



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: doc. Ing. Lukáš Vojtěch, Ph.D
Obor: Elektronika a komunikace
Studijní program: Elektronika
Říjen 2019

Poděkování | **Prohlášení**

Abstrakt

todo

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

Vedoucí: Ing. Bc. Marek Neruda, Ph.D

Abstract

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

Title translation: Wireless sensor
network for access control system

Obsah

Seznam zkratek 1

Seznam zkratek 1

1 Úvod **3**

Část I Theoretical part

2 Architektury přístupových systémů **6**

3 Výběr bezdrátové technologie pro senzorovou síť **8**

3.1 Hlavní kritéria pro výběr bezdrátové technologie 8

3.2 Kandidátní bezdrátové technologie 9

IQRF 9

IQRF 9

Wireless M-Bus 9

Wireless M-Bus 9

LoRa 9

LoRa 9

Zigbee 10

Zigbee 10

BLE 10

BLE 10

3.3 Vybraná přenosová technologie 11

Část II Practical part

4 Návrh senzorové sítě **15**

4.1 Návrh integrace WSN gateways do stávající infrastruktury přístupového systému 15

4.2 Protokol CKP v síti RS485 pro komunikaci s kontrolním panelem 17

4.3 Návrh a realizace gatewaye z embedded komponent 18

Zapojení komponent 18

Zapojení komponent 19

4.4 Použité vývojové nástroje k vytvoření FW 19

4.5 Návrh FW gatewaye 20

4.6 Update FW gatewaye 23

4.7 Log Gateawaye	24
4.8 Konfigurace gatewaye	24
4.9 Podpora koncových zařízení	28
4.10 Přidávání koncových zařízení ze serveru řízení přístupu	29
5 Testování navrženého řešení	31
6 Návrh vylepšení systému	35
6.1 Možnosti odstranění omezení navržené gatewaye - závislost na znalosti typu koncových zařízení senzorové sítě	35
6.2 Návrh gatewaye verze 2	36
7 Závěr	38
Literatura	39
Přílohy	
A Odborný článek	47

Obrázky

2.1 Příklad architektury přístupového systému [1110]	7
4.1 Architektura přístupového systému firmy IMA s rozšířením o gateway senzorové sítě	16
4.2 Blokový diagram navržené gatewaysy senzorové sítě, Dragino LoRa Shield [43], RS485 transceiver [44], NUCLEO-L073RZ [41]	18
4.3 Foto sestavené gatewaye	20
5.1 Rozmístění koncových zařízení sítě a zařízení CKP v testovaných prostorách budovy	32
5.2 Měřená rychlosť přenosu dat [bps] v síti RS485 během doby testování	33
6.1 Návrh gatewaye verze 2 - schéma	36
6.2 Návrh gatewaye verze 2 - plošný spoj	37

Tabulky

3.1 Souhrn porovnání parametrů kandidátní bezdrátových technologií	11
4.1 Vlastnosti mikrokontroléru STM32L073RZ [41]	18
4.2 Pinout připojení periférií k mikrokontroléru	19
4.3 Rozdělení programu na nezávislé podprogramy	21
4.4 Dodatečné pomocné podprogramy	21
4.5 Parametry ukládány do non-volatile paměti gatewaye	22
4.6 Defaultní konfigurace systému	28
4.7 Typy koncových zařízení	28
5.1 Frekvenční analýza délky paketu	32
5.2 Maximální počet připojených koncových zařízení v senzorové síti souběžně odesílající data skrze síť RS485 s určitou rezervou	34

Seznam zkratek

AES	Advanced Encryption Standard
AI	Artifical Inteligence
AppSKey	Application Session Key
ASCII	American Standard Code for Information Interchange
BLE	Bluetooth Low Energy
CMAC	Cipher-based message authentication code
CMSIS	Cortex Microcontroller Software Interface Standard
CPU	Central Processing Unit
CR	Carriage Return
CRC	Cyclic Redundancy Check
EEPROM	Electrically Erasable Programmable Read-Only Memory
FIFO	First In First Out
GPIO	General Purpose Input Output
HAL	Hardware Abstraction Layer
HW	HardWare
IDE	Integrated Development Environment
IoT	Internet of Things
ISM	Industrial, scientific and medical
IWDG	Independent Watchdog
LAN	Local Area Network
LBT	Listen Before Talk
LF	Line Feed
LPWAN	Low Power Wide Area Network
LPWSN	Low Power Wireless Sensor Network
MCU	Micro Controller Unit
NwkSKey	Network Session Key
PC	Personal Computer

PCB	Printed Circuit Board
RF	Radio Frequency
RTOS	Real Time Operating System
SDK	Software development kit
SF	Spreading Factor
SPI	Serial Peripheral Interface
UART	Universal Asynchronous Receiver Transmitter
USB	Universal Serial Bus
WSN	Wireless Sensor Network

Kapitola 1

Úvod

todo

Část I

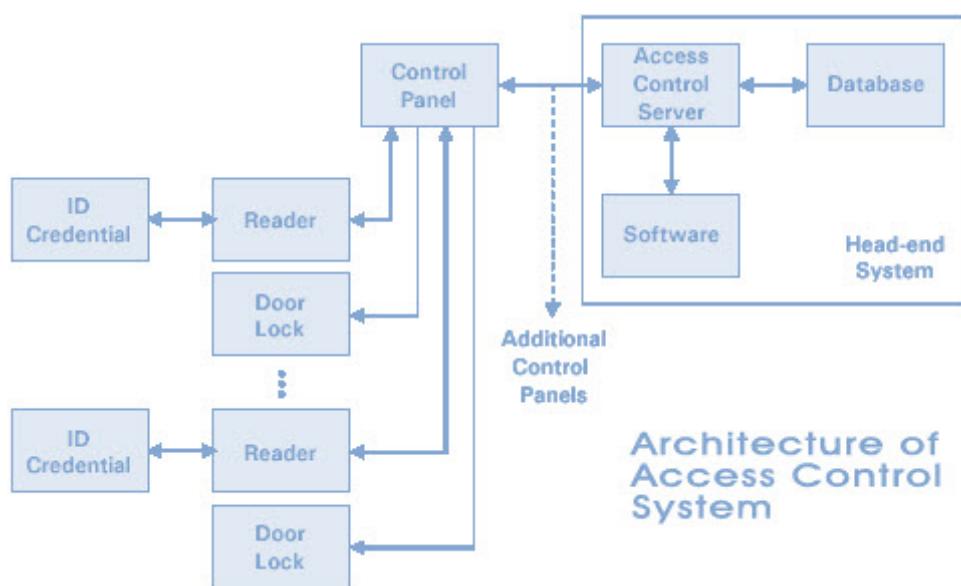
Theoretical part

Kapitola 2

Architektury přístupových systémů

Přístupové systémy jsou elektronické systémy řídící přístup uživatelů do omezených prostor v závislosti na jejich prokázané identitě. Běžně se s přístupovými systémy setkáváme zejména v kancelářních budovách, ale i nemocnicích, školách, úřadech apod. Kromě řízení přístupu uživatelů do vybraných prostor přístupový systém umožňuje i zaznamenávat příchody a odchody uživatelů, tudíž je možné ho zároveň využít jako docházkový systém. Tato kapitola osvětluje architekturu obecného přístupového systému jelikož se tato práce zabývá připojením senzorové sítě k infrastruktuře přístupového systému.

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. 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 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 [1110].



Obrázek 2.1: Příklad architektury přístupového systému [1110]

Kapitola 3

Výběr bezdrátové technologie pro senzorovou síť

Tato kapitola porovnává dostupné bezdrátové technologie vhodné pro tento vybraný případ senzorové sítě a na závěr vysvětluje která technologie byla nakonec vybrána a z jakých důvodů.

■ 3.1 Hlavní kritéria pro výběr bezdrátové technologie

Navržená senzorová síť má být připojena do infrastruktury přístupového systému, který je již zaveden v několika budovách. Jejím účelem je bezdrátové měření veličin např. teplota, vlhkost, CO₂, pomocí koncových zařízení sítě, která vydrží několik let napájena z baterie při periodě měření několik minut rozmístěných v budově a jejím okolí. 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. Dosah by tedy měl být pro pokrytí celé budovy a jejího okolí, ale je zde i možnost napojení více gatewayí rozmístěných po budově k dosažení požadovaného dosahu. Níže jsou vypsány hlavní kritéria pro výběr bezdrátové technologie pro tuto senzorovou síť.

- Nízká cena HW
- Jednoduché připojení koncových zařízení třetích stran (Third party)
- Velký počet dostupných koncových zařízení třetích stran na trhu
- Jednoduchá implementace
- Nízká spotřeba energie koncových zařízení

3.2 Kandidátní bezdrátové technologie

V této sekci jsou rozebrány dostupné bezdrátové technologie, které jsou běžně používány pro bezdrátové měření zařízeními napájenými z baterie a vyhovují stanoveným kritériím vypsaných výše.

IQRF

IQRF je technologie podporována 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 (Software Development Kit) [18] a IDE (Integrated Development Environment) [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 zřetězit více sítí, s jednotlivými koordinátory a různými RF kanály pro vyšší propustnost. Dosah na přímou viditelnost je až 500 m a velikost datového obsahu (payloadu) jednoho paketu může být až 64 B. 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].

Wireless M-Bus

Wireless M-Bus (Meter-Bus) je standard specifikovaný v evropské normě EN 13757 [22], popisující fyzickou, sítovou a aplikační vrstvu, původně navržen pro aplikace bezdrátového měření jako rozšíření průmyslové datové sběrnice M-Bus [23]. 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 [24], [25]. 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.

LoRa

LoRa (Long Range) je modulace navržena firmou Semtech. LoRaWAN je otevřený standardizovaný sítový protokol a systémová architektura navržen LoRa Aliancí definovný v LoRaWAN specifikaci [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) odpovídající přenosové rychlosti, 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 gatewayů s jejichž vzájemnou kompatibilitou není problém. Gateway přeposílá přijaté pakety s daty z koncových zařízení na server, kde je datový obsah (payload) zpracován na základě dokumentace od výrobce daného koncového zařízení. Semtech je jediným výrobcem integrovaných obvodů podporujících LoRa modulaci. Na trhu je dostupných mnoha transceiverů, které používají tento integrovaný obvod, některé dokonce obsahují implementovaný LoRaWAN protokol. Transceiver pro gateway má cenu okolo \$130 a umožňuje současně přijímat pakety od koncových zařízení na více kanálech a přenosových rychlostech. Je zde i možnost udělat jednokanálovou gateway, která je schopna přijímat v jednu chvíli pouze na jednom kanále 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 rychlosť.

Zigbee

Zigbee je specifikace navržena pro IoT aplikace, založena na standardu IEEE 802.15.4, vyvinuta Zigbee alliance [29]. Technologie 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, také je i na trhu dostupných mnoha Zigbee koncových zařízení.

BLE

BLE (Bluetooth Low Energy) 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 mnoha 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.

3.3 Vybraná přenosová technologie

Tabulka 3.1 shrnuje vlastnosti zmíněných technologií.

	IQRF	Wireless M-bus	LoRa	ZigBee	BLE
Topologie	mesh, star	star	star	mesh, star	Point-to-Point, Broadcast, Mesh
Max. velikost paketu	64 B	256 B	256 B	133 B	20 B (Bluetooth 4.0), 251 B (Bluetooth 4.2)
Přenosová rychlosť	19.2 kb/s	32.768 – 100 kb/s	0.3-50kb/s	250 kb/s	až 1 Mb/s
Pásma (Evropa)	868 MHz	868 MHz	868 MHz	2.4 GHz	2.4 GHz
Dosah	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)
Zabezp.	AES128	AES128	AES128	AES128	AES128
Max. vysílací výkon	až 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

Technologie IQRF byla zavrhnuta, jelikož je na trhu velmi málo dostupných koncových zařízení třetích stran, které bylo možné do sítě připojit. ZigBee a BLE mají příliš krátký dosah, což bylo možné vyřešit rozmístěním více gateway napojených na přístupový systém nebo použitím mesh topologie, ale zvyšuje to složitost instalace a cenu řešení. Wireless M-bus a LoRa mají jako nevýhodu vysokou cenu transceiveru pro gateway. LoRa má možnost použití v jednokanálovém módu, kde gateway může použít transceiver určen pro koncová zařízení, které je více jak desetkrát levnější a vyžaduje nižší výkon CPU (Central Processing Unit) než transceiver pro gateway, tudíž gateway v jednokanálovém módu je mnohem jednodušší a levnější řešení.

Vzhledem k definovaným kritériím tedy byla vybrána technologie LoRa se standardizovaným síťovým protokolem LoRaWAN v jednokanálovém módu, jako je to používáno ve vývojových projektech [34], tudíž to není plně LoRaWAN kompatibilní. V jednokanálovém módu jsou všechna zařízení v síti nakonfigurována na jeden konkrétní kanál a SF. LoRaWAN koncová zařízení třetích stran jsou plně kompatibilní s jakoukoliv LoRaWAN gateway pro daný region, tudíž mohou být implementovány do navrženého systému v tomto projektu, ale musí být překonfigurována ke komunikaci na

3.3. Vybraná přenosová technologie

zvoleném kanále a přenosové rychlosti. LoRaWAN síť má hvězdicovou topologii při dostatečném dosahu pro pokrytí budovy a jejím okolí, navíc dosah lze ladit parametrem SF. Pro tento vybraný případ senzorové sítě je to vhodné, jelikož pravděpodobně všechna zařízení v síti budou senzory napájeny z baterie, a není předpokládáno, že by byly připojeny zařízení umožňující směrování paketů z důvodu spotřeby energie. LoRaWAN síť umožňuje koncovým zařízením po změření dat senzory ihned odeslat na gateway bez nutnosti čekání na potvrzení, tudíž se koncové zařízení může ihned přepnout do režimu spánku a tím eliminovat spotřebu energie. Případné občasně kolize mají za důsledek selhání doručení paketu, ale pro vybraný případ měřícího systému to není příliš závažný problém. Frekvenční ISM pásmo 868 MHz, které používá LoRa je limitováno na maximální dobu vysílání 1% času jedním zařízením a přenosová rychlosť této technologie patří mezi nejnižší z kandidátních technologií. Pro vybraný případ měřícího systému se předpokládá přenášení pouhých hodnot senzorů o velikosti několik jednotek až desítek bytů s intervalem několika minut až hodin. LoRaWAN protokol je zabezpečen šifrováním AES-128 na dva způsoby, a to zabezpečení aplikační pro nečitelnst přenášených dat a síťové pro zabránění útočníkům opakovat již přenesené pakety nebo odesílat falešné packety, tudíž je toto zabezpečení dostatečné.

Část II

Practical part

Kapitola 4

Návrh senzorové sítě

Tato kapitola popisuje návrh řešení rozšíření přístupového systému o senzorovou síť.

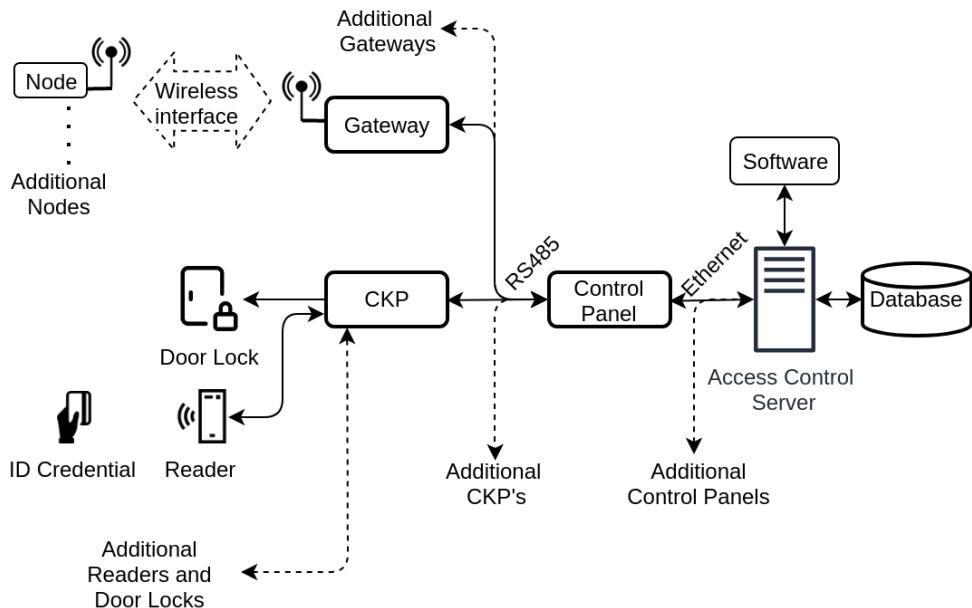
4.1 Návrh integrace WSN gatewaye do stávající infrastruktury přístupového systému

Přístupový systém k rozšíření o WSN je vytvořen firmou IMA a je komerčně distribuován. Jeho architektura se liší od všeobecné architektury zobrazené v blokovém schematu 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 a podobně, ale všechna tato CKP zařízení podporují CKP protokol v síti RS485 pro komunikaci s kontrolním panelem.

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. Nejvhodnější řešení rozšíření tohoto přístupového systému o senzorovou síť je připojením WSN gatewaye ke kontrolnímu panelu přes RS485 síť stejně jako CKP zařízení z důvodu jednoduché instalace. Jednu nebo i více gatewayí je pak možné připojit do vybraných sítí RS485 přístupového systému v budově pro dosažení požadovaného pokrytí senzorové sítě. Názorná blokové schéma přístupového systému firmy IMA s implementací WSN gatewaye je zobrazeno v obrázku 4.1.

WSN gateway tedy musí podporovat CKP protokol v síti RS485 navržen firmou IMA. Přístupový systém firmy IMA funguje tak, že CKP zařízení získává seznam všech platných identifikačních čísel karet ze serveru řízení přístupu a na základě tohoto seznamu pak CKP zařízení provádí odpovídající

4.1. Návrh integrace WSN gatewaye do stávající infrastruktury přístupového systému



Obrázek 4.1: Architektura přístupového systému firmy IMA s rozšířením o gateway senzorové sítě

akci po přiložení 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 pakety 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 pouze 6 B pro data z koncového zařízení, což je velké omezení. LoRaWAN protokol používá paket, jehož samotná hlavička je o minimální velikosti 13 B. Různá LoRaWAN koncová zařízení používají různé velikosti datového obsahu (payloadu), takže není možné odesílat celý payload koncového zařízení přes síť RS485. Tento problém je řešen ta, že LoRaWAN pakety z koncových zařízení jsou dešifrovány přímo v gatewayi a konečné hodnoty senzorů jsou vypočítány z payloadu zařízení na základě dokumentace poskytnuté výrobcem [40]. Vybrané hodnoty jsou odeslány na server řízení přístupu skrze kontrolní panel.

Pro každý podporovaný typ koncového zařízení musí být implementováno zpracování datového obsahu (payloadu) ve FW gatewaye. Pozdější přidání typů koncových zařízení tedy vyžaduje update FW gatewaye. Gateway tedy

4.2. Protokol CKP v síti RS485 pro komunikaci s kontrolním panelem

má uloženou informaci o typu koncového zařízení společně s jeho LoRaWAN adresou zařízení (device address). LoRaWAN protokol je zabezpečen šifrováním AES-128, a to zabezpečení aplikacní pro nečitelnst přenášených dat a síťové pro zabránění útočníkům opakovat již přenesené pakety nebo odesílat falešné pakety. Jsou zde tedy dva AES-128 šifrovací klíče, aplikacní klíč AppSKey (Application Session Key) a síťový klíč NwKSKey (Network Session Key).

Jelikož adresy koncových zařízení jsou předávány gatewayi stejně jako platné karty čtečce z aplikace na serveru řízení přístupu, není zde možnost předávat dva 16 B dlouhé šifrovací klíče pro každé koncové zařízení společně s adresou zařízení. Geteway 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 aktuátorů, jako je relé, motor, apod.

4.2 Protokol CKP v síti RS485 pro komunikaci s kontrolním panelem

CKP protokol v síti RS485 pro komunikaci s kontrolním panelem je kolizní protokol, kde všechna zařízení se řídí pravidlem LBT (Listen Before Talk), kolize jsou detekovány mechanismem kontroly integrity použitý v každém příkazu. V případě že zařízení přijme poškozený příkaz, vyžádá jeho opakování. V této síti je jedno zařízení typu master, a jedno nebo více zařízení typu slave, přičemž zařízení typu master je kontrolní panel a zařízení typu slave je jakékoli CKP zařízení, v tomto vybraném případě gateway. Každé zařízení má svoji adresu definovanou jedním bytem, která musí být unikátní pro jednu síť a každý příkaz v této síti obsahuje v hlavičce adresu odesílatele a adresu příjemce. Zařízení typu slave má dva možné statusy, offline a online, periodicky odesílá příkaz s informací o jeho aktuálním statusu, má povoleno odesílat příkaz s daty z koncového zařízení senzorové sítě "průchod" pouze má-li status online a změnu statusu daného zařízení typu slave provádí zařízení typu master. Zařízení typu slave svůj status změní samo z online na offline v případě, že zařízení typu master přestane odpovídat na příkaz "průchod".

Je-li CKP zařízení spuštěno, má status offline a periodicky odesílá příkaz s informací o jeho statusu na kontrolní panel, který po obdržení tohoto příkazu předá seznam adres koncových zařízení senzorové sítě sekvencí několika příkazů a pak ho přepne do statusu online. V této chvíli již gateway přeposílá data z koncových zařízení senzorové sítě na kontrolní panel.

4.3 Návrh a realizace gatewaye z embedded komponent

Pro otestování navrženého řešení je vytvořena gateway z embedded komponent, tj. LoRa transceiveru pro komunikaci s koncovými zařízeními senzorové sítě, RS485 transceiveru pro komunikaci s kontrolním panelem v síti RS485 a mikrokontrolér jako řídící jednotku viz. blokový diagram v obrázku 4.2. Konkrétní komponenty jsou: Dragino LoRa Shield [43], RS485 transceiver [44] a vývojový kit NUCLEO-L073RZ [41] jako řídící jednotka.



Obrázek 4.2: Blokový diagram navržené gatewaye senzorové sítě, Dragino LoRa Shield [43], RS485 transceiver [44], NUCLEO-L073RZ [41]

Vývojový kit NUCLEO-L073RZ s integrovaným mikrokontrolérem STM32L073RZ je vhodný pro vývoj kvůli jeho parametrům viz tabulka 4.1, pinoutu kompatibilním s Arduino UNO, dokumentaci a ceně (\$13 USD [41]). K vytvoření prototypu byl použit, protože splňuje všechny požadované parametry, je levný, dostatečně výkonný a jednoduchý pro vývoj. Kit obsahuje programátor ST-link pro nahrávání a debugování programu, tudíž není potřeba externí programátor během vývoje FW.

Parametr	Informace
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: Vlastnosti mikrokontroléru STM32L073RZ [41]

Dragino LoRa Shield [43] má kompatibilní pinout s Arduino UNO, tedy i s použitým vývojovým kitem NUCLEO-L073RZ a obsahuje LoRa transceiver RFM95w [42], tedy PCB (Printed Circuit Board) s čipem SX1276.

RS485 transceiver konvertuje rozhraní RS485/UART pro umožnění komunikace s kontrolním panelem přes síť RS485.

Zapojení komponent

CKP zařízení daného přístupového systému jsou obvykle napájena napětím 12 V z kontrolního panelu. Použitý kit NUCLEO-L073RZ obsahuje stabilizátor tudíž je možné připojit gateway přímo ke kontrolnímu panelu přes vyvedené svorky GND, +12V, A a B.

LoRa shield [43] 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 4.3.

Pro komunikaci s LoRa transceiverem je použito SPI1, pro komunikaci přes USB je použito USART2 a pro připojení RS485 transceiveru je použito LPUART1. Připojení periférií k GPIO (General Purpose Input Output) mikrokontroléru je znázorněno v tabulce 4.2.

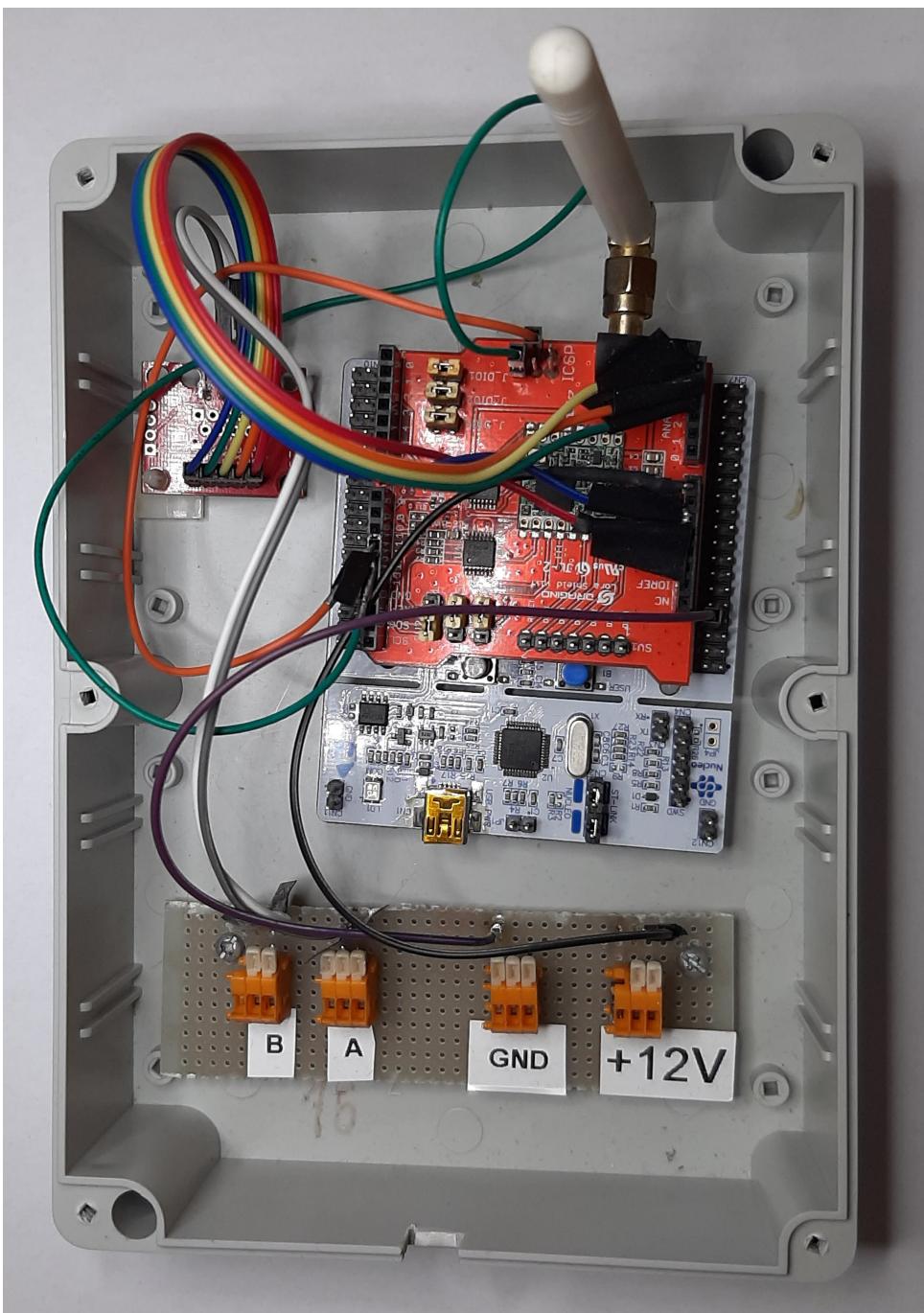
Periférie	Název pinu	GPIO mikrokontroléru
LoRa transceiver	CS	PB6
	CLK	PA5
	MISO	PA6
	MOSI	PA7
	RST	PC7
	DIO0	PA10
RS485 transceiver	RX	PC1
	TX	PC0
	RTS	PB1
USB konektor	RX	PA3
	TX	PA2

Tabulka 4.2: Pinout připojení periférií k mikrokontroléru

4.4 Použité vývojové nástroje k vytvoření FW

Výrobce použitého mikrokontroléru STMicroelectronics poskytuje grafický nástroj STM32CubeMX [46] ke konfiguraci mikrokontrolérů STM32 a generování odpovídajícího kódu v programovacím jazyce C. Pomocí tohoto nástroje byl vygenerován kód pro předběžnou konfiguraci systémového hodinového signálu, IWDG, GPIO a rozhraní.

Kód byl vyvíjen v textovém editoru Visual Studio Code [47], kompilován kompilátorem arm-none-eabi-gcc [48] pomocí nástroje GNU make [49], výsledný binární soubor byl nahráván do procesoru pomocí nástroje st-flash [50] a debugován pomocí Visual Studio Code rozšíření Cortex-Debug [51].



Obrázek 4.3: Foto sestavené gatewaye

4.5 Návrh FW gatewaye

Pro návrh FW gatewaye není použit RTOS (Real Time Operating System), jelikož zde není potřeba řešení více úloh souběžně. K vývoji jsou použity drivery distribuovány výrobcem mikrokontroléru, CMSIS (Cortex

Microcontroller Software Interface Standard) a HAL (Hardware Abstraction Layer). Vyvinutý program je rozdělen na několik nezávislých podprogramů viz tabulka 4.4.

Název podprogramu	Popis
LoRa	Knihovna zahrnující komunikaci s transceiverem RFM95W po rozhraní SPI, nainicializovaném v režimu komunikace LoRa
LoRaWAN_packet	Knihovna zahrnující LoRaWAN protokol, tedy dekódování a dešifrování přijatého LoraWAN paketu i vytvoření paketu pro odeslání. Tato knihovna je závislá na knihovnách aes a cmac.
LoRa_sensors	Knihovna zahrnující dekódování payloadu podporovaných koncových zařízení a zapsání výsledných hodnot do bufferu, který je pak odeslán na kontrolní panel přes síť RS485
rs485_protocol	Podprogram zahrnující síťový protokol v síti RS485
usb	Podprogram zahrnující konfiguraci systému přes USB
eeprom	Knihovna zahrnující práci s non-volatile paměti procesoru EEPROM

Tabulka 4.3: Rozdělení programu na nezávislé podprogramy

Každý z těchto podprogramů je implementován ve zdrojovém souboru (source file) s koncovkou .c a hlavičkovém souboru (header file) s koncovkou .h. Pro vytvoření knihovny zahrnující LoRaWAN protokol jsou použity open source knihovny pro šifrování, tiny-AES128-C [52] pro zašifrování payloadu a openpana [53] pro vytvoření CMAC (Cipher-based Message Authentication Code)

Název podprogramu	Popis
buffer_ring	Knihovna implementující cyklický buffer o velikosti 256 B
ByteArray	Knihovna zahrnující pomocné funkce pro práci s polem bytů
LinkedList_ByteArray	Knihovna implementující linked list s neomezenou velikostí o datové struktuře pole bytů s ukládáním do části paměti heap
aes	Knihovna implementující šifrování AES-128 [52]
cmac	Knihovna pro výpočet CMAC, převzatý pouze potřebný kód z knihovny [53]

Tabulka 4.4: Dodatečné pomocné podprogramy

Do non-volatile paměti je ukládána konfigurace a adresa a typ všech

koncových zařízení senzorové sítě. Jako non-volatile paměť je zde využita EEPROM (Electrically Erasable Programmable Read-Only Memory) o velikosti 6144 B. Paměť je tedy rozdělená tak, že od adresy 0 až po adresu 6080 je prostor pro ukládání LoRaWAN zařízení a od 6080 až po adresu 6144 je prostor pro ukládání konfigurace gatewaye. Každé LoRaWAN zařízení v síti má v paměti uložené LoRaWAN adresu zařízení (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 760 koncových zařízení. Ukládaná konfigurace obsahuje parametry v tabulce 4.5 má celkovou velikost 37 B, na konfiguraci je vyhrazeno 64 B, tudíž je zde rezerva 27 B.

Velikost [B]	Parametr
1	Adresa gatewaye v síti RS485
1	Adresa kontrolního panelu v síti RS485
1	Doba čekání na potvrzení od kontrolního panelu v síti RS485
1	LoRa kanál
1	LoRa SF
16	LoRaWAN NwkSKey
16	LoRaWAN AppSKey

Tabulka 4.5: Parametry ukládány do non-volatile paměti gatewaye

Po spuštění programu je nejprve inicializován mikrokontrolér, hodinový signál, GPIO, rozhraní, timery a IWDG (Independent Watchdog). Systémový hodinový signál je nakonfigurován na maximální hodnotu, což je 32 MHz. Po inicializaci mikrokontroléru je z non-volatile paměti EEPROM vyčtena a vypsána v logu aktuální konfigurace gatewaye a následuje inicializace LoRa transceiveru RFM95w dle načtené konfigurace a nakonec je vstoupeno do hlavní smyčky běhu programu, kde jsou zpracovávány cyklické buffery přijatých dat přes USB a RS485 a fronty přijatých LoRaWAN paketů a příkazů k odeslání na kontrolní panel přes síť RS485.

Jsou zde použity 2 timery, TIM2 pro restartování procesoru a TIM3 pro resetování IWDG. Resetování procesoru po daném intervalu defaultně není použito, ale je implementováno a v případě potřeby je možné využít. IWDG je resetováván timerem tudíž tvoří pojistku tak, že resetuje procesor v případě, že by se program zhroutil.

Komunikace s transceiverem RS485 přes LPUART1 je implementována pro vysílání v blokujícím módu a přijímání přes interrupt, kde přijatý byte je zapsán do cyklického bufferu o velikosti, který je zpracováván v hlavní smyčce běhu programu. Jelikož komunikace v síti RS485 je half-duplex a platí zde pravidlo LBT, vysílání je zde blokováno po dobu 20 ms od posledního přijatého bytu.

Komunikace s LoRa transceiverem RFM95W přes rozhraní SPI1 je implementována v blokujícím módu zápisem a čtením registrů. LoRa transceiver je nakonfigurován na kontinuální příjem na zvoleném kanále a SF, přijatý LoRa paket signalizuje zvednutím logické úrovně pinu DIO0. Toto je řešeno interrupt pinem, po jehož přerušení je vyčten přijatý LoRa paket z FIFO (First In First Out) paměti transceiveru a přidán do fronty tvořené linked listem, zpracovávané v hlavní smyčce běhu programu, kde pakety z této fronty jsou postupně dekódovány a diešifrovány, na základě typu zařízení jsou vypočteny hodnoty senzorů z payloadu a zakódovány do bufferu o délce 6 B, který je připojen do fronty tvořené linked listem, zpracovávané v hlavní smyčce běhu programu.

Komunikace přes USB přes USART2 je implementována obdobně jako komunikace v síti RS485 kde přijatá data jsou zapsána do cyklického bufferu, který je zpracováván v hlavní smyčce běhu programu, ale vysílání není blokováno během přijímání, jelikož se jedná o full-duplex.

4.6 Update FW gatewaye

K nahrání FW do gatewaye je využit ST-link na vývojovém kitu NUCLEO-L073RZ. Po připojení gatewaye k PC přes USB se v PC gateway zobrazí jako externí flash paměť, do které je soubor FW nakopírován. Proces je tedy stejný, jako kdyby byl soubor FW zkopirován na externí flash disk připojen k PC.

4.7 Log Gateways

Po připojení ke gatewayi přes sériovou linku je možné kontinuálně snímat log gateways obsahující informace o proběhlých událostech. Je-li gateway v normálním pracovním režimu, loguje informace automaticky přes sériovou linku a komunikace je zde pouze jednosměrná, tedy gateway vysílá a PC přijímá. Níže je příklad výpisu logu v případě, kdy gateway přijala LoRaWAN paket z koncového zařízení senzorové sítě, zpracovala ho a výslednou informaci odeslala na kontrolní panel přes RS485 síť.

```
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: "FF1F100D00D0F61F01281A0934CDFFFF09202E"

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

Nejprve jsou vypsány data týkající se LoRaWAN protokolu, zašifrovaný i dešifrovaný datový obsah (payload) koncového zařízení, typ zařízení a výsledné hodnoty dekódované z payloadu.

4.8 Konfigurace gateways

Konfigurace gatewaye se provádí obousměrnou komunikací po sériové lince. Po spuštění je gateway v normálním pracovním režimu, přeposílá tedy pakety ze senzorové sítě přes RS485 síť na kontrolní panel a informace loguje přes sériovou linku. Po vstoupení do stavu konfigurace je pozastavena činnost gatewaye, komunikace s koncovými zařízeními LoRaWAN sítě a komunikace s kontrolním panelem v síti RS485 nejsou aktivní. Do režimu konfigurace je vstoupeno odesláním "config", následuje vypsání současného stavu konfigurace a následně uživatel postupuje zadáním čísla pro výběr možnosti z menu či konkrétního parametru dle vyzvání. Z konfigurace je možné vystoupit kdykoliv bez uložení změn příkazem "quit". Procházení jednotlivými menu je navrženo jednoduše tak, aby uživatel nepotřeboval dokumentaci a aby zde vždy bylo

uvedeno dost informací pro srozumitelnost. Níže je zobrazen příklad výpisu po vstupu do konfigurace obsahující informaci o aktuální konfiguraci a hlavní konfigurační menu.

```
----- 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
```

Jsou zde tedy tři sekce konfigurace, LoRa kanál, RS485 kanál a parametry LoRaWAN protokolu. Dále jsou zde další možnosti hlavně pro diagnostické účely, a to možnost ručně přidat LoRaWAN koncové zařízení a vymazání všech koncových zařízení, ačkoliv je to obvykle prováděno ze serveru řízení přístupu, a navrácení stavu gatewaye do defaultního stavu. Dále jsou zde možnosti vystoupení z menu s či bez uložení změn, tedy zapsání nově nakonfigurovaných parametrů do non-volatile paměti.

Při procházení jednou ze tří možných konfigurací je vždy pro každý parametr vypsáno jaká data mají být uživatelem 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. Pokud uživatel některý parametr nechce měnit, přeskočí ho odesláním ASCII znaku LF (0x0D) u většiny terminálových aplikací stačí pouze stisknout na klávesnici Enter. Po provedení některé 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. Pokud je vybráno "Exit without save", gateway se pouze restartuje.

■ Konfigurace LoRa kanálu

Položka v menu pod názvem "Config LoRa channel" zahrnuje nastavení SF, tedy přenosovou rychlosť a frekvenční kanál. 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.
```

■ Konfigurace RS485 kanálu

Položka v menu pod názvem "Config RS485 channel" zahrnuje nastavení adresy gatewaye, tedy tohoto zařízení, adresy kontrolního panelu a timeout, což je doba čekání na potvrzení od kontrolního panelu 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
```

■ Konfigurace LoRaWAN protokolu

Položka v menu pod názvem "Config LoRaWAN protocol" 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)
1111111222222233333344444444
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)
1111111222222233333344444444
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 4.6. 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 4.6: Defaultní konfigurace systému

4.9 Podpora koncových zařízení

Jak již bylo zmíněno v sekci , z důvodu datového omezení protokolu sítě RS485 jsou LoRaWAN pakety koncových zařízení dekódovány v gatewayi a z datového obsahu (payloadu) vypočítány konečné hodnoty dle dokumentace daného LoRaWAN zařízení a přes síť RS485 na kontrolní panel jsou odesány pouze vybraná data. Gateway má pro každé koncové zařízení uloženou 4 byty dlouhou adresu a 1 byte typ zařízení. Momentálně jsou podporovány dva typy koncových zařízení, dle potřeby je možné rozšířit FW gatewaye o další typy koncových zařízení. Tabulka 4.7 ukazuje hodnotu bytu označující typ koncového zařízení odpovídající konkrétním typům koncových zařízení.

Typ zařízení	Hodnota
RHF1S001	0x00
IMA_tempPress	0x01

Tabulka 4.7: Typy 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 odesán přes síť RS485 příkazem "průchod".

RHF1S001

Senzor od firmy RisingHF měřící teplotu a vlhkost [40].

```

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

```

4.10. Přidávání koncových zařízení ze serveru řízení přístupu

```
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 6 B long buffer, to be transmitted to the control panel */
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;
```

4.10 Přidávání koncových zařízení ze serveru řízení přístupu

Přidávání koncových zařízení senzorové sítě se provádí z uživatelského rozhraní serveru řízení přístupu stejně jako přidávání platných RFID karet, s

4.10. Přidávání koncových zařízení ze serveru řízení přístupu

délkou UID 8 B. Adresa koncového zařízení (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 serveru řízení přístupu. Při odesílání příkazu "průchod" se tedy už typ zařízení neposílá z důvodu omezené velikosti tohoto příkazu. Na serveru řízení přístupu se UID nastavuje jako dekadické číslo.

Příklad

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

Kapitola 5

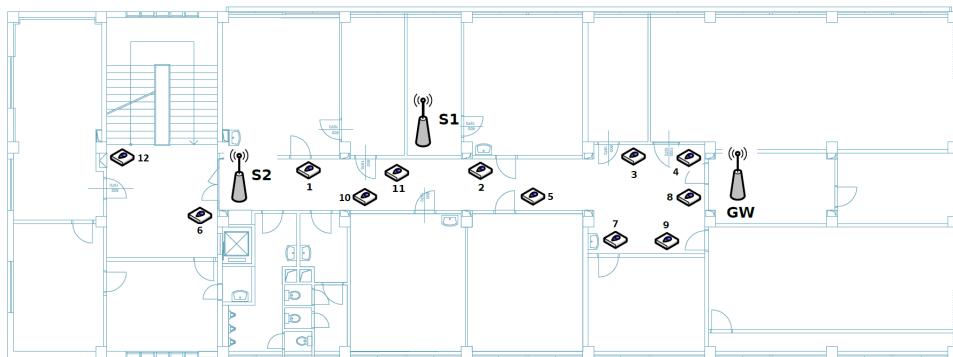
Testování navrženého řešení

Tato kapitola zahrnuje testování navržené gatewaye senzorové sítě viz. kapitola 4, napojené přes síť RS485 na infrastrukturu přístupového systému firmy IMA v univerzitní budově univerzity ČVUT za reálného provozu s připojenými koncovými zařízeními senzorové sítě, které souběžně odesílají data. Ze zachyceného provozu dat v síti RS485 je odhadnut maximální počet připojených koncových zařízení souběžně odesílající data v senzorové síti při zachování správné funkce přístupového systému.

Testování je provedeno v jednom bloku patra univerzity, kde je do jednoho kontrolního panelu připojeno dvanáct CKP zařízení přes síť RS485. Každé z nich ovládá jedny dveře, tedy jednu čtečku a dveřní zámek. Do této sítě RS485 je navíc připojena navržená gateway jako třinácté CKP zařízení. K této navržené gatewayi senzorové sítě jsou připojena dvě koncová zařízení typu RHF1S001, dostupné na trhu, vyrobené firmou RisingHF, obsahující senzory teploty a vlhkosti. Pro tento test jsou nakonfigurovány k odesílání dat ze senzorů s intervalom 5 minut.

Gateway a CKP zařízení jsou zapojena dle blokového schematu v obrázku 4.1. Konkrétní rozmístění stávajících dvanácti CKP zařízení, gatewaye a dvou koncových zařízení senzorové sítě v testovaných prostorách budovy je zobrazeno v obrázku 5.1.

Testování probíhalo od 21. září do 31. října, tedy v době přítomnosti studentů a zaměstnanců v testovaných prostorách. Po tuto dobu testování byly zaznamenávány přenášené pakety sítě RS485, kontrolní panel přijal 1 876 978 paketů (14 074 522 B) a odeslal 1 101 556 paketů (8 295 219 B), dohromady tedy 2 978 534 paketů (22 369 741 B). Z naměřených hodnot byla provedena metoda frekvenční analýzy. Z přenesených paketů byly nejdělsí 3 o velikosti 40 bytů. S ohledem na celkové množství paketů je to zanedbatelné množství, tj. 1,3E-04 %. Avšak vzhledem k povaze systému, tedy systému s



Obrázek 5.1: Rozmístění koncových zařízení sítě a zařízení CKP v testovaných prostorách budovy

primární funkcí řízení přístupu do omezených oblastí, se za nejhorší scénář považuje neprekonatelný limit velikosti paketu.

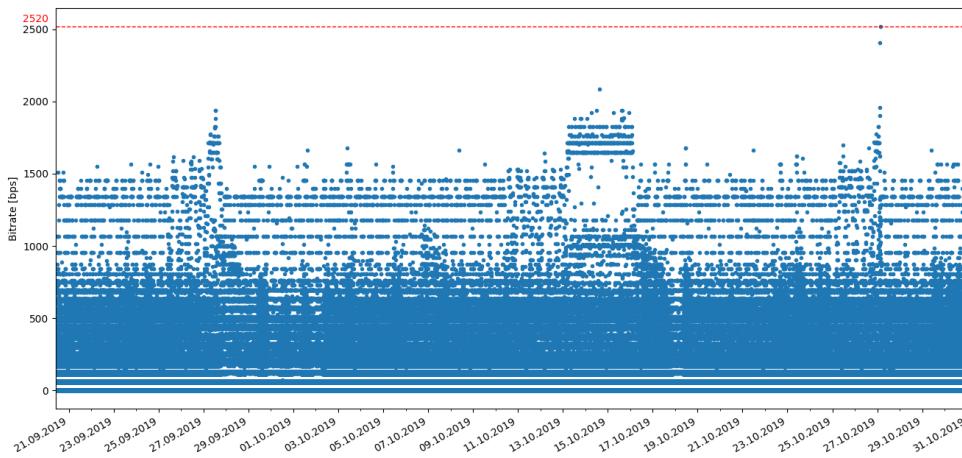
Maximální počet koncových zařízení připojených ke gatewayi při kterém není ovlivněn stávající přístupový systém je možné vypočítat z rychlosti přenosu dat v síti RS485. Tato rezerva rychlosti přenosu dat je uvažována za účelem ochrany přístupového systému před dysfunkcí nebo poruchou, například před dlouhým čekáním na otevření dveří.

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: Frekvenční analýza délky paketu

Na základě frekvenční analýzy uvedené v tabulce 5.1 a IMA know-how, pakety přenášející data z koncových zařízení jsou dlouhé 19 byte a pakety potvrzení IMA protokolu jsou dlouhé 7 byte. Alespoň dva pakety jsou potřeba k přenesení dat z koncových zařízení přes síť RS485, tj. paket s daty koncového zařízení a paket potvrzení.

V obrázku 5.2 jsou dvě důležité charakteristiky, maximální délka paketu (červená přerušovaná čára) a medián délky paketu (červená nepřerušovaná čára), určeny frekvenční analýzou v tabulce 5.1. Průměrné zatížení provozu kanálu sítě RS485 je 6,38 pps, tj. 0,85 Bps.



Obrázek 5.2: Měřená rychlosť prenosu dat [bps] v sítí RS485 během doby testování

Z testování provozu jsou zachyceny délky přenášených paketů (l) s časovou přesností na tisícinu sekundy. Údaje o čase jsou převedeny na jednotky sekund pomocí funkce sum, aby byly získány data jako bitová rychlosť v bitech za sekundu (bps). V obrázku 5.2 červená přerušovaná čára s hodnotou 2520 bps ukazuje jeden sekundový interval ve kterém součet přenesených paketů v síti RS485. Na základě podrobných znalostí protokolu IMA se ukazuje, že je využito méně než 20% kapacity sítě RS485.

Aby bylo zabráněno přetížení sítě RS485, maximální počet koncových zařízení připojených ke gatewayi S_{MAX} je možné vypočítat vztahem:

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

kde:

v_{485} rychlosť prenosu dat v sítí RS485 [bps]

B počet bitů v bytu (pro přepočítání rychlosti prenosu dat na byty)

l_{MAX} maximální délka paketu

R rezerva rychlosť prenosu dat [%]

P počet paketů k přenesení dat z koncového zařízení

S ohledem na výše uvedené limity, navržené rezervy a rychlosť prenosu dat v sítí RS485 je vypočítán maximální počet koncových zařízení senzorové sítě, které souběžně odesílají data přes síť RS485 viz. tabulka 5.2.

Použité hodnoty pro výpočet jsou:

v_{485} = RS485 network data rate

B = 8

l_{MAX} = 40

P = 2

RS485 rychlosť prenosu dat v_{485} [bps]	Rezerva R			
	0 %	10 %	20 %	30 %
1200	1	1	1	1
2400	3	3	3	2
4800	7	6	6	5
9600	15	13	12	10
19200	30	27	24	21
38400	60	54	48	42
57600	90	81	72	63
115200	180	162	144	126
230400	360	324	288	252
460800	720	648	576	504
921600	1440	1296	1152	1008

Tabuľka 5.2: Maximálny počet pripojených koncových zařízení v senzorovej sítí souběžně odesílající data skrze síť RS485 s určitou rezervou

Např. v senzorovej sítí môže byť až 54 koncových zařízení pripojených ke gateway, ktorá je napojena na síť RS485 s prenosovou rychlosťou 38400 bps a rezervou 10 % nebo 42 koncových zařízení s prenosovou rychlosťou 38400 bps a rezervou 30 %. Tento výsledek ukazuje, že jeden blok patra univerzity, tj. jedna síť RS485 je schopna fungovať s desítkami koncovými zařízeniami senzorovej sítě souběžně vysílajúcimi data s dostatečnou rezervou chránící přístupový systém.

Kapitola 6

Návrh vylepšení systému

V této kapitole jsou navrženy způsoby vylepšení navrženého systému.

■ 6.1 Možnosti odstranění omezení navržené gatewaye - závislost na znalosti typu koncových zařízení senzorové sítě

Jedním z největších omezení navrženého systému je, že FW gatewaye musí podporovat typy všech koncových zařízení senzorové sítě, tudíž přidání nového typu zařízení do sítě vyžaduje update FW gatewaye. Je zde několik možností jak toto obejít, aby gateway nebyla závislá na znalosti typu koncových zařízení senzorové sítě, ale všechny tyto možnosti zapříčinují nežádoucí vliv a to zvýšení objemu přenášených dat v síti RS485 přístupového systému. Původní řešení totiž klade důraz na nízký objem přenášených dat v síti RS485.

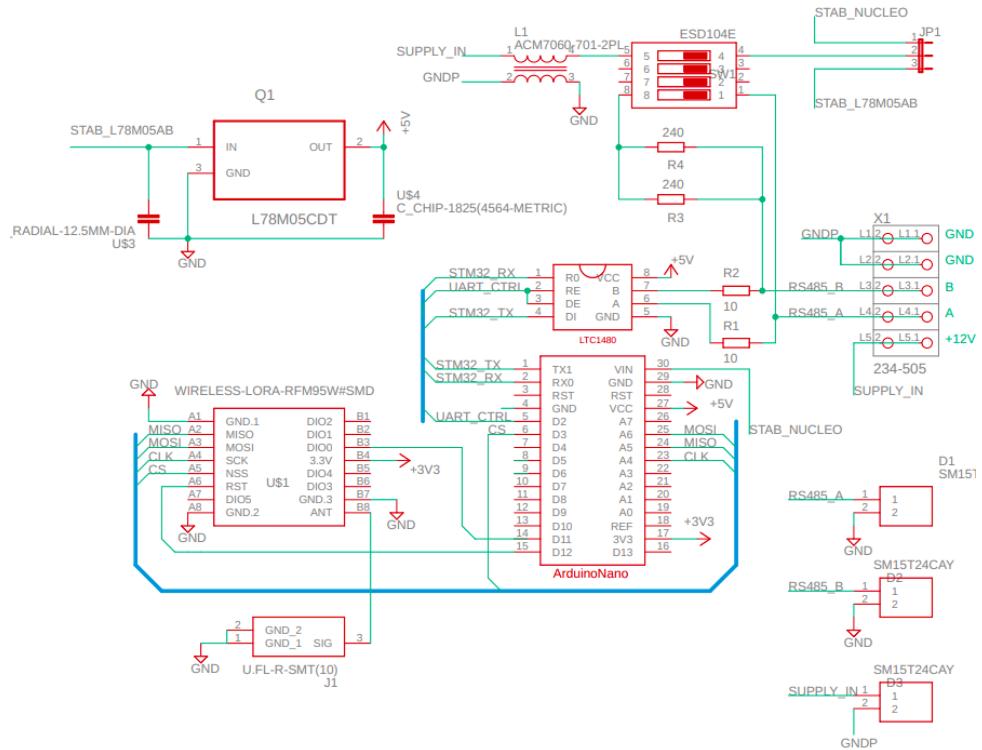
Například použitý typ koncového zařízení RHF1S001 4.9 odesílá LoRaWAN pakety o délce 22 bytů, z toho je 9 bytů aplikační payload. Protokol umožňuje posílat pakety o velikosti až 256 bytů, z toho je nejméně 13 bytů data protokolu, tedy maximální délka aplikačního payloadu může být až 243 bytů.

Nejfektivnější řešení by bylo rozšíření CKP protokolu sítě RS485 přístupového systému o nový typ příkazu umožňující odeslat paket o maximální délce payloadu až 243 bytů, tedy aby jedním tímto paketem bylo možné odeslat celý aplikační payload. Je zde bezpečnostní výhoda, že aplikační payload by pak mohl být dešifrován až na serveru LoRaWAN klíčem AppSKey, tudíž by data z koncových zařízení by nebyla odhalitelná v síti RS485. Toto řešení tedy vyžaduje update FW všech kontrolních panelů, čož je velmi náročné.

Nicméně je možné implementovat podobné řešení bez nutnosti zavádění nového typu paketu pro aplikační payload koncového zařízení senzorové sítě tak, že aplikační payload by byl rozdělen a odeslán posloupností několika paketů průchod. Např. z dostupných 6 byte v jednom paketu průchod by jeden byte obsahoval informaci o čísle paketu dané sekvence a zbylých 5 byte by byly data payloadu daného koncového zařízení Zařízení typu RHF1S001, které má aplikační payload o velikosti 9 byte by byl takto odeslán dvěma pakety průchod. Jelikož každý paket průchod je potvrzován, toto řešení by rapidně zvýšilo objem přenášených dat v síti RS485.

6.2 Návrh gatewaye verze 2

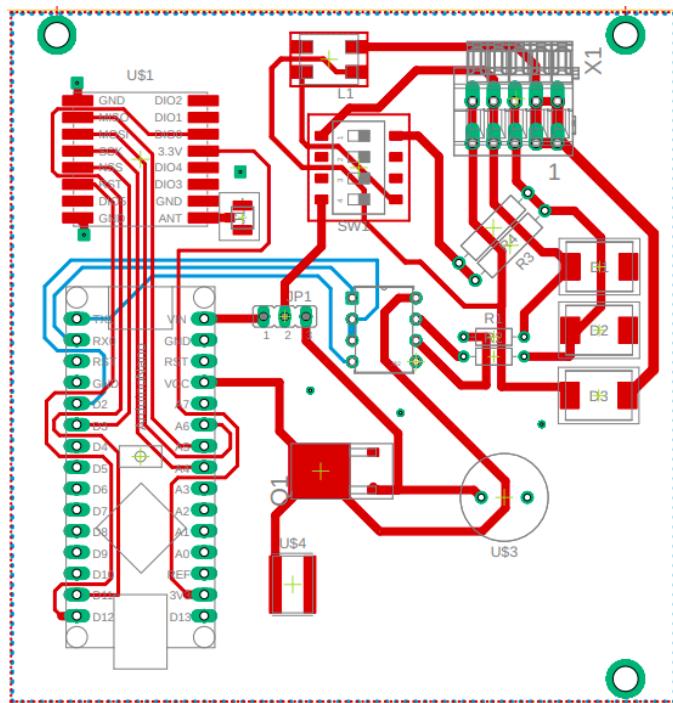
Pro lepší mechanické uspořádání byla navržena verze 2 s navrženým plošným spojem (PCB). Schéma zapojení je v obrázku 6.1 a plošný spoj je v obrázku 6.2. Je zde použit jiný vývojový kit NUCLEO-L432KC s výkonnějším procesorem STM32L432KC, který má pinout stejný jako Arduino Nano, tedy je pod tímto názvem ve shématu. LoRa transceiver je použit RFM95w [42] bez shieldu. RS485 transceiver je použit LTC1480. Do zařízení je dále přidán externí stabilizátor, napěťový filtr, přepínač volitelné impedanční zakončení sítě RS485 a napěťové ochrany pro linky A, B a napájení.



Obrázek 6.1: Návrh gatewaye verze 2 - schéma

Použitý procesor neobsahuje paměť EEPROM, tudíž pro ukládání

6.2. Návrh gatewaye verze 2



Obrázek 6.2: Návrh gatewaye verze 2 - plošný spoj

konfigurace gatewaye a zařízení senzorové sítě je použita paměť flash.

Kapitola 7

Závěr

V této práci jsou diskutovány podmínky rozšíření stávajícího systému řízení přístupu pracujícího v průmyslově standardizované síti RS485 s bezdrátovou senzorovou sítí založenou na jednokanálovém režimu LoRaWAN.

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] [Online]. Available: https://ec.europa.eu/eip/ageing/standards/ict-and-communication/data/en-13757_en [Accessed: 2-Apr-2020].
- [23] [Online]. Available: <https://automatizace.hw.cz//sbernice-wireless-mbus-jde-i-bezdratove> [Accessed: 9-Jun-2018].
- [24] *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].
- [25] *Wireless M-Bus in Industrial Wireless Sensor Networks.* Radiocrafts. [Online]. Available: <https://radiocrafts.com/technologies/wireless-m-bus-technology-overview/> [Accessed: 9-Jun-2018].
- [26] Silicon labs: *WIRELESS M-BUS SOFTWARE IMPLEMENTATION.* [Online]. Available: <https://www.silabs.com/documents/public/application-notes/AN451.pdf> [Accessed: 9-Jun-2018].
- [27] 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://lora-alliance.org/sites/default/files/2018-04/lorawantm_specification_v1.1.pdf [Accessed: 9-Sep-2019].
- [34] 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].
- [40] 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].
- [41] *NUCLEO-L073RZ*. ST Microelectronics [Online]. Available: <https://www.st.com/en/evaluation-tools/nucleo-l073rz.html> [Accessed: 20-Sep-2019].
- [42] *RFM95/96/97/98(W) - Low Power Long Range Transceiver Module*. HopeRF electronic. V1.0. [Online]. Available: <https://www.hoperf.com/modules/lora/RFM95.html> [Accessed: 20-Sep-2019].
- [43] *Lora Shield*. Dragino. [Online]. Available: http://wiki.dragino.com/index.php?title=Lora_Shield [Accessed: 20-Sep-2019].
- [44] *SparkFun Transceiver Breakout - RS-485* Sparkfun. [Online]. Available: <https://www.sparkfun.com/products/10124> [Accessed: 20-Sep-2019].
- [45] *NUCLEO-L073RZ ARM Mbed*. [Online]. Available: <https://os.mbed.com/platforms/ST-Nucleo-L073RZ/> [Accessed: 20-Sep-2019].

- [46] [Online]. Available: <https://www.st.com/en/development-tools/stm32cubemx.html> [Accessed: 20-Sep-2019].
- [47] [Online]. Available: <https://code.visualstudio.com/> [Accessed: 20-Sep-2020].
- [48] [Online]. Available: <https://developer.arm.com/tools-and-software/open-source-software/developer-tools/gnu-toolchain/gnu-rm/downloads> [Accessed: 20-Sep-2020].
- [49] [Online]. Available: <https://www.gnu.org/software/make/manual/make.html> [Accessed: 20-Sep-2019].
- [50] [Online]. Available: <https://github.com/texane/stlink> [Accessed: 20-Sep-2019].
- [51] [Online]. Available: <https://marketplace.visualstudio.com/items?itemName=marus25.cortex-debug> [Accessed: 20-Sep-2019].
- [52] *tiny-AES128-C* bitdust. [Online]. Available: <https://github.com/bitdust/tiny-AES128-C> [Accessed: 20-Sep-2019].
- [53] *openpana*. OpenPANA. [Online]. Available: <https://github.com/OpenPANA/openpana> [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=1D12BD2186DD8FA9065DCE9301C63D4D2F67C3557C4677D06FCE5DBB92C96984BFCF132B6DD37ED892EAF6F1BBC28DC0> [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].

Přílohy

Příloha A

Odborný článek

LORA NODES IN EXISTING ACCESS CONTROL SYSTEM INFRASTRUCTURE: A FEASIBILITY STUDY

*Tomas HYHLIK^{1,2}, Marek NERUDA¹, Pavel BEZPALEC¹, Lukas VOJTECH¹,
Vlastimil BENES²*

¹Department of Telecommunication Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague,

Technicka 2, Prague, Czech Republic

²Institut of Microelectronic Applications, IMA s.r.o.,
Na Valentince 1003/1, Prague, Czech Republic

[hyhlito1 | marek.neruda | pavel.bezpalec | lukas.vojtech]@fel.cvut.cz, vlastimil.benes@ima.cz

DOI: 10.15598/aeee.v13ix.xxxx

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.

lications are typically based on a special kind of wireless technology called Low Power Wide Area Network (LPWAN) [3]. 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 [4] and can have one of the following topologies: star (centralized), star of stars (decentralized) and mesh (distributed) [5]. 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 [6].

The industry of IoT is growing because of its enormous potential. Cisco study [7] 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

Keywords

Access control system, LoRa, LPWAN, WSN.

1. Introduction

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 ap-

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 [12]. 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 [14] 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.

The ID Credential represents the user identification, provided for instance by RFID tag, fingerprint, QR code. The Reader reads the data from the ID Credential and sends it to the Control Panel. The Door Lock is used to control the physical access of users to the restricted area, e.g., building, room, floor. The Control Panel is the interface between Access Control Server and pairs the Reader with the Door Lock. It typically connects these pairs via RS485 and Access Control Server via Ethernet, i.e., TCP/IP protocol. The main function is the management of these pairs. The Database contains user IDs. The Access Control Server uses Software (SW) to manage the Database and communicates with all Control Panels. The Reader scans data from submitted ID Credential and transmits the data to the Control Panel, which resends it to the Access Control Server. The Access Control Software finds the received user data in the Database and, if found, sends a command to the corresponding Control Panel to switch the corresponding Door Lock.

2) 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].

2.2. Specific System Design for Testing Proposes

1) 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. 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. 2. 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 proto-

2. System Design

2.1. General System Design

1) Architecture of Access Control Systems

Access control systems are electronic systems controlling the access of users into restricted areas depending on the user identity [15]. A typical system architecture is shown in Fig. 1.

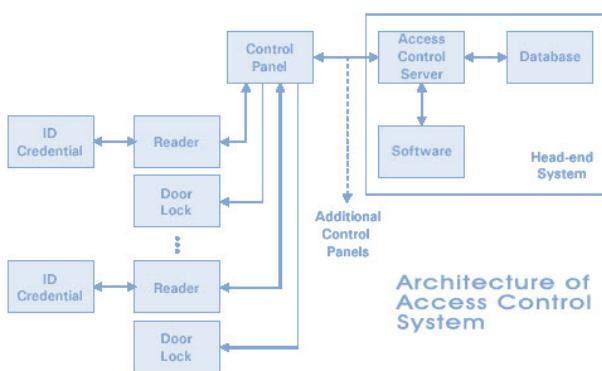


Fig. 1: Example of access control system architecture [15]

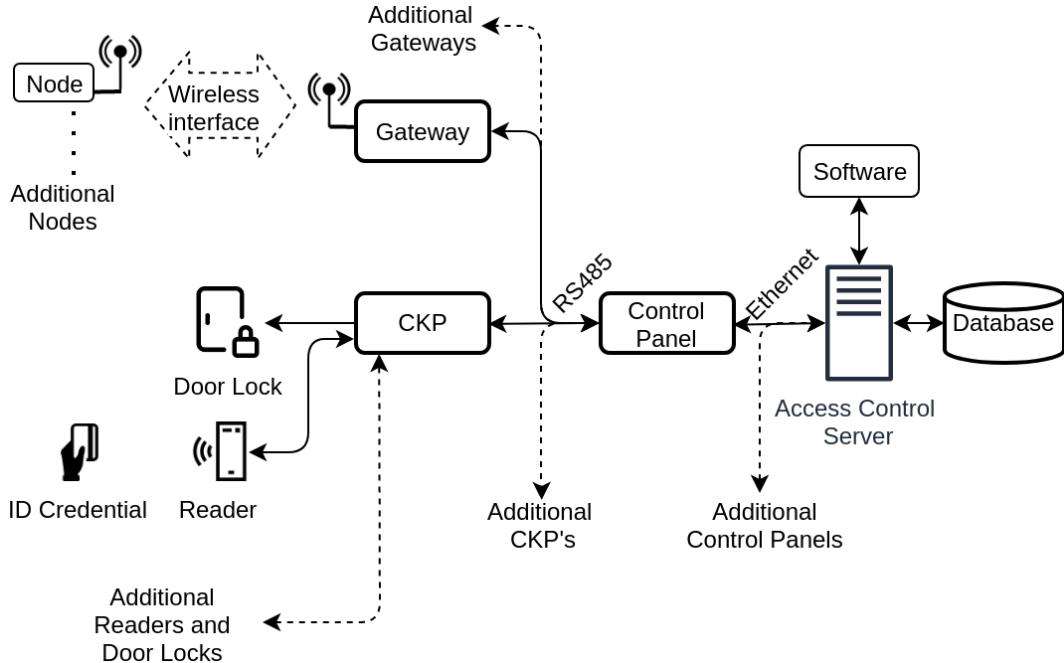


Fig. 2: IMA access control system architecture with WSN extension

col, 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.

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.

2) 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 [21], RFM95w LoRa Shield [22] and RS485 transceiver [24], Fig. 4.

The NUCLEO-L073RZ development board with STM32L073RZ microcontroller is suitable for the development purposes because of its parameters,

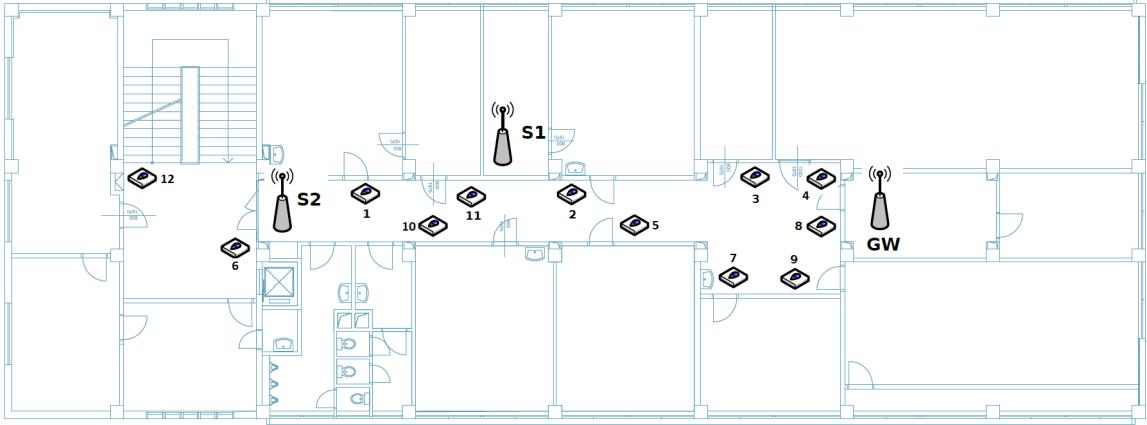


Fig. 3: Location of sensor nodes and CKP devices on the university floor



Fig. 4: Gateway block diagram, RFM95w [22], RS485 transceiver [24], NUCLEO-L073RZ [21]

Tab. 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.

Tab. 1: The STM32L073RZ features [21]

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

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.

Tab. 2: Packet length frequency analysis

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

Based on the frequency analysis given in Tab. 2 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

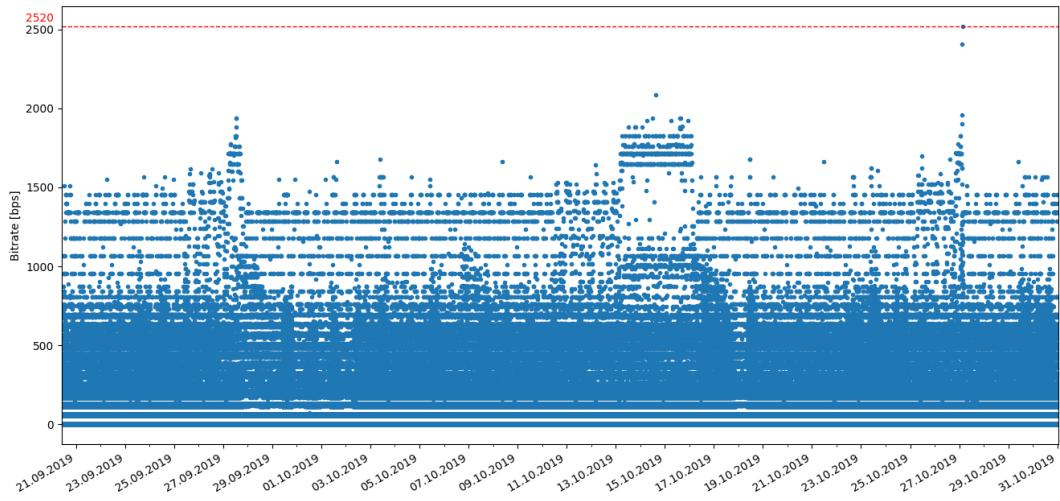


Fig. 5: Measured data rate in [bps] in RS485 network during long-term operation test

packets are required to handle sensor data via RS485 network, i.e., one carrying sensor data and 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. 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:

$$S_{MAX} = \frac{\frac{v_{485}}{B} - R}{P} \quad (1)$$

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. 3.

Values for calculation are:

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

Tab. 3: Maximum number of sensor nodes simultaneously transmitting their data in RS485 network with desired reserve

RS485 data rate v_{485} [bps]	Reserve R			
	0 %	10 %	20 %	30 %
1200	1	1	1	1
2400	3	3	3	2
4800	7	6	6	5
9600	15	13	12	10
19200	30	27	24	21
38400	60	54	48	42
57600	90	81	72	63
115200	180	162	144	126
230400	360	324	288	252
460800	720	648	576	504
921600	1440	1296	1152	1008

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.

4. Conclusions

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.

Acknowledgment

This work was supported by the TA CR grant "The Multichannel Communication Platform for the Internet of Things (IoT)" TH02010568 and by the internal CTU grant under project SGS18/183/OHK3/3T/13.

References

- [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 IoT 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-DS01588Outdoor-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].

About Authors

Tomas HYHLIK was born in Pardubice, Czech Republic. He received his Bc. degree from the Czech Technical University in Prague, Faculty of Electrical Engineering in 2017. His research interests include Internet of Things.

Marek NERUDA was born in Hradec Kralove, Czech Republic. He received the M.Sc. and Ph.D. degree in electrical engineering from the Czech Technical University in Prague, Faculty of Electrical Engineering, Czech Republic in 2007 and in 2014, respectively. Currently, he works as an assistant professor at the Department of telecommunication engineering, CTU in Prague. His research interests include RFID technology, the Internet of Things and electrically conductive textile materials.

Pavel BEZPALEC was born in Prague, Czech Republic. He received the M.Sc. and Ph.D. degree in electrical engineering from the Czech Technical University in Prague, Faculty of Electrical Engineering, Czech Republic in 1998 and in 2007, respectively. Currently, he works as an assistant professor at the Department of telecommunication engineering, CTU in Prague. His research interests include networking, (cyber)security and telephony technology.

Lukas VOJTECH was born in Nachod. He received the M.Sc. degree in electrical engineering from the Czech Technical University in Prague, Faculty of Electrical Engineering, in 2003. In 2005, he received the bachelor degree engineering pedagogy from the Masaryk Institute of Advanced Studies in Prague. In 2010, he received the Ph.D. degree from Czech Technical University in Prague, Faculty of Electrical Engineering. Currently, he works as an assistant professor at the Department of telecommunication engineering, CTU in Prague. His research interests include wireless technologies, technology RFID and mainly EMC in area of shielding materials.

Vlastimil BENES received the M.Sc. degree in electrical engineering from the Czech Technical University in Prague, Faculty of Automated control systems, Czech Republic in 1986. His research interests include RFID technology, access control systems and the Internet of Things.