



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 zkratk	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
3.1.2 Wireless M-Bus	9
3.1.3 LoRa	9
3.1.4 Zigbee	9
3.1.5 BLE	10
3.2 Shrnutí vlastností vybraných technologií	10
3.3 Vybraná přenosová technologie .	11

Část II

Practical part

4 Realizace zařízení	14
4.1 Implementace WSN do přístupového systému	14
4.2 Návrh WSN gatewaye	15
4.2.1 Komunikace přes sériovou linku	16
4.3 Log Gatewaye	17
4.3.1 Přidávání koncových zařízení ze serveru řízení přístupu K4	18
4.3.2 Nahrání programu do MCU .	18
5 Měření výsledky a diskuse	19
6 Závěr	22
Literatura	23

Obrázky

2.1 Příklad architektury přístupového systému [1110]	6
4.1 IMA access control system architecture with WSN extension .	15
5.1 Measured data rate in [bps] in RS485 network during long-term operation test	20

Tabulky

3.1 Souhrn porovnání parametrů kandidátní bezdrátových technologií	10
4.1 Parametry sériové linky PC terminálu pro komunikaci s gatewayí	16
5.1 Packet length frequency analysis	20

■ 0.1 Seznam zkratek

AI	Artificial Intelligence
AppSKey	Application Session Key
BLE	Bluetooth Low Energy
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) [1114]. 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 [1115] and can have one of the following topologies: star (centralized), star of stars (decentralized) and mesh (distributed) [1111]. 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 [1113].

The industry of IoT is growing because of its enormous potential. Cisco study [1112] 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 [1117]. 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 [1116] 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 ment 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.

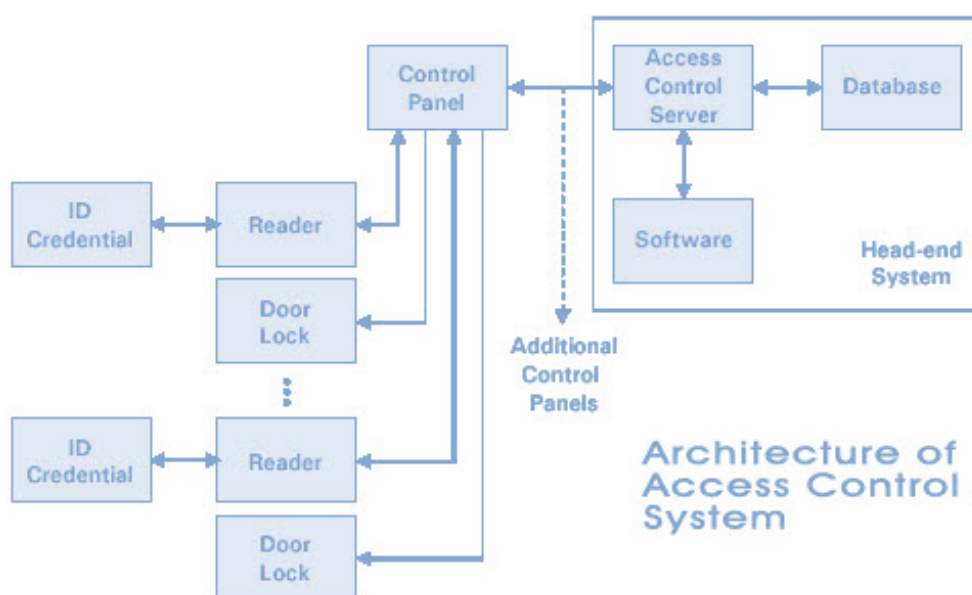
Část I

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 [1110]

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 rozhraní mezi serverem řízení přístupu (Access Control Server) a páry čteček a zámků dveří. kontrolní panely jsou obvykle připojeny k serveru řízení přístupu přes TCP/IP síť a páry čtečka a zámků dveří jsou obvykle připojeny ke kontrolnímu panelu přes RS485 síť. Databáze obsahuje všechna uživatelské

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 musí používat pouze bezlicenční pásmo ISM a musí umožňovat implementaci celé sítě bez závislosti na síti třetích stran.

3.1 Kandidátní bezdrátové technologie

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

3.1.1 IQRF

IQRF je technologie vyvinuta IQRF aliancí [20], která je jediným výrobcem IQRF transceiveru [19] za cenu v rozsahu \$15-20 za kus a k tomu poskytuje nástroje jako je SDK [18] a IDE [17]. Technologie IQRF bývá použita k realizaci sítí o topologii typu mesh nebo hvězdice. Jedna síť má jednoho koordinátora, který slouží jako gateway a může obsahovat až 240 zařízení (včetně koordinátora). Pro požadavek vyššího počtu zařízení je efektivnější zřetěžit více sítí, s jednotlivými koordinátory a různými RF kanály pro vyšší propustnost. Dosah na přímou viditelnost je až 500 m a velikost payloadu jednoho packetu může být až 64 B. Z hlediska kritérií pro tento projekt je u této technologie nevýhodou nízký počet zařízení třetích stran dostupných na trhu. Většinou je tato technologie použita pro realizaci uživatelsé sítě, kde gateway je použita jedna z dostupných od IQRF aliance a koncová zařízení

sítě jsou vytvořena vývojáři s použitím transceiverů od IQRF aliance [21].

■ 3.1.2 Wireless M-Bus

Wireless M-Bus (Meter-Bus) je standard specifikovaný v evropské normě EN 13757, popisující fyzickou, síťovou a aplikační vrstvu, původně navržen pro aplikace bezdrátového měření jako rozšíření průmyslové datové sběrnice M-Bus [24]. Po několika letech v průmyslu bezdrátových měřících systémů se tato technologie rozšířila do oblasti průmyslu senzorových sítí. Komunikace koncových zařízení je rozdělena do několika módů v závislosti na orientaci komunikace a objemu vysílaných dat [22] [23]. Wireless M-Bus síť má hvězdicovou topologii o dosahu 500 m v pásmu 868 MHz. Komunikaci vždy zahajuje koncové zařízení, které koncentrátor obsluhuje. Transceivery vyrábí více různých firem za cenu okolo \$25-30 za kus.

■ 3.1.3 LoRa

LoRa (Long Range) je modulace navržena firmou Semtech. LoRaWAN je otevřený standardizovaný síťový protokol a systémová architektura navržen LoRa Aliancí definovaný v LoRaWAN Specification [33] vytvářející MAC (media access control) vrstvu nad fyzickou vrstvou LoRa se zabezpečením přenášených dat. Síť má hvězdicovou topologii, kde komunikaci zahajuje koncové zařízení a koncentrátor ho obsluhuje. Pro nízkou spotřebu protokol umožňuje ladit SF (Spreading Factor) neboli přenosovou rychlost, pro regulaci dosahu, který je až 15-22 km mimo městskou část a 3-8 km ve městské části [33]. V některých oblastech některé firmy poskytují pokrytí LoRaWAN sítí a proto je tato technologie velmi populární. Na trhu je mnoho koncových zařízení i gatewayí, s jejichž vzájemnou kompatibilitou není problém. Gateway přeposílá přijaté packety s daty z koncových zařízení na server, kde je payload zpracován na základě dokumentace od výrobce daného koncového zařízení. Semtech je jediným výrobcem integrovaných obvodů podporujících LoRa modulaci. Na trhu je dostupných mnoho transceiverů, které používají tento integrovaný obvod, některé dokonce obsahují implementovaný LoRaWAN stack. Transceiver pro gateway má cenu okolo \$130 a umožňuje současně přijímat packety od koncových zařízení na více kanálech a přenosových rychlostech. Je zde i možnost udělat jednokanálovou gateway, která je schopna přijímat v jednu chvíli pouze jedním kanálem a jedné přenosové rychlosti s použitím transceiveru pro koncová zařízení za cenu okolo \$5-20. V takové síti pak musí být všechna koncová zařízení nakonfigurována na jednu konkrétní frekvenci a přenosovou rychlost.

■ 3.1.4 Zigbee

Zigbee je specifikace navržena pro IoT aplikace, založena na standardu IEEE 802.15.4, vyvinuta Zigbee aliancí [29]. Technologii Zigbee podporuje

topologie mesh a hvězdice, většinou je použita topologie mesh pro rozšíření dosahu sítě, který je mezi dvěma zařízeními do 300 m na přímou viditelnost a 75 až 100 m v budově [30]. Jedna síť může obsahovat až 65000 zařízení. Dostupné transceivery na trhu se pohybují okolo \$8–30 od více různých výrobců, taktéž je i na trhu dostupných mnoho Zigbee koncových zařízení.

3.1.5 BLE

Bluetooth Low Energy (BLE) je verze Bluetooth navržena pro minimální spotřebu energie, podporující topologie point-to-point, broadcast a mesh [31]. Dosah mezi dvěma zařízeními je až 100 m [32]. Dostupné transceivery na trhu se pohybují okolo \$5–20 od více různých výrobců. Stejně tak je i na trhu mnoho dostupných koncových zařízení, ale mnohdy jsou tato koncová zařízení kompatibilní pouze se zařízení v rámci jednoho výrobce, tudíž může být problém je implementovat do vlastní senzorové sítě.

3.2 Shrnutí vlastností vybraných technologií

V tabulce 3.1 jsou shrnuty vlastnosti zmíněných technologií.

	IQRF	Wireless M-bus	LoRa	ZigBee	BLE
topology	mesh, star	star	star	mesh, star	Point-to-Point, Broadcast, Mesh
maximum size of packet	64 B	256 B	256 B	133 B	20 B (Bluetooth 4.0), 251 B (Bluetooth 4.2)
data rate	19.2 kb/s	32.768 – 100 kb/s	0.3–50 kb/s	250 kb/s	up to 1 Mb/s
band (Europe)	868 MHz	868 MHz	868 MHz	2.4 GHz	2.4 GHz
range	500 m (line of sight)	500 m (line of sight)	15–22 km suburban, 3–8 km urban	300 m (line of sight), 75–100 m (indoor)	100 m (class 1), 10 m (class 2), less than 10 m (class 3)
security	AES-128	AES-128	AES-128	AES-128	AES-128
max radio output power	up to 8 mW	0.16–20 mW	24 mW	1–100 mW	100 mW (class 1), 5 mW (class 2), 1 mW (class 3)

Tabulka 3.1: Souhrn porovnání parametrů kandidátní bezdrátových technologií

■ 3.3 Vybraná přenosová technologie

Pro tento projekt byla vybrána technologie LoRa se standardizovaným síťovým protokolem LoRaWAN v jednokanálovém módu, jako je to používáno ve vývojových projektech [19], tudíž není to plně LoRaWAN kompatibilní. V jednokanálovém módu jsou všechna zařízení v síti nakonfigurována na jeden konkrétní kanál a přenosovou rychlost. Výhoda použití této technologie v jednokanálovém módu je, že gateway může použít transceiver určen pro koncová zařízení, který je víc jak desetkrát levnější a vyžaduje nižší výkon CPU než transceiver pro gateway, tudíž gateway v jednokanálovém módu je mnohem jednodušší a levnější řešení. LoRaWAN koncová zařízení třetích stran jsou plně kompatibilní s jakoukoliv LoRaWAN gatewayí pro daný region, tudíž mohou být implementovány do navrženého systému v tomto projektu, ale musí být překonfigurována ke komunikaci na zvoleném kanále a přenosové rychlosti.

Část II

Practical part

Kapitola 4

Realizace zařízení

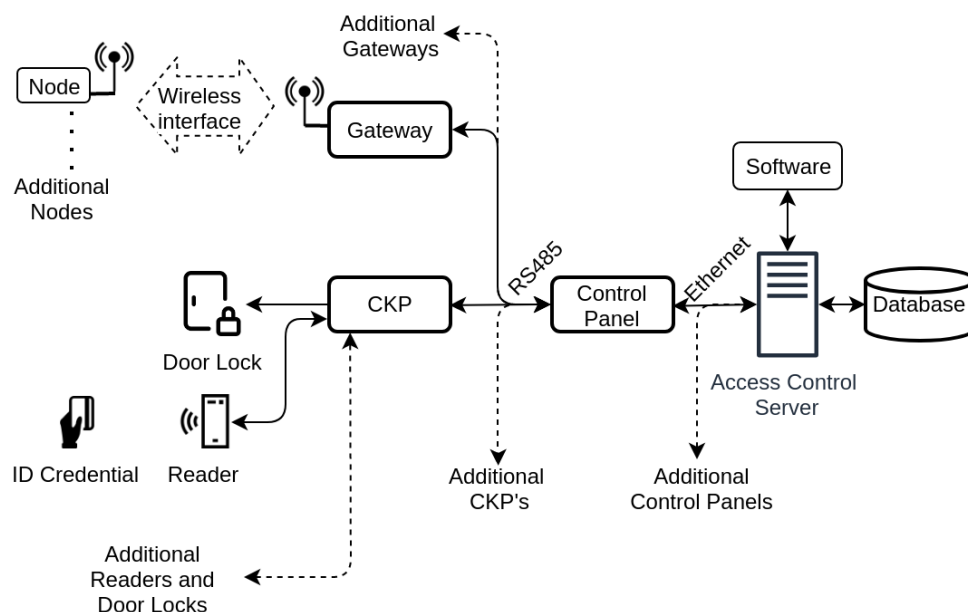
4.1 Implementace WSN do přístupového systému

Přístupový systém k rozšíření o WSN pro tento projekt je vytvořen firmou IMA a je komerčně distribuován. Jeho architektura se liší od všeobecné architektury zobrazené v blokovém schématu 2.1 přidáním zařízení CKP, tvořícího rozhraní mezi kontrolním panelem a čtečkou s dveřním zámkem. Přístupový systém má několik typů CKP zařízení podporujících různé typy čteček, dveřních zámků, závor, vrat apodobně, ale všechna tato CKP zařízení podporují CKP protokol v síti RS485 pro komunikaci s kontrolním panelem.

Rozšíření tohoto Přístupového systému o WSN je vytvořeno připojením WSN gatewaye ke kontrolnímu panelu přes RS485 síť stejně jako CKP zařízení. Názorná blokové schéma přístupového systému firmy IMA s implementací WSN gatewaye je zobrazeno v obrázku 4.1. V budovách, kde již je tento přístupový systém nainstalován je obvykle více kontrolních panelů, vždy jeden kontrolní panel pro několik dveří s CKP zařízeními propojenými sítí RS485. K jednomu přístupovému systému je možné připojit několik WSN gatewayů k libovolným kontrolním panelům v budově pro dosažení požadovaného pokrytí WSN.

WSN gateway tedy musí podporovat CKP protokol v síti RS485 navržený firmou IMA. Jedná se o kolizní protokol, kde všechna zařízení se řídí pravidlem "listen before talk", kolize jsou detekovány mechanismem kontroly integrity použitý v každé zprávě. V případě že zařízení přijme poškozený příkaz, vyžádá jeho opakování.

Přístupový systém firmy IMA funguje tak, že CKP zařízení získává seznam všech platných karet (ID Credentials) ze serveru řízení přístupu a na základě tohoto seznamu pak CKP zařízení provádí odpovídající akci po přiložení



Obrázek 4.1: IMA access control system architecture with WSN extension

karty ke čtečce. Je-li ke čtečce přiložena karta, jejíž číslo není obsaženo v seznamu platných karet, CKP zařízení pouze signalizuje událost uživateli (např. červené bliknutí nebo pípnutí), ale zprávu o této události neodesílá na server řízení přístupu. Je-li ke čtečce přiložena karta, jejíž číslo je obsaženo v seznamu platných karet, CKP zařízení signalizuje událost uživateli (např. zelené bliknutí nebo pípnutí) a zprávu o této události odesílá na server řízení přístupu příkazem tzv. "průchod". Navržená gateway bere seznam platných karet jako seznam platných koncových zařízení senzorové sítě. Gateway pak zpracovává packety pouze od zařízení z tohoto seznamu a ostatní ignoruje, tudíž v síti RS485 jsou přenášena pouze relevantní data. Data z koncových zařízení jsou odesílána na server řízení přístupu příkazem "průchod", který má fixní velikost a po přidání adresy koncového zařízení o velikosti 4 B zde už zbývá poze 6 B pro data z koncového zařízení, což je velké omezení. LoRaWAN protokol používá packet, jehož samotná hlavička je o minimální velikosti 13 B. Různá LoRaWAN koncová zařízení používají různé velikosti payloadu, takže není možné odesílat celý payload koncového zařízení přes síť RS485. Tento problém je řešen tak, že LoRaWAN packety z koncových zařízení jsou dešifrovány přímo v gatewayi a konečné hodnoty senzorů jsou vypočítány z payloadu zařízení na základě dokumentace poskytnuté výrobcem [20]. Vybrané hodnoty jsou odeslány na server řízení přístupu skrze kontrolní panel.

4.2 Návrh WSN gatewaye

Jak již bylo zmíněno v předchozí sekci, gateway dešifruje packety z koncových zařízení a na základě typu koncového zařízení vypočítává z

payloadu hodnoty senzorů z nichž vybrané odesílá na server řízení přístupu přes kontrolní panel a to z důvodu datového omezení protokolu v síti RS485, do které je gateway připojena. Pro každý podporovaný typ koncového zařízení musí být implementováno zpracování payloadu ve FW gatewaye. Pozdější přidání typů koncových zařízení tedy vyžaduje update FW gatewaye. Gateway tedy má uloženou informaci o typu koncového zařízení společně s jeho LoRaWAN device address.

LoRaWAN protokol je zabezpečen šifrováním AES-128 na dva způsoby, a to zabezpečení aplikační pro nečitelnost přenášených dat a síťové pro zabránění pro zabránění útočníkům opakovat již přenesené pakety nebo odesílat falešné pakety. Jsou zde tedy dva AES-128 šifrovací klíče, aplikační klíč AppSKey (Application Session Key) a síťový klíč NwKSKey (Network Session Key).

Jelikož adresy koncových zařízení jsou předávány gatewayi stejně jako platné karty čteče z aplikace na serveru řízení přístupu, není zde možnost předávat dva 16 B dlouhé šifrovací klíče pro každé koncové zařízení společně s adresou zařízení. Gateway tedy má tyto dva klíče pro všechna zařízení stejné, uložené v non-volatile paměti, konfigurovatelné pouze přímo na gatewayi. V tomto návrhu není implementován opačný směr komunikace, tedy ze serveru řízení přístupu na koncové zařízení, ale je také možné implementovat pro ovládání aktuatorů, jako je relé, motor, apod.

■ Stavba gatewaye

■ 4.2.1 Komunikace přes sériovou linku

Gateway má implementovanou komunikaci přes sériovou linku, umožňující konfiguraci a log. K připojení lze použít PC s libovolnou aplikací umožňující obousměrnou komunikaci přes sériovou linku s nastavením parametrů dle tabulky 4.1.

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

Tabulka 4.1: Parametry sériové linky PC terminálu pro komunikaci s gatewayí

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

4.3 Log Gateway

Po připojení ke gatewayi přes sériovou linku dle instrukcí v sekci Komunikace přes sériovou linku je možné kontinuálně snímat a log gatewaye obsahující informace o proběhlých událostech. Níže je příklad výpisu logu pro případ, že gateway přijala LoRaWAN paket z koncového zařízení senzorové sítě, zpracovala ho a výslednou informaci odeslala na kontrolní panel přes RS485 síť.

```
Rx -> LoRaWAN, pktCnt: 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: "FF1F100D00D0F61F01281A0934CDFFFF09202E"

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

Nejprve jsou vypsaná data týkající se LoRaWAN protokolu, zašifrovaný i dešifrovaný payload, typ zařízení a konečné informace dekodované 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.

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

4.3.1 Přidávání koncových zařízení ze serveru řízení přístupu K4

4.3.2 Nahrání programu do MCU

Kapitola 5

Měření výsledky a diskuse

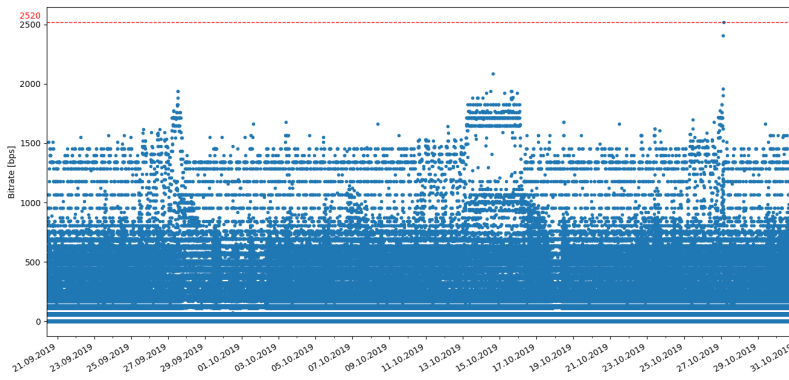
One floor block of university building is selected to perform the test. It is equipped with twelve CKP devices, each controlling one Door Lock and one Reader. One Gateway is added to the infrastructure, i.e., thirteen devices are connected to one RS485 network. Two temperature/humidity sensor nodes are 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. ??.

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 acknowledgements 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 operate 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] *RF*. IQRF Alliance. [Online]. Available: <https://www.iqrf.org/technology/rf> [Accessed: 9-Jun-2018].
- [17] *RF*. IQRF Alliance. [Online]. Available: <https://www.iqrf.org/technology/iqrf-ide> [Accessed: 9-Jun-2018].
- [18] *IQRF SDK*. IQRF Alliance. [Online]. Available: <https://www.iqrf.org/technology/iqrf-sdk> [Accessed: 9-Jun-2018].
- [19] *Transceivers*. IQRF Alliance. [Online]. Available: <https://www.iqrf.org/products/transceivers> [Accessed: 9-Jun-2018].
- [20] *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].
- [21] [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8399666> [Accessed: 9-Sep-2019].
- [22] *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].
- [23] *Wireless M-Bus in Industrial Wireless Sensor Networks*. Radiocrafts. [Online]. Available: <https://radiocrafts.com/technologies/wireless-m-bus-technology-overview/> [Accessed: 9-Jun-2018].
- [24] [Online]. Available: <https://automatizace.hw.cz//sbernice-wireless-mbus-jde-i-bezdratove> [Accessed: 9-Jun-2018].
- [25] Silicon labs: *WIRELESS M-BUS SOFTWARE IMPLEMENTATION*. [Online]. Available: <https://www.silabs.com/documents/public/application-notes/AN451.pdf> [Accessed: 9-Jun-2018].
- [26] 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].
- [29] *The Zigbee Alliance*. Zigbee alliance. [Online]. Available: <http://www.zigbee.org/zigbee-for-developers/about-us/> [Accessed: 9-Jun-2018].

- [30] *The Zigbee Alliance*. Zigbee alliance. [Online]. Available: <https://zigbeealliance.org/solution/zigbee/> [Accessed: 9-Jun-2018].
- [31] *BLE Packet*. [Online]. Available: <https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/radio-versions/> [Accessed: 9-Jun-2018].
- [32] *BLE Packet*. [Online]. Available: <https://blog.nordicsemi.com/getconnected/things-you-should-know-about-bluetooth-range> [Accessed: 9-Jun-2018].
- [33] LoRa Alliance, "LoRaWAN 1.1 Specification", version 1.1, October 11, 2017 [Online]. Available: https://loro-alliance.org/sites/default/files/2018-04/lorawantm_specification_v1.1.pdf [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-DS015880outdoor-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].
- [112] *NUCLEO-L073RZ* ARM Mbed. [Online]. Available: <https://os.mbed.com/platforms/ST-Nucleo-L073RZ/> [Accessed: 20-Sep-2019].
- [114] *Lora Shield*. Dragino. [Online]. Available: http://wiki.dragino.com/index.php?title=Lora_Shield [Accessed: 20-Sep-2019].
- [115] *tiny-AES128-C* bitdust. [Online]. Available: <https://github.com/bitdust/tiny-AES128-C> [Accessed: 20-Sep-2019].

- [116] *openpana*. OpenPANA. [Online]. Available: <https://github.com/OpenPANA/openpana> [Accessed: 20-Sep-2019].
- [117] *SparkFun Transceiver Breakout - RS-485* Sparkfun. [Online]. Available: <https://www.sparkfun.com/products/10124> [Accessed: 20-Sep-2019].
- [119] 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].
- [1110] [Online]. Available: <https://www.elprocus.com/understanding-about-types-of-access-control-systems/> [Accessed: 9-Sep-2019].
- [1111] [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8678997> [Accessed: 9-Sep-2019].
- [1112] [Online]. Available: <https://blogs.cisco.com/innovation/the-internet-of-things-5-predictions-for-2018> [Accessed: 9-Sep-2019].
- [1113] [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8711814> [Accessed: 9-Sep-2019].
- [1114] [Online]. Available: <https://reader.elsevier.com/reader/sd/pii/S2405959517302953?token=1D12BD2186DD8FA9065DCE9301C63D4D2F67C3557C4677D06FCE5DBB92C96984BFCF132B6DD37ED892EAF> [Accessed: 9-Sep-2019].
- [1115] [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7721743> [Accessed: 9-Sep-2019].
- [1116] [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8323908> [Accessed: 9-Sep-2019].
- [1117] [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8125884> [Accessed: 9-Sep-2019].