z-Wave> [Accessed: 9-Jun-2018].
- [29] *What is thread*. Thread group. [Online]. Available: <https://www.threadgroup.org/What-is-Thread> [Accessed: 10-Jun-2018].
- [30] *Thread (network protocol)*. Wikipedia. [Online]. Available: [https://en.wikipedia.org/wiki/Thread_\(network_protocol\)](https://en.wikipedia.org/wiki/Thread_(network_protocol)) [Accessed: 10-Jun-2018].
- [31] *Experimental Study of Thread Mesh Network for Wireless Building Automation Systems*. EXAMENSARBETE INOM ELEKTROTEKNIK. STOCKHOLM. SVERIGE 2016. [Online]. Available: <http://www.diva-portal.org/smash/get/diva2:1040491/FULLTEXT02> [Accessed: 10-Jun-2018].
- [32] *RPMA TECHNOLOGY*. Internet of things. [Online]. Available: https://theinternetofofthings.report/Resources/Whitepapers/4cbc5e5e-6ef8-4455-b8cd-f6e3888624cb_RPMA%20Technology.pdf [Accessed: 10-Jun-2018].
- [33] *RPMA*. Ublox. [Online]. Available: <https://www.u-blox.com/en/rpma> [Accessed: 10-Jun-2018].
- [34] *RPMA TECHNOLOGY*. Ingenu. [Online]. Available: <https://www.ingenu.com/technology/rpma/> [Accessed: 10-Jun-2018].