VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV RADIOELEKTRONIKY
DEPARTMENT OF RADIO ELECTRONICS

BEZDRÁTOVÝ SBĚR DAT V PRŮMYSLOVÉM PROSTŘEDÍ
WIRELESS DATA ACQUISITION IN INDUSTRY ENVIRONMENT

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Jáchym Macura**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Jaromír Kolouch, CSc.**
SUPERVISOR

BRNO 2016

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Elektronika a sdělovací technika**
Ústav radioelektroniky

Student: Jáchym Macura ***ID:*** 164327
Ročník: 3 ***Akademický rok:*** 2015/16

NÁZEV TÉMATU:

Bezdrátový sběr dat v průmyslovém prostředí

POKYNY PRO VYPRACOVÁNÍ:

Navrhněte systém snímačů a modulů pro bezdrátový sběr dat v průmyslovém prostředí určený pro měření na samostatných testerech umístěných ve výrobní hale, které nemají síťové připojení. Přenos dat musí být zabezpečen, zašifrován a odolný proti průmyslovému rušení. Prozkoumejte možná řešení a navrhněte vhodnou infrastrukturu sítě, protokol, šifrování, předávání dat, způsob opakování přenosů.

Pro ověření a demonstraci funkce navrženého řešení realizujte moduly pro připojení ke třem testerům.

DOPORUČENÁ LITERATURA:

[1] MANN, B. C pro mikrokontroléry. Praha: BEN, 2003.

[2] PUŽMANOVÁ, R. Bezpečnost bezdrátové komunikace. Brno: Computer Press, 2005.

Termín zadání: 8.2.2016 ***Termín odevzdání:*** 26.5.2016

Vedoucí práce: doc. Ing. Jaromír Kolouch, CSc.
Konzultant bakalářské práce: Ing. Ondřej Pavelka, Honeywell

doc. Ing. Tomáš Kratochvíl, Ph.D., *předseda oborové rady*

ABSTRAKT

Bakalářská práce se v první části zabývá vybráním vhodného standardu pro bezdrátový sběr dat v průmyslovém prostředí. Dále práce popisuje vlastnosti vybraného standardu ZigBee. Další část práce popisuje jednotlivé, běžně dostupné ZigBee moduly a je zde provedeno i jejich vzájemné porovnání. V praktické části práce je představen přenosový řetězec a následně důkladný popis jednotlivých bloků. V poslední části práce jsou naměřené výsledky.

KLÍČOVÁ SLOVA

ZigBee, Referenční model ZigBee, Mesh topologie, zabezpečení, ZigBee moduly, Xbee, přenosový řetězec, modul pro sběr dat

ABSTRACT

In the first part of Bachelor thesis is discussed selecting an appropriate standard for wireless data acquisition in industrial environments. In the next part are described the properties of the selected standard ZigBee. The next part is used to introduce and comparison of different ZigBee modules, which are available. In the practical part is represent transmission chain and its description. In the last section of Bachelor thesis are measured results.

KEYWORDS

ZigBee, Reference Model ZigBee, Mesh topology, security, ZigBee modules, Xbee, transmission chain

MACURA, J. *Bezdrátový sběr dat v průmyslovém prostředí*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav radioelektroniky, 2016. 31 s., 2 s. příloh. Bakalářská práce. Vedoucí práce: doc. Ing. Jaromír Kolouch, CSc.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma Bezdrátový sběr dat v průmyslovém prostředí jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne ....

(podpis autora)

PODĚKOVÁNÍ

Ve své práci bych rád poděkoval vedoucímu bakalářské práce doc. Ing. Jaromíru Kolouchovi, CSc. a konzultantovi z firmy Honeywell panu Ing. Ondřeji Pavelkovi za pomoc ve formě konzultací a cenných rad při psaní práce.

V Brně dne ....

(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

V dnešní době jsou velice rozšířené bezdrátové technologie. Používají se v mnoha odvětvích, například pro domácí využití, v medicíně pro dálkovou kontrolu pacientů, v průmyslovém prostředí pro sběr dat. Tato práce je zaměřena pouze na průmyslové prostředí.

Cílem bakalářské práce je vybrat vhodný standard pro bezdrátový sběr dat v průmyslovém prostředí. Vybraný standard musí splňovat podmínky, jako je topologie typu Mesh, odolnost proti průmyslovému rušení, zabezpečený přenos dat.

Zvolený standard by měl být důkladně prostudován a v práci popsán. Na základě získaných teoretických poznatků by měla být vytvořena prototypní síť, která prokáže teoretické poznatky.

Při nedostatečné ochraně dat při přenosu by měla být prozkoumána možnost dalšího zabezpečení. Šifrování jako zabezpečení dat by mohlo zanést do sítě nezanedbatelné zpoždění. V souvislosti s tím je potřeba změřit dobu zašifrování dat.

Pro ověření správné funkce sítě by měly být zkonstruovány bezdrátové moduly pro přenos dat. V našem případě budou data reprezentována teplotami. Tato data by měla být zašifrována a přenesena do centrálního bodu, kde budou dešifrována a zpracována.

1 VÝBĚR STANDARDU

Jako první musí být vybrán vhodný standard, který bude vyhovovat zadaným parametrům.

Navrhovaná síť bude sloužit ke sběru dat z čidel. Nejdůležitějším parametrem je samozřejmě cena, ale ta musí být brána v potaz až po výběru vhodného standardu. Důležitým zadaným parametrem je odolnost proti průmyslovému rušení. Proto musíme dbát, aby vybraný standard byl schopen potvrzovat přijatá data, popřípadě si o ně znovu zažádat. Dále je známo, že v síti se bude přenášet malý objem dat (100Kb/s). Vzhledem ke vzdálenosti komunikačního dosahu budou moduly umístěny ve výrobních halách. Z toho vyplývá, že potřebný dosah bude v řádu desítek až stovek metrů.

Na obrázku 1-1 je tabulka s přehledem vybraných standardů a jejich základní parametry.

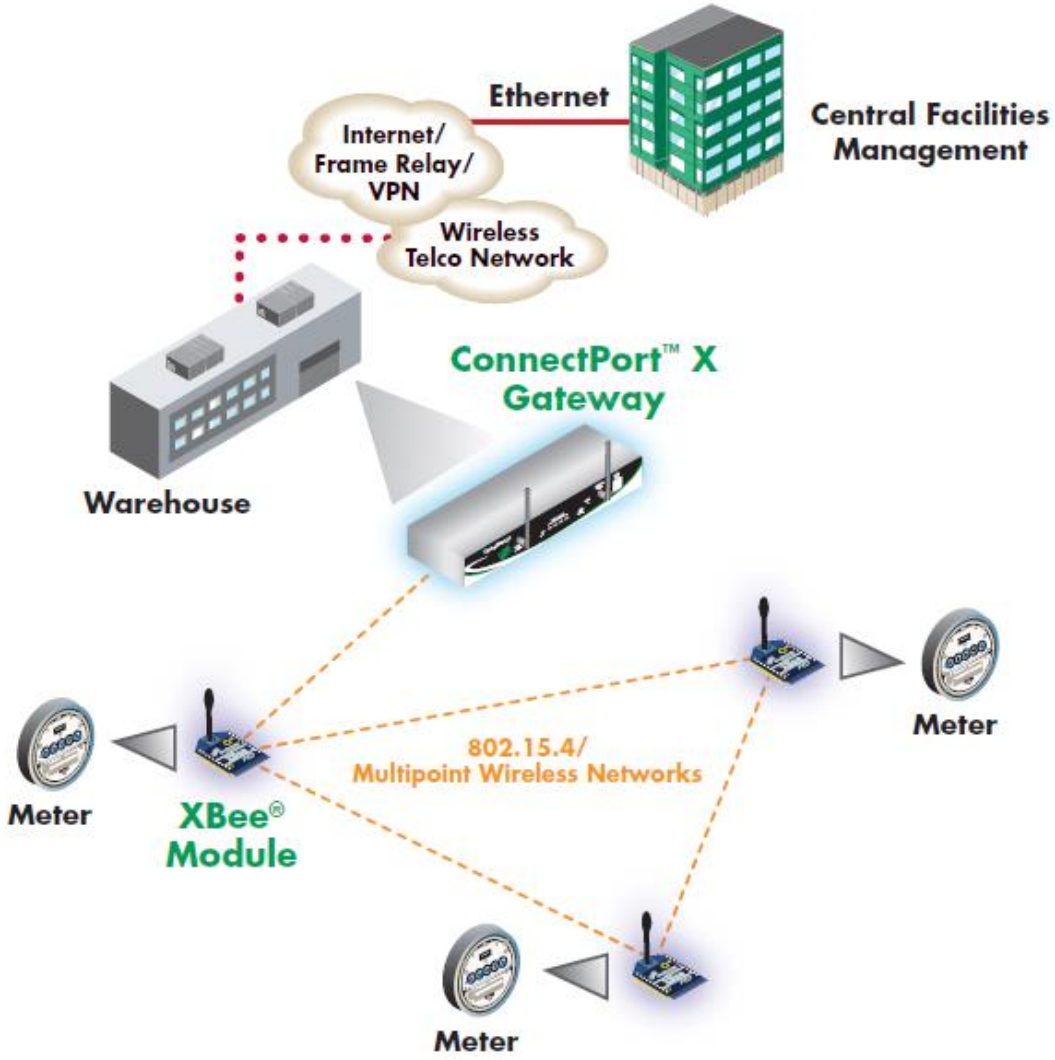
Obchodní jméno Standard	GPRS/GSM 1xRTT/CDMA	Wi-Fi™ 802.11b	Bluetooth™ 802.15.1	ZigBee™ 802.15.4
Aplikační zaměření	Široké oblasti Hlas & Data	Web, Email, Video	Náhrada za kabel	Monitorování & Řízení
Systémové zdroje (paměť)	16MB a více	1MB a více	250KB a více	4KB - 32KB
Životnost baterií (dny)	1-7	0.5 - 5	1 - 7	100 – 1 000 i více
Max. velikost sítě (počet uzlů/síť)	1	32	7	65 000 (příp. až 2^{64})
Přenosová rychlost (Kb/s)	64 – 128	11 000	720	20 - 250
Komunikační dosah (m)	1 000 i více	1 - 100	1 - 10	1 – 100
Výhody	Dosažitelnost, Kvalita	Rychlost, Flexibilita	Cena, Jednoduchost	Spolehlivost, Výkon/Cena

Obrázek 1-1: Přehled standardů a jejich parametry, převzato z [1]

2 ZIGBEE

ZigBee je standard platný od roku 2004, nesoucí označení IEEE 802.15.4. Jde o standard pro osobní bezdrátové sítě WPAN (Wireless Personal Area Network). Standard je primárně určen pro průmyslovou automatizaci a řízení, tedy tam, kde není nutné přenášet velké množství dat, to je do 250 Kb/s. V dnešní době již existují ZigBee moduly, které dokážou přenášet data rychlostí až 2 Mb/s.

Na obrázku 2-1 je naznačen sběr dat a následné předání až k centrálnímu bodu.



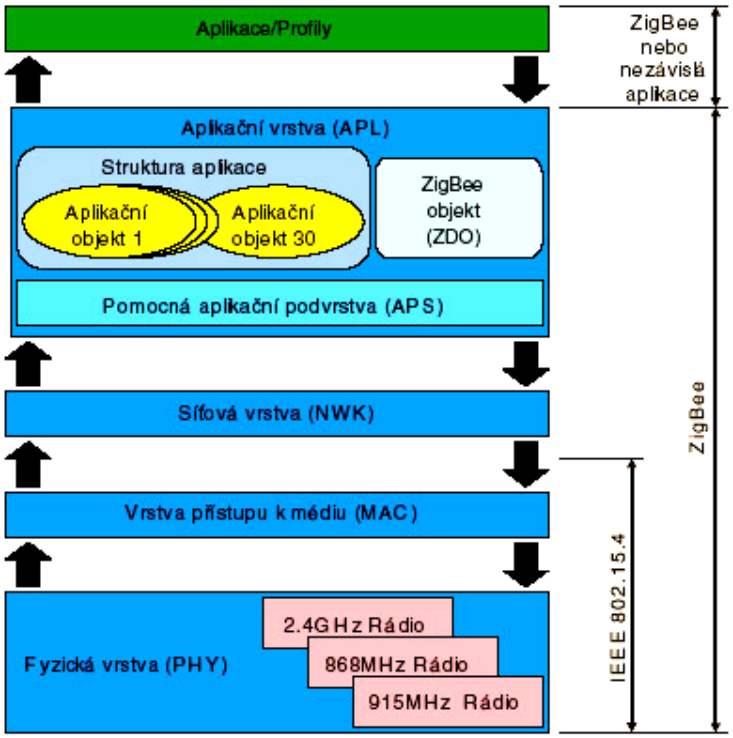
Obrázek 2-1: Přenosový řetězec, převzato z [2]

3 REFERENČNÍ MODEL

Model vychází ze sedmivrstvého modelu ISO/OSI. U ZigBee jsou použity pouze vrstvy, které zajišťují nízkou spotřebu energie a nízkou přenosovou rychlost dat. Fyzická vrstva (PHY) a Přístupová vrstva k médiu (MAC) jsou definované standardem IEEE 802.15.4. ZigBee Alliance potom definuje ostatní vyšší vrstvy, kterými jsou Síťová vrstva (NWK) a Aplikační vrstva (APL). Vrstvy mezi sebou komunikují přes tzv. přístupový bod služby (SAP). SAP je schopnost protokolových vrstev vyžádat si služby od jiné protokolové vrstvy, například přístupový bod služby vrstvy PHY (PD-SAP) je místo, kde vrstva MAC požaduje kteroukoli datovou službu z PHY vrstvy.

Bezpečnostní prvky jsou definovány v obou standardech.

Obrázek 3-1 znázorňuje referenční model pro ZigBee.



Obrázek 3-1: Referenční model ZigBee, převzato z [3]

3.1 Fyzická vrstva (PHY)

Fyzická vrstva je nejblíže hardwarové vrstvě a specifikuje komunikaci mezi zařízeními, hardwarové požadavky, jako je citlivost přijímače, a výstupní výkon vysílače. Při komunikaci mezi zařízeními je jako přenosové médium použita elektromagnetická vlna. Fyzická vrstva má za úkol zapnutí a vypnutí vysílače/přijímače, vysílat a přijímat data, nastavení přenosové frekvence, zajištění volného kanálu a zjišťování kvality spoje.

3.1.1 Kmitočtová pásma a přenosové kanály

ZigBee používá 3 frekvenční pásma:

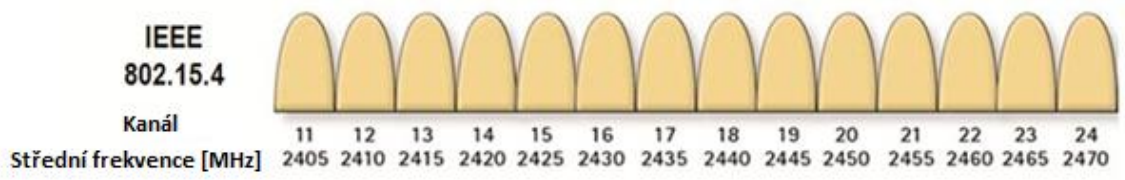
- 868 – 868,6 MHz
- 902 – 928 MHz
- 2400 – 2483,5 MHz

Pásmo 868 MHz je používané v Evropě pro spoustu aplikací, včetně vysílání na krátké vzdálenosti. Zbylá dvě pásma (915 MHz a 2,4 GHz) jsou pásma z takzvaného ISM (Industrial, Scientific, and Medical). ISM jsou volná pásma pro rádiové vysílání v oborech průmyslovém, vědeckém a zdravotnickém. Frekvenční pásmo 915 MHz se používá hlavně v Severní Americe, zatímco 2,4 GHz se používá celosvětově.

Frekvenční pásmo 2,4 GHz se jeví jako nejvhodnější, proto to bude další parametr při výběru modulů. Pro tento kmitočet jsou definovány 11-26 kanály. Pro střední frekvenci jednotlivých kanálů platí vztah [11]:

$$\text{Střední frekvence} = 2405 + 5 * (\text{Číslo kanálu} - 11)\ [\text{MHz}]$$

Na obrázku 3-2 jsou naznačeny všechny kanály z frekvenčního pásma 2,4 GHz a jejich střední frekvence.



Obrázek 3-2: Zastoupení kanálů v 2,4 GHz pásmu, převzato z [10]

3.1.2 Energy Detection (ED)

Zařízení připravené vysílat data musí nejprve přejít do přijímacího módu a zjistit úroveň signálu v kanálu, kde chce vysílat. Tento postup se nazývá detekce energie (ED). Při ED se zjišťuje pouze úroveň signálu, nikoli jeho typ či původ.

Standard IEEE 802.15.4 umožňuje 10 dB rozdíl mezi citlivostí přijímače a ED. Pokud má tedy přijímač citlivost -90 dBm, ED musí naměřit nejméně do -80 dBm, přičemž měřící rozsah musí být nejméně 40 dB. O provedení detekce žádá MAC vrstva a PHY vrstva jí vrací 8 - bitové číslo, indikující energetickou úroveň.

V pracovních halách, kde budou moduly umístěny, by na pracovním kmitočtu nemělo být rušení vyšší než je citlivost modulů.

3.1.3 Carrier Sense (CS)

CS ověřuje, podobně jako ED, zda je frekvenční kanál k dispozici. Na rozdíl od ED je v CS signál demodulovaný pro ověření toho, že detekovaný signál je v souladu s IEEE 802.15.4 PHY.

3.1.4 Posouzení kvality spoje

V ZigBee existují dva parametry, podle kterých lze posoudit kvalitu spoje mezi zařízeními.

První z nich je The Link Quality Indicator (LQI), neboli indikátor kvality spojení, který kvalitu spojení vyhodnocuje na základě chybně přijatých paketů. LQI může nabývat hodnot <0 – 255>, přičemž vyšší číslo značí vyšší kvalitu přenosové linky. LQI je dále hlášeno MAC vrstvě a je přístupné i pro NWK a APL vrstvy pro různé analýzy. Například NWK vrstva se díky LQI může rozhodnout, jak bude směrovat pakety v síti.

Další možností, jak nahlížet na kvalitu spoje, je parametr nazývaný „odstup signál - šum“ (SNR). Při použití tohoto způsobu posouzení kvality spoje porovnáváme velikost přijatého signálu, neboli Received signal strength (RSS), se šumem v daném pásmu a dostaneme hodnotu SNR. Čím vyšší hodnota SNR je, tím se snižuje možnost výskytu chyby v přenášeném paketu.

3.1.5 Clear channel assessment (CCA)

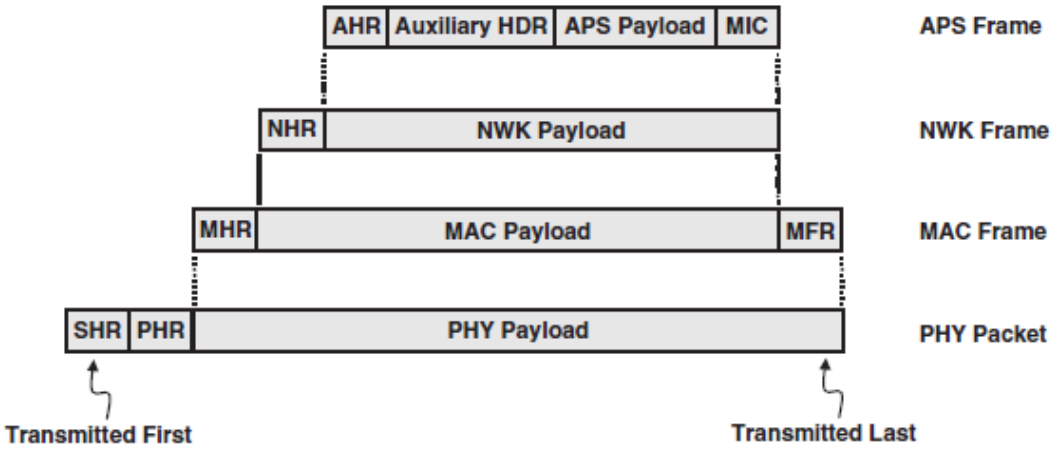
ZigBee využívá jako přístupovou metodu Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA). CSMA-CA před každým vysíláním nejprve zjistí stav kanálu, po kterém chce vysílat (CCA), čímž je zajištěno, že kanál již není používán. Pro posuzování, zda je kanál volný či ne, nejprve provede ED. Pokud je již pásmo obsazeno, ED neumožňuje zjistit, zda se jedná o IEEE 802.15.4 signál. Alternativně se dá využít metoda CS, která zprávu demoduluje. V případě, že kanál volný není, vygeneruje se pseudonáhodný čas, za který se kanál otestuje znovu.

Ve standardu IEEE 802.15.4 existují 3 režimy pro CCA, přičemž každé zařízení musí být schopno podporovat všechny zmíněné:

- Režim 1: Při rozhodování, zda je kanál obsazený či ne, se bere v úvahu pouze měření ED. Pokud je měřená hodnota vyšší než prahová, která je udána výrobcem, kanál je považován za obsazený.
- Režim 2: Režim 2 využívá pouze výsledku CS. Kanál je vyhodnocen jako obsazený, pokud CS naměří signál v souladu s IEEE 802.15.4.
- Režim 3: Jedná se o kombinaci předchozích režimů. Pokud jeden z režimů nesplňuje své podmínky, kanál se vyhodnotí jako obsazený.

3.1.6 Formát paketu PHY

Na obrázku 3-3 je zobrazena struktura ZigBee paketu a obsah jednotlivých vrstev.



Obrázek 3-3: Struktura ZigBee paketu a obsah jednotlivých vrstev, převzato z [11]

Paket je tvořen Synchronization header (SHR), PHY header (PHR) a PHY Payload. SHR slouží k synchronizaci přijímače, zatímco PHR obsahuje informace o délce rámce. PHY Payload v sobě ukrývá hlavičky z vyšších vrstev a užitečná data.

3.2 Vrstva přístupu k médiu (MAC)

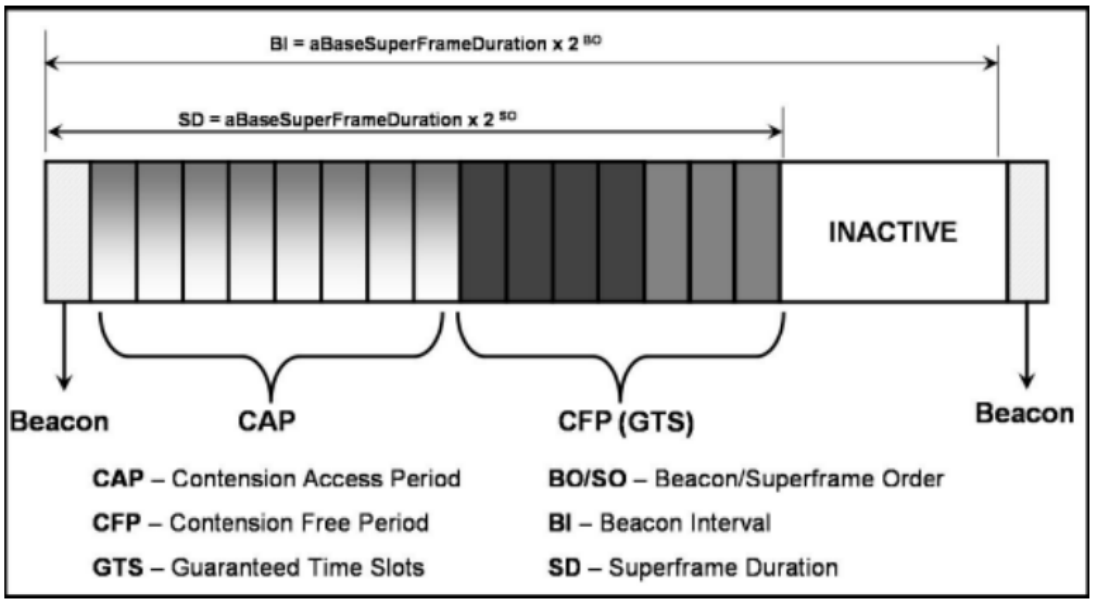
MAC vrstva leží mezi PHY vrstvou a NWK vrstvou. MAC vrstva zajišťuje generování tzv. beacons rámců (pokud je zařízení koordinátor) pro synchronizaci zařízení v síti, využívá CSMA-CA pro přístup na kanál, řídí garantovaný časový interval (GTS), ověřování platností rámců a potvrzení doručených rámců.

3.2.1 Beacon-Enabled Operation and Superframe Structure

Zařízení, která chtějí vysílat, musí nejdříve dostat přístup na kanál. V prvním případě mohou použít mechanismus CSMA-CA a první zařízení, které najde kanál, začne vysílat. Druhá možnost je dostat od koordinátora konkrétní GTS. Pro zajištění GTS musí koordinátor synchronizovat všechna zařízení v síti. K synchronizaci se používají tzv. Beacon zprávy.

V síti, kde budou Beacon zprávy povoleny, můžeme využívat super rámců. V super rámci se mohou vyskytnout až tři typy časových období. Nejprve je to doba, kdy koordinátor komunikuje se všemi zařízeními (Contention Access Period = CAP) v rámci privátní sítě (PAN). Následuje volný čas pro odesílání dat (Contention-Free Period = CFP), obsahující GTS, které slouží pro prioritní a pomalá zařízení. Maximální počet GTS je omezen na 7 slotů. Následuje neaktivní sekvence, kdy se všechna zařízení v síti uspí.

Neexistuje žádná záruka, že během CAP jakékoli zařízení obsadí vysílací kanál dle potřeby. Proto je zde výhodné využít období CFP, zaručující časový slot pro konkrétní zařízení. Tato volba je vhodná tam, kde je zapotřebí přesné časové odebírání dat. Na obrázku 3-4 je zobrazeno schéma super rámce.



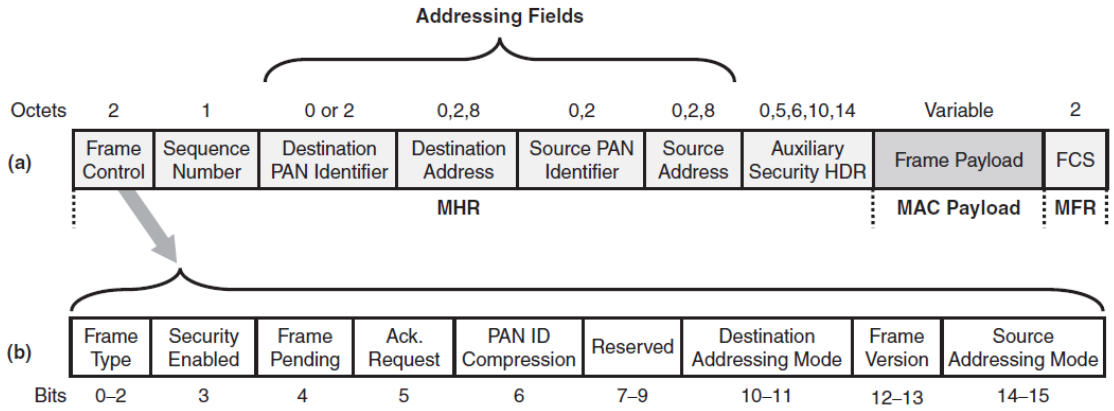
Obrázek 3-4: Schéma Super rámce, převzato z [11]

3.2.2 Non-Beacon

V síti, kde máme Beacon zprávy vypnuté, nelze použít super rámec. Oproti Beacon-enable síti má ale výhodu vyšší životnosti baterií. Díky absenci synchronizačních zpráv se celá síť neprobouzí jen kvůli synchronizaci. Tato konfigurace je tedy výhodnější tam, kde je k dispozici pouze napájení z baterií.

3.2.3 Obecný formát MAC rámce

Na obrázku 3-5 a) je uveden obecný popis MAC rámce a na obrázku 3-5 b) detailní popis jeho kontrolního pole. Obecný MAC rámec se skládá ze tří částí, a to z MAC header (MHR), MAC Payload a MAC footer (MFR).



Obrázek 3-5: a) obecný popis MAC rámce b) Kontrolní pole MAC rámce, převzato z [11]

První pole z MAC rámce je Frame Control, který v sobě dále definuje další typy podpolí (beacon, data, potvrzení a MAC příkazy). Pokud podpole Security Enabled nastavíme do jedničky, do MAC rámce se přidá pole Auxiliary a bude součástí MAC rámce. V opačném případě se toto pole v MAC rámci neobjeví.

Frame Pending se používá jako část nepřímé metody při přenosu dat. Pokud je toto pole nastaveno na 1, znamená to, že jsou k dispozici data pro vysílání. Pokud při vysílání dat nastavíme Ack. Request do jedničky, požadujeme po přijímací straně potvrzovací paket.

PAN ID Compression je nastaven v jedničce, pokud je zdrojový a koncový PAN ID shodné. Slouží tedy k zabránění přenosu redundantních dat. Destination a Source Addressing Mode určuje režim adresování (16 - bitové nebo 64 – bitové).

Další pole v MAC rámci je Sequence number. Toto pole slouží pro případ, že budou přijaty dva rámce se stejným sekvenčním číslem. To znamená, že jeden z rámců byl znovu poslán. Pak se přijme pouze jeden z nich a druhý je ignorován.

Pole Auxiliary security, jak již bylo řečeno, je aktivováno bitem v poli Security enabled. Toto pole obsahuje informace o zabezpečení a bezpečnostních klíčích použitých k ochraně MAC rámců.

Poslední pole je Frame Check Sequence (FCS), které slouží pro kontrolu špatně přijatých rámců.

3.2.4 Typy rámců v MAC vrstvě

V předchozí kapitole byl probrán obecný rámec MAC vrstvy a důkladný popis jeho jednotlivých polí. V MAC vrstvě se můžou vyskytnout 4 typy rámců.

- Beacon Frame
- Data Frame
- Acknowledgment Frame
- MAC Command Frame

Beacon Frame

Vlastnosti toho rámce vycházejí z vlastností sítě Beacon-enable. Rámec tedy slouží pro synchronizaci a může být vyslán pouze koordinátorem. MAC payload navíc obsahuje super rámec typický pro síť Beacon-enable s GTS polem.

Beacon frame je zobrazen na obrázku 3-6.

Octets: 2	1	4/10	2	variable	variable	variable	2
Frame control	Sequence number	Addressing fields	Superframe specification	GTS fields (Figure 38)	Pending address fields (Figure 39)	Beacon payload	FCS
MHR			MAC payload				MFR

Obrázek 3-6: Beacon frame, převzato z [10]

Data Frame

Datový rámec slouží pro přenos užitečných dat. Na obrázku 3-7 je znázorněno jeho schéma.

Octets: 2	1	(see 7.2.2.2.1)	variable	2
Frame control	Sequence number	Addressing fields	Data payload	FCS
MHR			MAC payload	MFR

Obrázek 3-7 Schéma Datového rámce, převzato z [10]

Acknowledgment Frame

Acknowledgment Frame, neboli potvrzovací rámec, slouží k potvrzení o příjmu dat. Na obrázku 3-8 je znázorněné schéma Acknowledgment Frame.

Octets: 2	1	2
Frame control	Sequence number	FCS
MHR		MFR

Obrázek 3-8: Schéma Acknowledgment Frame, převzato z [10]

MAC Command Frame

MAC Command Frame využívá koordinátor pro vysílání síťových klíčů a jiných konfiguračních nastavení. Obrázek 3-9 zobrazuje schéma MAC Command Frame.

Octets: 2	1	(see 7.2.2.4.1)	1	variable	2
Frame control	Sequence number	Addressing fields	Command frame identifier	Command payload	FCS
MHR			MAC payload		MFR

Obrázek 3-9: Schéma MAC Command Frame, převzato z [10]

3.2.5 Frame Check Sequence (FCS)

Na odhalování případných chyb v datovém paketu využívá FCS v IEEE 802.15.4 16 - bitový FCS na základě cyklicky redundantní kontroly (Cyclic Redundancy Check = CRC).

CRC využívá následující algoritmus: Všechny bity v MHR a v MAC payload jsou považovány za koeficienty polynomu. Tento polynom je dále dělen jiným polynomem, který je znám jak na přijímací tak i odesílací straně. Vygenerovaným cyklickým kódem je poté uložen do pole FSC. Na přijímací straně se provede stejná operace a očekává se stejný výsledek. V ZigBee se používám polynom ve tvaru [11]:

$$G_{16}(x) = x^{12} + x^{12} + x^5 + 1$$

3.3 Síťová vrstva (NWK)

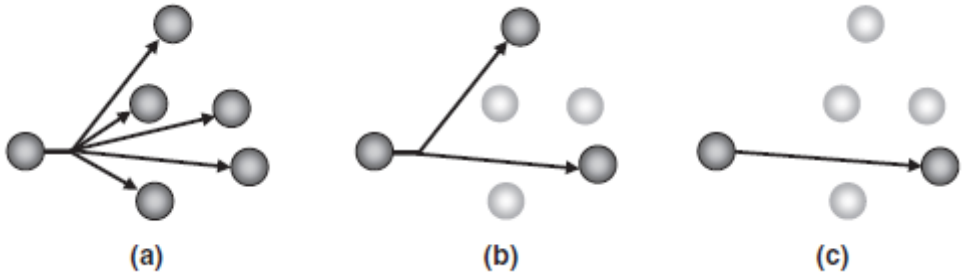
Síťová vrstva je zodpovědná za správu sítě a směrování v ní. Směrování je činnost, kdy se vybírá nejlepší cesta skrze síť k doručení zprávy. Koordinátor a router zajišťují vytvoření a udržování trasy v síti. Koordinátor a router provádí zjišťování trasy ke koncovému zařízení. Dále NWK vrstva omezuje, přes tzv. počet hopů, konstantu, která představuje vzdálenost, kterou je paketům povolena cestovat v síti. Počet hopů se určí na straně odesílatele a v každém průchozím uzlu se sníží o jedna. To zabrání paketům putovat donekonečna sítí a tím ji zatěžovat.

V NWK vrstvě je koordinátor zodpovědný za založení nové sítě a výběr topologie. Koordinátor také přiřazuje síťové adresy zařízením v jeho síti, pokud není nastaveno statické adresování.

Ve vrstvě NWK se využívají 3 typy zpráv:

- Broadcast
- Multicast
- Unicast

Na obrázku 3-10 jsou uvedeny všechny tři typy zpráv.



Obrázek 3-10: Typy zpráv v ZigBee sítích a) Broadcast b) Multicast c) Unicast, převzato z [11]

Broadcast

Pokud je zpráva vyslána jako broadcast, znamená to, že bude odeslána na všechna zařízení v síti. V ZigBee sítích, kde je použito krátké adresování, se používá pro broadcast zprávu adresa 0xffff. ZigBee ale neumožňuje vysílat broadcast přes vícero sítí, neboli přes více sítí s rozdílnými PAN ID adresami. Pokud je tedy vyslána zpráva s PAN ID adresou 0xffff, je automaticky přenastavena na vlastní PAN ID vysílacího zařízení. V tomto typu předávání zprávy se neprovádí jeho potvrzení koordinátorovi.

Multicast

Zpráva vyslaná jako multicast bude přepravena pouze určité skupině zařízení. Skupina je identifikována podle 16 - bitového multicastového ID. Zařízení se stejným multicast ID tvoří společně jednu skupinu. Každé zařízení může být členem více než jedné skupiny.

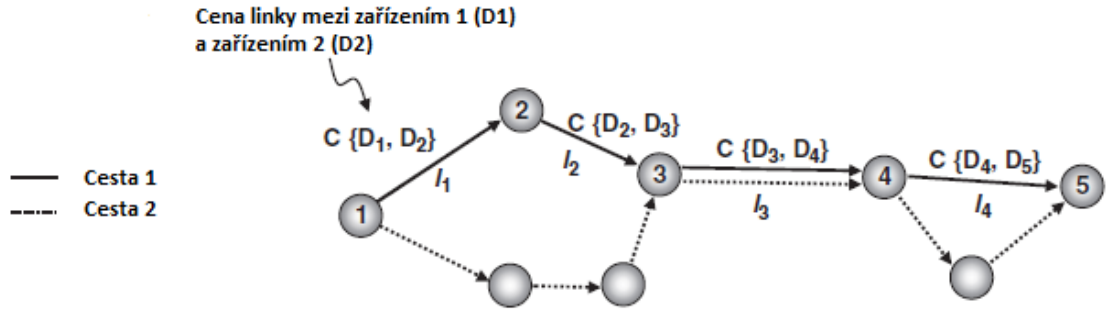
Unicast

Zpráva typu unicast znamená, že v síti je pouze jedno zařízení, pro které je zpráva určena. Nejčastěji se unicast využívá pro předání zpráv od koncového zařízení ke koordinátorovi, který zprávy předává do externí databáze.

3.3.1 Směrování

Směrování je proces, při kterém se vybírá nejvhodnější cesta pro přenos zprávy. Za objevování a udržování spojů v síti je zodpovědný koordinátor a router. Koncové zařízení těchto úkonů není schopné. Délka trasy se určuje jako počet hopů přes přenosové členy, včetně počátečního a koncového zařízení.

Na obrázku 3-11 je uveden příklad dvou cest. První cesta je dlouhá pět hopů, zatímco druhá cesta je dlouhá 7 hopů.



Obrázek 3-11: Příklad určení délky cest v síti, převzato z [11]

Počet hopů není jediný parametr, který má vliv na výběr přenosové cesty mezi komunikujícími zařízeními. Další parametry mohou být kvalita linky, energetická náročnost spoje. Pro zjednodušení se z těchto parametrů vytvoří jeden, zvaný cena linky. Čím nižší je pravděpodobnost správně doručeného paketu, tím roste cena linky. Ta je na obrázku 3-11 naznačena písmenem *C* a dvěma proměnnými (přenosová zařízení v síti) v závorkách.

V ZigBee se používá jednoduchý algoritmus [11]:

$$C\{l\} = \left(\frac{1}{Pl^4}\right)$$

pro zjištění ceny linky. Výsledek se vždy zaokrouhluje na celá čísla a ty mohou nabývat hodnot od 0 do 7. Proměnná *Pl* představuje pravděpodobnost úspěšného doručení paketu.

Další důležitou funkcí v NWK vrstvě je vytvářet a udržovat si směrovací tabulku. Tuto činnost vykonává pouze koordinátor a router. Směrovací tabulka slouží k vytvoření trasy do určité cílové adresy.

Další tabulka v NWK vrstvě je Route Discovery table. Tato tabulka se používá v průběhu objevování nových cest. Tabulka obsahuje parametry jako je cena linky, adresa zdrojového zařízení (zařízení, které požádalo o trasu) a adresu cílového zařízení, do kterého se má směrovat. Výsledek objevené trasy bude vyslán zpět ke zdroji zprávy, kde zdrojové zařízení vybere nejvhodnější cestu. Obsah v této tabulce je pouze dočasný a zmizí po určitém čase (v řádu milisekund).

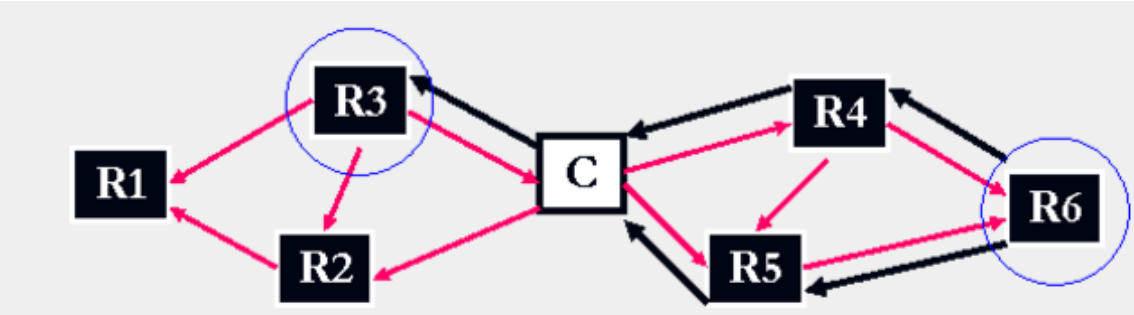
Poslední tabulkou v NWK vrstvě je tabulka sousedů. Ta obsahuje informace o sousedních zařízení. Tabulka je aktualizována po každém přijetí paketu od sousedního zařízení.

3.3.2 Objevování cest

Pro objevování trasy v síti se v ZigBee standardně používá metoda zvaná Route Discovery. Existují i další metody, které mohou být typické pro daného výrobce. V této práci je popsána pouze metoda Route Discovery.

Hledání cesty touto metodou bude nejlépe vysvětleno na modelovém příkladu na obrázku 3-12. Růžovou barvou jsou naznačeny zprávy typu broadcast a černou unicast zprávy. Zařízení, v našem případě R3, hledající cílového adresáta, v našem případě R6, vyšle Route Request Packet broadcast s následujícími informacemi:

1. Route Request ID
2. Síťovou adresu cílového zařízení
3. Cenu linky
4. Síťovou adresu zdrojového zařízení



Obrázek 3-12: Modelová situace pro nalezení cesty pomocí Route Discovery, převzato z [5]

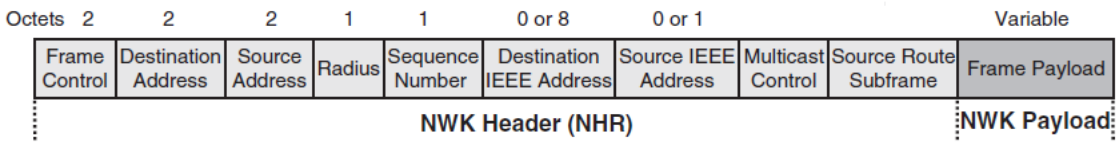
Po nalezení cesty do cíle přes uzel R4, vytvoří uzel R6 Route Discovery tabulku a odešle unicast zprávu (s aktualizovanou cenou linky). Informace v unicast zprávě mají stejné složení, jako tomu bylo u bradcastu zprávy.

Pokud cílový uzel R6 obdrží Route Request Packet od jiného zařízení, např. R5, porovná cenu linky dané trasy s původní přes R4. Pokud bude cena linky lepší než předchozí, vyšle se opět unicast po nově nalezené trase a uzly po cestě aktualizují své Route Discovery table. Pokud je cena linky horší, paket se zahodí. Po ustálení stavu se tedy komunikuje přes uzel R4 do cíle R6. Může se stát, že uzel R4 přestane pracovat a tato trasa by byla zcela ochromena. Jednou ze ZigBee vlastností je Self – Healing, což

znamená, že se zprávy předávají více než jednou cestou. Pokud tedy uzel R4 přestane být funkční po předem určeném počtu zahozených paketů, začne se v síti znovu hledat nová cesta. Celý proces objevování cesty se zopakuje. Self-healing je použitelný pouze u topologie typu Mesh.

3.3.3 Typy rámců v NWK vrstvě

Na obrázku 3-13 je naznačen formát NWK rámce. První pole Frame Control slouží pro nastavování parametrů, jako tomu bylo u vrstvy MAC. Dále jsou zde uvedeny pole Destination Address a Source Address (cílová a zdrojová adresa) a Destination IEEE Address a Source IEEE Address. Ty se od sebe liší velikostí, protože v ZigBee existují dva typy adres (viz. Kapitola Adresování). Multicast Control pole se v rámci objeví, jedině pokud je zpráva vyslána jako multicast a slouží ke kontrole, zda se dostala ke všem adresátům. Pole Source Route Subframe je velice důležité, při použití krátkého, 16 - bitového adresování, drží adresy všech uzlů, přes které se má zpráva přenést.



Obrázek 3-13: Zobrazení obecného formátu NWK rámce, převzato z [11]

Modifikací obecného NWK rámce je mnoho. V této práci jsou uvedeny pouze jejich názvy, podle kterých se dá vydedukovat funkce. Jsou to:

- Route Request
- Route Reply
- Route Error
- Leave
- Rejoin Request

3.4 Aplikační vrstva (APL)

Aplikační vrstva je nejvyšší vrstvou v ZigBee. APL vrstva je tvořena ze tří částí a to Application support (APS), ZigBee Device Object (ZDO) a application Framework. Podvrstva APS slouží jako rozhraní mezi APL a NWK. Application Framework je softwarová podpora, která kontroluje a pomáhá řídit naše aplikace. ZDO poskytuje rozhraní mezi APS a Application frameworkem. ZDO obsahuje funkce, které jsou společné ve všech aplikacích, jako je konfigurace role zařízení (koordinátor, router, koncové zařízení).

4 TYPY ZAŘÍZENÍ A JEJICH ROLE V SÍTÍCH ZIGBEE

4.1 Typy zařízení

Zařízení můžeme dělit do 2 skupin:

- Plně funkční zařízení (FFD)
- Zredukované funkční zařízení (RFD)

FFD zařízení jsou schopna vykonat jakýkoli úkol popsaný IEEE 802.15.4 standardem a může se zhostit jakékoli role v síti. Například FFD může komunikovat s ostatními zařízeními v síti, ale RFD může komunikovat pouze s FFD. RFD je tedy primitivnější zařízení pro jednodušší aplikace jako zapínání/vypínání přepínače.

4.2 Role zařízení

V ZigBee standardu rozdělujeme 3 základní typy zařízení:

- Koordinátor (K)
- Router (R)
- Koncové zařízení (KZ)

Každá síť musí mít koordinátora. Koordinátor spravuje celou síť a tvoří koncový bod, přes který se sbírají data od KZ. Dále má na starost přidělování adres, určuje topologii sítě, synchronizuje zařízení v síti.

Router slouží jako obousměrné zařízení. Používá se jako spojovací článek v sítích tam, kde koordinátor není v přijímací vzdálenosti od Koncového zařízení.

Koncová zařízení tráví většinu času v režimu spánku a probouzí se pouze tehdy, pokud je potřeba poslat data. Daty mohou být naměřené hodnoty teploty, otáček v motoru atd.

5 TOPOLOGIE SÍTÍ V ZIGBEE

Standard ZigBee podporuje čtyři různé typy topologií:

- Rovný s rovným (Peer-to-peer)
- Hvězda (Star)
- Strom (Tree)
- Mesh

5.1 Rovný s rovným (Peer-to-peer)

V topologii rovný s rovným může každé zařízení komunikovat přímo s jiným zařízením v jeho blízkosti. Není zde určen koordinátor, protože v tomto typu topologie může být každé FFD koordinátor. Dá se říct, že první zařízení v síti bude koordinátor.

5.2 Hvězda (Star)

V topologii hvězda může každé zařízení v síti komunikovat pouze s koordinátorem nebo přes koordinátora. Tato topologie je velice náchylná na ztrátu dat. Pokud vypadne spoj mezi koordinátorem a ED, data nebudou přenesena a dojde k jejich ztrátě. Pokud by vypadl koordinátor, celá síť bude ochromena a nefunkční.

5.3 Strom (Cluster)

Topologie Strom je ve skutečnosti rozšíření Star topologie, a to tak, že mezi koordinátora a koncové zařízení přidáme router. Router může spravovat celou větev koncových zařízení. Tato topologie nám už tedy nabízí větší možnosti (např. při potřebě obcházení překážek).

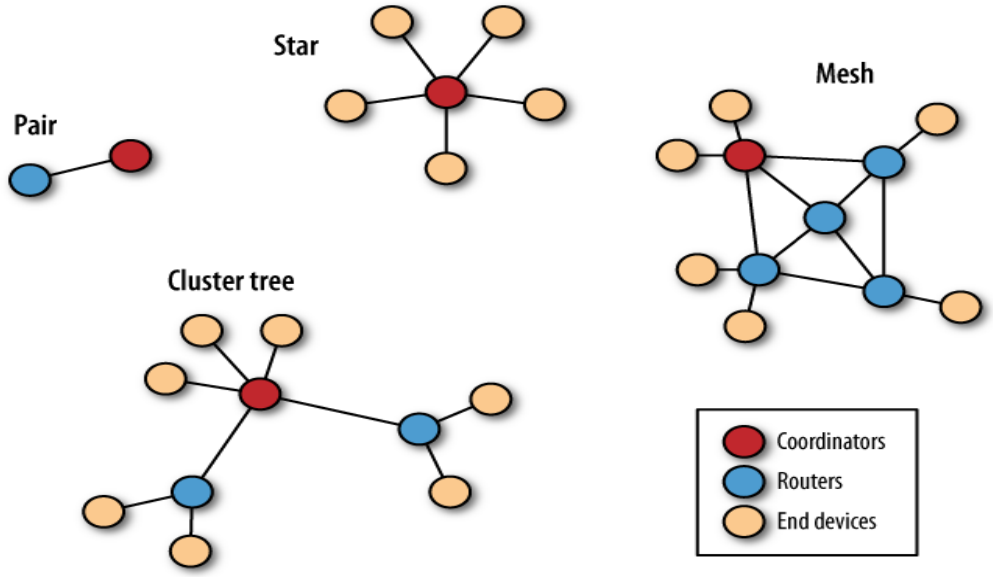
5.4 Mesh

Mesh topologie je skloubení topologií Hvězda a Strom. Koncové zařízení může komunikovat s koordinátorem více cestami. Pokud je koncové zařízení v přímém dosahu koordinátora, může s ním komunikovat přímo a pokud ne, využije libovolnou nejvýhodnější cestu přes router.

Tato topologie je ze všech uvedených nejspolehlivější. Pokud vypadne uzel v síti, zpráva si najde jinou cestu do cíle.

Některé starší ZigBee moduly Mesh topologii nepodporovaly. Proto podpora Mesh topologie bude další parametr v našem výběru modulů.

Na obrázku 5-1 jsou zobrazeny všechny jmenované topologie včetně barevného rozdělení typů zařízení.



Obrázek 5-1: Podporované topologie v sítích ZigBee, převzato z [12]

6 ADRESOVÁNÍ

Standard IEEE 802.15.4 využívá 2 druhy adres:

- 16 – bitové (krátké adresování)
- 64 – bitové (dlouhé adresování)

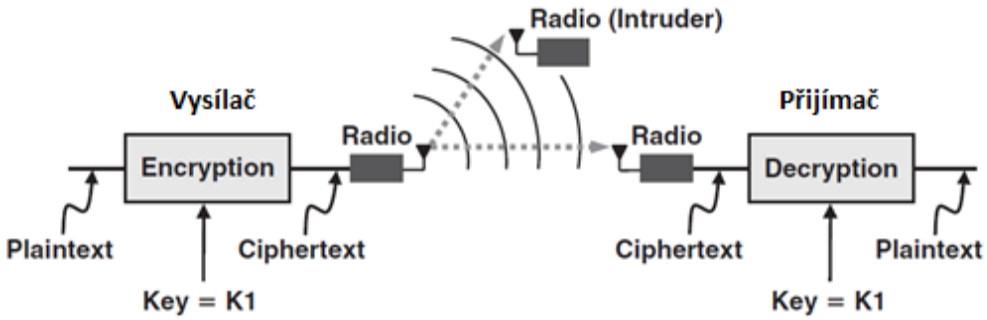
Krátké adresování umožňuje redukci délky vysílané zprávy a šetří místo v paměti. V kombinaci s unikátním PAN identifikátorem může být použito pro komunikaci mezi nezávislými sítěmi. PAN ID slouží k rozlišení překrývajících se sítí. Maximální počet zařízení při použití krátkého adresování v síti je 2^(16). Při využití dlouhého adresováni je to tedy 2^(64), jedná se o nelimitovanou síť.

7 ZABEZPEČENÍ

V této kapitole je probráno šifrování v sítích ZigBee a ověřování zařízení a dat.

7.1 Šifrování

Šifrování je metoda pro utajení přenášené zprávy převodem do podoby, která je čitelná pouze speciálním algoritmem nebo klíčem. Standard ZigBee pro šifrování využívá Advanced Encryption Standard (AES). Na obrázku 7-1 je zobrazen základní koncept šifrování.



Obrázek 7-1: Mechanismus základního šifrování, převzato z [11]

Nezašifrovaná zpráva se označuje jako Plaintext. Po zašifrování pomocí klíče K1 se zpráva nazývá Ciphertext. Poté je zpráva přenesena a na přijímací straně dešifrována.

Algoritmus samotného AES je veřejně dostupný, ale hodnota klíče je vždy tajná. Klíč je N-bitové (N = 8, 16, 32, 64, 128, 256) binární číslo. Při použití 8 - bitového klíče stačí útočníkovi vyzkoušet 2^8 (256) možností pro zisk klíče. Ve standardu ZigBee se používá 128 - bitová délka klíče, což znamená 2^128 (3,4E38) možností. To už je na prolomení velice výpočetně obtížné. Z obrázku 7-1 je patrné, že je klíč na vysílací a přijímací straně stejný. Tato metoda se nazývá metoda symetrického klíče. ZigBee standard podporuje pouze metodu symetrického klíče. Klíč tedy musí být mezi jednotlivými zařízeními distribuován.

Existují 2 druhy klíče při zabezpečené komunikaci:

- Linkový klíč
- Síťový klíč

Linkový klíč je sdílen mezi dvěma a pouze jen dvěma zařízeními, která využívají ke komunikaci zprávy typu unicast. Síťový klíč je sdílen v celé síti zprávou typu broadcast. Každá zabezpečená ZigBee síť má zařízení zvané Trust centrum. Trust centrum je vždy pouze jedno v síti (určené koordinátorem) a slouží k distribuci síťového klíče.

Trust centrum využívá dva pracovní režimy:

- Pro komerční využití
- Pro nekomerční využití

V této práci je popsán pouze režim komerční, neboť ten je cílem práce. V komerčním režimu má Trust centrum za úkol udržovat seznam zařízení v síti, master klíč, linkový a síťový klíč. Každý přijatý NWK rámec se kontroluje, zda za se jedná o originál. V případě duplikátu není rámec přijat.

Pro předání linkového klíče existují tři metody:

- Předinstalace
- Key transport
- Key establishment

Předinstalace

V metodě Předinstalace je již od výrobce (například pomocí DIP přepínače) možnost zvolit si předprogramovaný klíč. Tato metoda je velice bezpečná, jelikož není nutné žádat Trust centrum o klíč.

Key transport

V této metodě si zařízení vyžádá heslo od Trust centra. Trust centrum může vyslat klíč žádajícímu zařízení po, v tu chvíli nezabezpečeném, spojení. V tento okamžik je síť zranitelná. Existuje zde ještě možnost použití tzv. key-transport key, neboli externí klíč, který je použit při přenosu Key transport mezi Trust centrem a žádajícím zařízením.

Key establishment

Tato metoda je založena na protokolu Symmetric-Key Key Establishment (SKKE). První ze zařízení musí mít předdefinovaný master klíč. Master klíč musí být předdefinovaný i na druhém zařízení. Jedno ze zařízení vyšle specifickou zprávu, ze které obě zařízení odvodí linkový klíč, za předpokladu stejného master klíče. Pro síťový klíč tato metoda nejde použít. Tato metoda je nejspolehlivější, neboť samotný klíč není přenášen.

V ZigBee sítích je každá vrstva zodpovědná za bezpečnost rámců inicializovaných v dané vrstvě. Jelikož v každém uzlu sítě se musí nacházet vždy všechny vrstvy, používá se pro jednoduchost stejný bezpečnostní klíč pro všechny vrstvy (APL, NWK, MAC).

7.2 Autentizace

ZigBee podporuje ověřování (autentizaci) zařízení v síti a ověřování dat. Ověřené zařízení je takové zařízení, které je schopné přijmout síťový klíč a nastavit správné atributy v požadovaném čase. V případě ověření dat, se kontroluje, zda data nebyla při přenosu pozměněna.

7.2.1 Autentizace zařízení

Autentizace zařízení se provádí v Trust centrum. Po připojení nového zařízení do zabezpečené sítě dostane tento status "Připojený ale neověřený". V Trust centru se dále rozhodne, zda zařízení bude schváleno a přijato do sítě nebo vyřazeno ze sítě.

V komerčním módu při připojení nového zařízení do sítě si nejprve Trust centrum zjistí, zda nové zařízení zná master klíč. Pokud ano, je klíč poslán. Pokud nové zařízení master klíč nezná, bude mu master klíč poslán přes nechráněnou linku a spustí Key establishment protokol. Toto ověření musí být provedeno do určitého času, pokud zařízení nestihne všechny tyto kroky, nebude ověřeno a vyřazeno ze sítě.

7.2.2 Autentizace dat

Ověření dat slouží k ujištění se, že data nebyla změněna při přenosu. K tomuto účelu se využívá specifický kód Message Integrity Code (MIC), který je přenášen v přenosovém rámci. MIC musí být znám na straně vysílače i přijímače, z čehož vyplývá, že nepovolené zařízení nebude schopno MIC zprávu vytvořit. Úroveň zabezpečení MIC se dá zvýšit bitovým prodloužením tohoto kódu. ZigBee podporuje délky MIC 32-bit, 64-bit a 128-bit.

8 ANALÝZA TRHU

Standard ZigBee je již velmi rozšířený a proto jeho produkty můžeme nalézt u mnoha výrobců. V této práci jsou uvedeny pouze vybraní výrobci, kteří nabízejí nejvhodnější výrobky pro navrhovanou síť.

- Atmel
- Microchip
- Anaren
- Digi International

Vybírat lze ze tří možných nabízených typů zařízení (pouze u některých výrobců):

- Vysílač/přijímač
  Vysílače/přijímače vybíráme podle základních parametrů, jako jsou frekvenční pásmo, ve kterém pracují, výkon vysílače, citlivost přijímače. Dalším parametrem může být typ rozhraní, přes které komunikuje s řídícím obvodem (mikroprocesor).

- Jednočipové řešení
  Jednočipové řešení kombinuje funkci řídícího obvodu a vysílače/přijímače v jednom pouzdře. Toto řešení je nejvhodnější pro aplikace vyžadující minimální rozměry desky plošných spojů.

- ZigBee moduly
  Moduly jsou již hotová zařízení, která obsahují řídící obvod, přijímač/vysílač a ostatní podpůrné součástky, bez kterých by obvod nebyl funkční. Navíc zde bývají i některé obvody jako například teplotní čidla, LED diody pro uživatelsky zvolenou indikaci.

V této práci jsou uvedeny pouze moduly, jež jsou nejvýhodnější, co se týče realizace hardwaru. Někteří výrobci nabízejí velký sortiment modulů, a proto jsou v této práci vybrány pouze ty moduly, které jsou pro řešený problém výhodné.

8.1 Atmel

Atmel nabízí všechny 3 typy zařízení, která jsou založena na vysokofrekvenčních vysílačích a známých procesorech z této rodiny a to 8 bitové nebo 32 bitové AVR a ARM. ARM procesory mají velký výpočetní výkon, který je ale pro naši aplikaci snímání hodnot ze senzorů zbytečný, a proto zde nejsou uvedeny.

Atmel pro lepší vývoj a rychlejší vytváření prototypů nabízí vývojové kity a celou řadu volně dostupných softwarových balíčků zvaných BitCloud, kde se dají nalézt demo programy, knihovny a manuály.

Moduly od společnosti Atmel pracující ve standardu 802.15.4 a jsou vydávány pod označením ZigBit moduly. ZigBit modul je buď proveden v jednočipovém řešení doplněném o podpůrné součástky jako je oscilátor, anténa a další, nebo v řešení přijímač/vysílač doplněném mikroprocesorem jako řídícím obvodem a podpůrnými součástkami, bez kterých by obvod nebyl schopen pracovat správně.

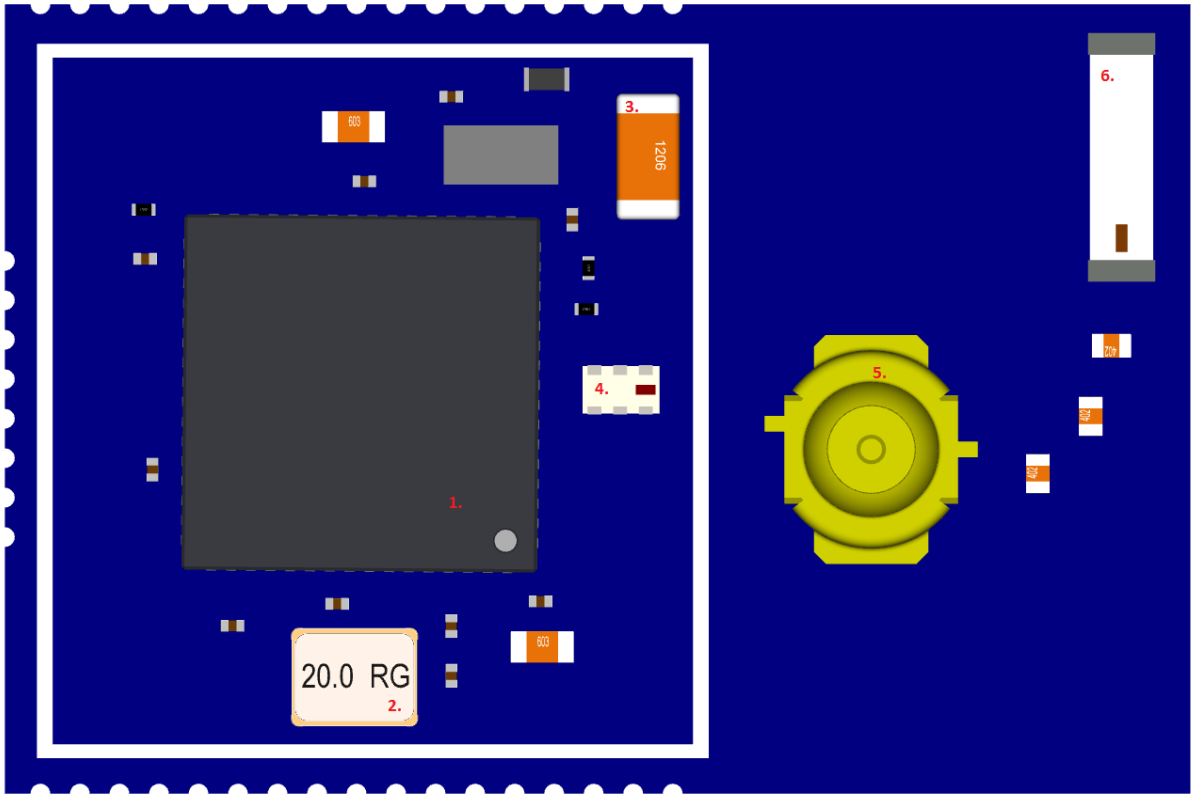
8.1.1 ATmega256RFR2 ZigBit Wireless Module

Jedná se již o modul s mikroprocesorem Atmega256RFR2, který reprezentuje jednočipového řešení, doplněné o podpůrné součástky. Modul pro vnější komunikaci je vybaven rozhraními SPI, I2C a UART. Parametry modulu jsou uvedeny v tabulce 8-1.

Tabulka 8-1: Parametry modulu ZigBit ATmega256RFR2

Parametry	Hodnota	Jednotka
Napájecí napětí:	1,8 až 3,6	V
Frekvenční pásmo:	2,4	GHz
Max. rychlost přenosu dat	2	Mb/s
Výstupní výkon:	3,5	dBm
Citlivost přijímače:	-100	dBm
Proud v režimu přijímač:	12,5	mA
Proud v režimu vysílač:	14,5	mA
Pracovní teplota:	-40 až 125	°C

Na obrázku 8-1 je naznačeno rozložení komponent na desce plošných spojů a její popis.



Obrázek 8-1: Rozložení komponent ATmega256RFR2 ZigBit Wireless Module, převzato z [7]

1. Atmega256RFR2
2. Krystal
3. Balun
4. Analogový přepínač pro výběr antény
5. UFL konektor pro připojení externí antény
6. Integrovaná anténa

V praxi je u modulů řídící obvod obklopen krytem, který chrání před fyzickým poškozením komponent a elektromagnetickým zářením. Mimo tento kryt se nachází pouze antény. Ve finální verzi si můžeme modul prohlédnout na obrázku 8-2.

Obrázek 8-2: Reálný modul ATmega256RFR2 ZigBit Wireless Module, převzato z [7]

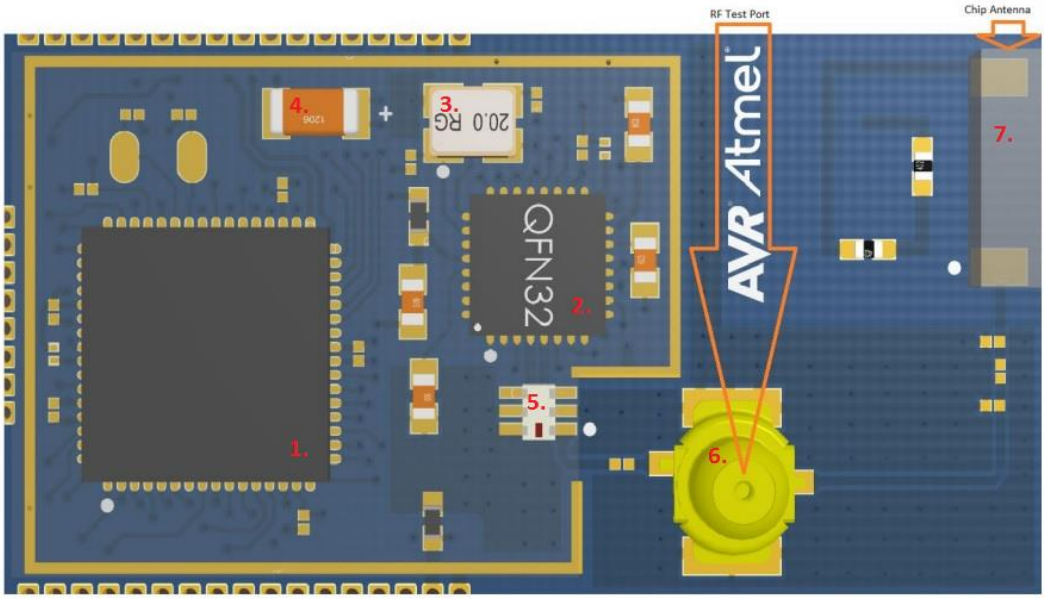
8.1.2 ATxmega256A3U and AT86RF233 ZigBit Wireless Module

Jedná se o druhý typ modulů, kdy je vysílač/přijímač a mikroprocesor umístěn ve svém vlastním pouzdře. Modul kombinuje parametry mikroprocesoru Atmega256A3U a vysílače/přijímače AT86RF233. Parametry jsou uvedeny v tabulce číslo 8-2.

Tabulka 8-2: Parametry modulu ZigBit ATxmega256A3U and AT86RF233

Parametry	Hodnota	Jednotka
Napájecí napětí:	1,8 až 3,6	V
Frekvenční pásmo:	2,4	GHz
Max. rychlost přenosu dat	2	Mb/s
Výstupní výkon:	4	dBm
Citlivost přijímače:	-101	dBm
Proud v režimu přijímač:	6	mA
Proud v režimu vysílač:	13,8	mA
Pracovní teplota:	-40 až 125	°C

Na obrázku 8-3 je naznačen modul s rozložení komponent. Reálný modul je ve skutečnosti na pohled téměř shodný s modulem ATmega256RFR2 ZigBit z obrázku 8-2.



Obrázek 8-3: Rozložení komponent ATxmega256A3U and AT86RF233 ZigBit Wireless Module, převzato z [6]

1. Atmega256A3U
2. AT86RF233
3. Krystal
4. Balun
5. Analogový přepínač pro výběr antény
6. UFL konektor pro připojení externí antény
7. Integrovaná anténa

8.2 Microchip

Firma Microchip nabízí ze všech typů zařízení pouze moduly. Moduly pracují na pracovním kmitočtu 2,4 GHz. Tyto moduly nejsou tvořeny přímo pro standard ZigBee, ale podporují i jiné jako MiWi™, MiWi™ P2P, MiWi™ PRO.

8.2.1 MRF24J40MD

Modul je kompatibilní s PIC mikrokontroléry (PIC16, PIC18, PIC24, PIC32), se kterými komunikuje přes rozhraní SPI. Na desce je integrovaná PCB anténa.

Tabulka 8-3: Parametry modulu MRF24J40MD

Parametry	Hodnota	Jednotka
Napájecí napětí:	1,8 až 3,6	V
Frekvenční pásmo:	2,4	GHz
Max. rychlost přenosu dat	2	Mb/s
Výstupní výkon:	19	dBm
Citlivost přijímače:	-104	dBm
Proud v režimu přijímač:	25	mA
Proud v režimu vysílač:	77	mA
Pracovní teplota:	-40 až 85	°C

Na obrázku 8-4 je zobrazen modul MRF24J40MD.

Obrázek 8-4: ZigBee modul MRF24J40MD, převzato z [8]

Tento výrobce na svých oficiálních stránkách uvádí ještě dva moduly a to MRF24J40MA a MRF24J40ME. Jde o stejné moduly, které se liší pouze ve velikosti výstupního výkonu a vstupní citlivosti. Tyto změny se také samozřejmě projeví v odebíraném proudu, jinak vše zůstává stejné.

8.3 Anaren

Anaren moduly pracují ve standardu ZigBee a jsou označovány A2530E24xx a A2530R24xx. Tyto moduly využívají mikrokontroléry od firmy Texas Instrument CC2530, které představují jednočipové řešení. Moduly jsou vybaveny rozhraním SPI a UART.

Šestý a devátý znak v názvu modulu je důležitý. Šestý znak udává, zda je zařízení FFD (znak E) nebo RFD (znak R). Devátý znak v názvu určuje, zda se jedná o typ s integrovanou anténou (znak A) nebo pouze s U-FL konektorem (znak C).

8.3.1 A2530E24AZ1

V tabulce 8-4 jsou uvedeny parametry modulu A2530E24AZ1.

Tabulka 8-4: Parametry modulu A2530E24AZ1

Parametry	Hodnota	Jednotka
Napájecí napětí:	2,2 až 3,6	V
Frekvenční pásmo:	2,4	GHz
Max. rychlost přenosu dat	2	Mb/s
Výstupní výkon:	1	dBm
Citlivost přijímače:	-95	dBm
Proud v režimu přijímač:	28	mA
Proud v režimu vysílač:	67	mA
Pracovní teplota:	-40 až 85	°C

8.3.2 A2530R24CZ1

V tabulce 8-5 jsou uvedeny parametry modulu A2530R24CZ1.

Tabulka 8-5: Parametry modulu A2530R24CZ1

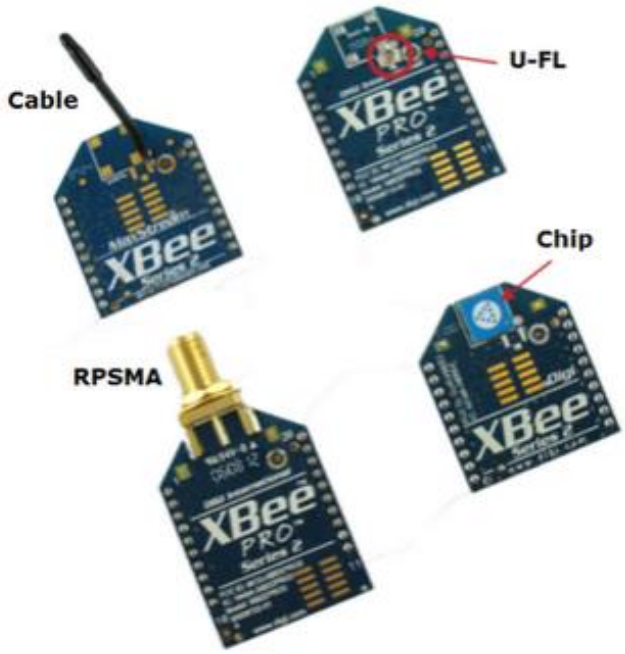
Parametry	Hodnota	Jednotka
Napájecí napětí:	2,2 až 3,6	V
Frekvenční pásmo:	2,4	GHz
Max. rychlost přenosu dat	2	Mb/s
Výstupní výkon:	0	dBm
Citlivost přijímače:	-95	dBm
Proud v režimu přijímač:	28	mA
Proud v režimu vysílač:	68	mA
Pracovní teplota:	-40 až 85	°C

8.4 Digi International

Digi International nabízí ZigBee moduly pod označením XBee. V dnešní době, kdy si už ZigBee prošlo vývojem, nabízí Digi dvě generace. První generace pod označením S1 ještě nebyla schopná využít topologii typu Mesh, proto moduly z této generace nebudou zmiňovány. Každá generace se ještě dělí na standardní zařízení a tzv. PRO zařízení. PRO zařízení se liší pouze vyšším výstupním výkonu a citlivosti přijímače.

Nespornou výhodou modulů od tohoto výrobce je zdarma nabízené vývojové prostředí X-CTU, které umožňuje konfiguraci modulů přes grafické rozhraní nebo pomocí AT-příkazů.

Dále každý modul můžeme dostat ve 4 variantách a to podle druhu osazené antény či konektoru. Obrázek 8-5 zobrazuje všechny možnosti antén a konektorů.



Obrázek 8-5: Druhy antén a konektorů u modulů XBee, převzato z [2]

8.4.1 XBee 2mW Wire Antenna - Series 2

Parametry XBee modulu 2mW Wire Antenna S2 jsou uvedeny v tabulce číslo 8-6a.

Tabulka 8-6: Parametry modulu XBee modulu 2mW Wire Antenna S2

Parametry	Hodnota	Jednotka
Napájecí napětí:	2,1 až 3,6	V
Frekvenční pásmo:	2,4	GHz
Max. rychlost přenosu dat	0,25	Mb/s
Výstupní výkon:	3	dBm
Citlivost přijímače:	-96	dBm
Proud v režimu přijímač:	40	mA
Proud v režimu vysílač:	45	mA
Pracovní teplota:	-40 až 85	°C

8.4.2 XBee PRO 63mW Wire Antenna - Series 2

Parametry XBee modulu 63mW Wire Antenna S2 jsou uvedeny v tabulce číslo 8-7.

Tabulka 8-7: Parametry modulu XBee modulu 2mW Wire Antenna S2

Parametry	Hodnota	Jednotka
Napájecí napětí:	2,1 až 3,6	V
Frekvenční pásmo:	2,4	GHz
Max. rychlost přenosu dat	0,25	Mb/s
Výstupní výkon:	18	dBm
Citlivost přijímače:	-102	dBm
Proud v režimu přijímač:	47	mA
Proud v režimu vysílač:	205	mA
Pracovní teplota:	-40 až 85	°C

8.5 Cenové porovnání uvedených modulů

V tabulce číslo 8-8 je uveden soupis všech uvedených modulů a jejich cena od nabízejících distributorů, jako www.mouser.com, www.sparkfun.com, www.DigiKey.com nebo přímo ze stránek výrobce. Kvůli stále se měnícímu kurzu jsou ceny uvedeny v dolarech.

Tabulka 8-8: Cenové porovnání modulů

ATmega256RFR2 ZigBit Wireless Module	$31.71
ATxmega256A3U and AT86RF233 ZigBit Wireless Module	$28.39
MRF24J40MD	$18.55
A2530E24AZ1	$30.64
A2530R24CZ1	$22.70
XBee 2mW Wire Antenna - Series 2	$22.95
XBee PRO 63mW Wire Antenna - Series 2	$40.95

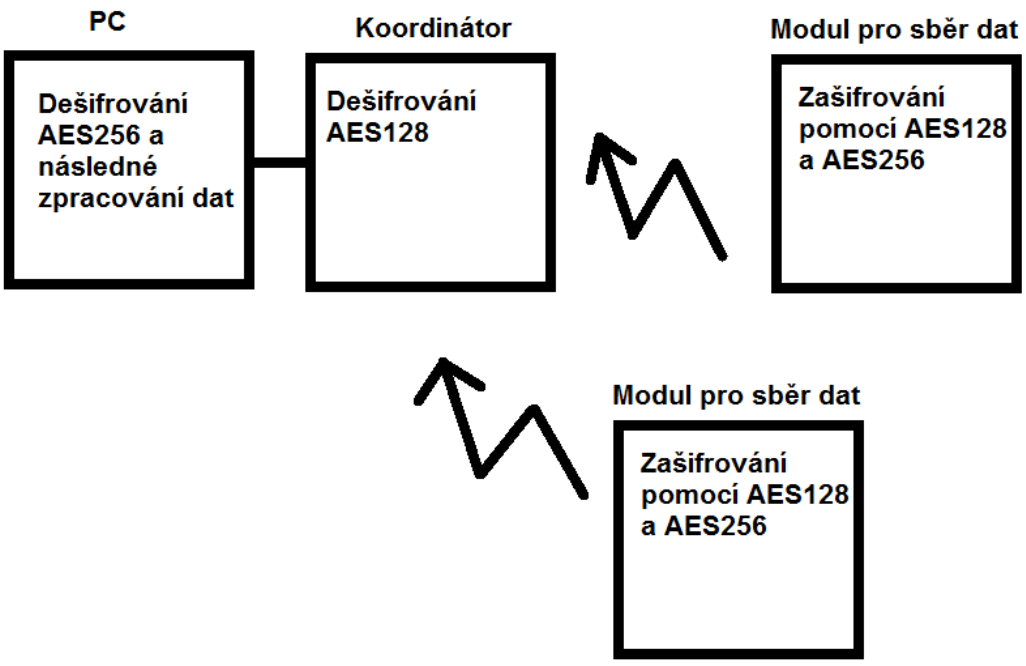
9 PŘENOSOVÝ ŘETĚZEC

Data z jednotlivých čidel jsou pomocí mikroprocesoru zpracována a zakódována a přes Xbee modul odeslána. Dešifrování dat bylo vyzkoušeno dvěma způsoby.

- Dešifrování dat v mikroprocesoru
- Dešifrování dat v PC (Personal Computer)

Dešifrování dat v mikroprocesoru se ukázalo jako nevýhodné a to z důvodu velmi dlouhého procesu dešifrování. Navíc je potřeba dvou UART rozhraní. Jedno pro komunikaci s Xbee a druhé pro komunikaci s PC.

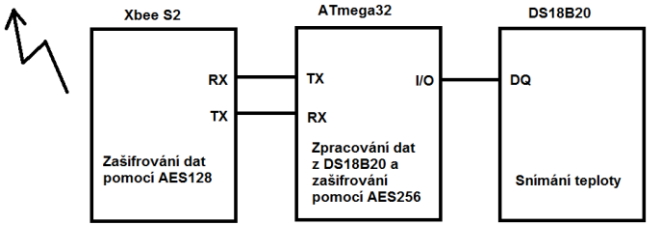
Dešifrování dat v PC se ukázalo jako výhodnější možnost. Xbee koordinátor slouží pouze jako spoj mezi čidly a PC. Dešifrování dat v PC je mnohem rychlejší a máme možnost je rovnou zpracovat do požadovaného formátu. Tento způsob je využit v této práci.



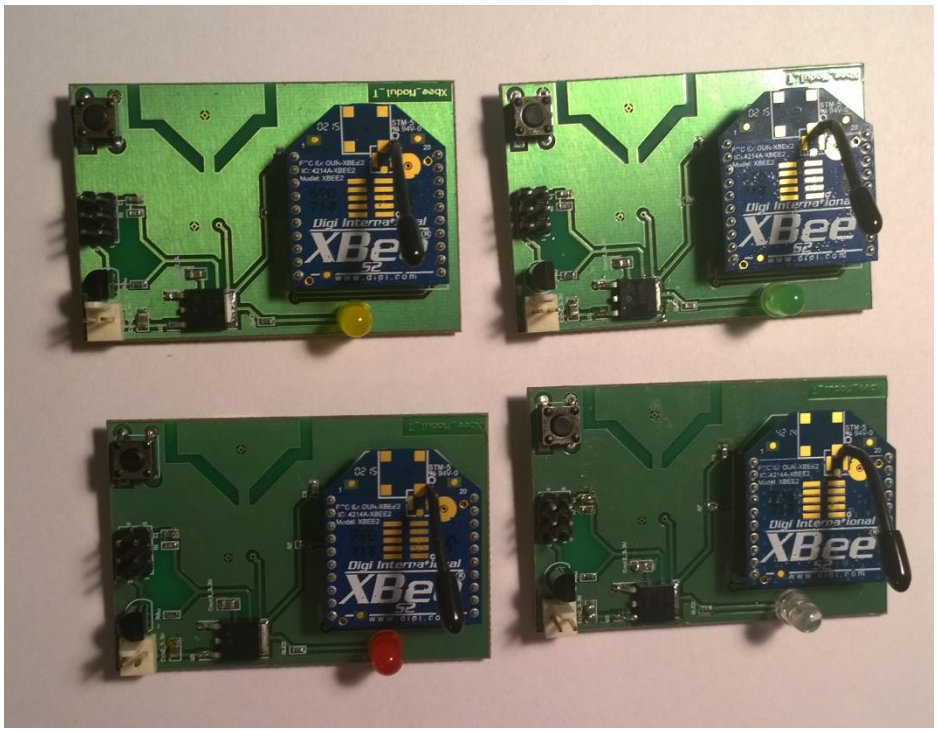
Obrázek 9-1: Blokové schéma přenosového řetězce

10 MODUL PRO SBĚR A PŘENOS DAT

V našem případě bude snímanou veličinou teplota. Ta bude snímána pomocí teplotního senzoru DS18B20. Data z teplotního senzoru budou dále zpracovávána v mikroprocesoru typu ATmega 32, kde budou pomocí šifry AES256 zakódována a přes UART předána zvolenému ZigBee modulu, kde jsou znovu zakódována pomocí AES128 a odeslána k centrálnímu bodu. Každý modul má pro lepší identifikaci odlišnou barvu signalizační LED diodu.



Obrázek 10-1: Blokové schéma modulu pro sběr a následné zpracování dat



Obrázek 10-2: Moduly pro sběr dat

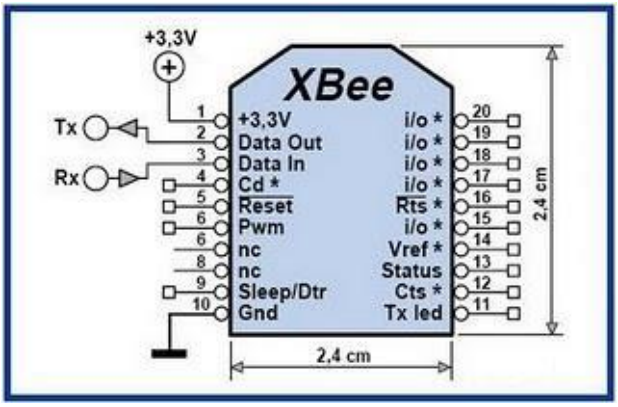
10.1 Teplotní senzor DS18B20

Digitální teploměr DS18B20 poskytuje 9 a 12 - bitové rozlišení měření teploty. Rozsah měřené teploty se pohybuje od -55°C do +125°C. DS18B20 komunikuje s mikroprocesorem po sběrnice 1-Wire, tím odpadá nutnost velkého množství vodičů. DS18B20 je také vybaveno funkcí alarm, tzn., že pokud není nutné stroje neustále monitorovat a shromažďovat data, můžeme pouze nastavit hraniční teplotu, při jejímž překročení je aktivován alarm a hodnota je odeslána. V této práci je použito 12 - bitové rozlišení a jelikož jde o sběr dat, aktuální teplotu budeme vyčítat v pravidelných intervalech.

10.2 Zigbee modul Xbee S2

10.2.1 Bližší popis modulu

Obecné parametry modulu Xbee S2 jsou popsány v kapitole 8.4.1. Hlavními důvody pro zvolení těchto modulů jsou jejich snadná dostupnost, nízká cena a snadná konfigurace. Modul je vybaven integrovaným mikroprocesorem, který zprostředkovává přenos dat a ovládání pinů. Paměť modulu je dostatečná pro konfiguraci, avšak implementace dalšího vlastního algoritmu není možná. Modul je vybaven 20 piny, z nichž některé se dají využít například jako generátor PWM, A/D převodník nebo jako vstupně/výstupní porty. Pro konfiguraci modulu nebo ke komunikaci například s mikroprocesorem slouží rozhraní UART. Navíc je obvod vybaven piny CTS (Clear To Send) a RTS (Request To Send). Pokud je CTS v nízké úrovni, znamená to pro hosta, že může vysílat. Pin RTS je použit, pokud je buffer mikroprocesoru plný a ten není schopen data přijmout. Pak se nastaví na tento pin vysoká úroveň a Xbee data podrží ve svém bufferu. Zbytek jsou standardní piny jako napájení, zem nebo reset modulu. Na obrázku 9-1 je znázorněna funkce jednotlivých pinů.



Obrázek 10-3: Pinout modulu Xbee, převzato z [14]

10.2.2Připojení modulu k PC

Pro připojení modulů k PC a jejich konfiguraci bylo použito zařízení Xbee Explorer USB. Toto zařízení dokáže komunikovat se všemi typy Xbee modulů. Hlavní částí je FT231X, což je převodník mezi USB-UART. V této práci bylo použito toto zařízení ke konfiguraci všech Xbee modulů.

Obrázek 10-4: Xbee Explorer USB, převzato z [13]

10.2.3Konfigurace modulů

Pro správnou funkčnost modulů je potřeba je prvně nakonfigurovat. K tomuto účelu byl použit software X-CTU přímo od společnosti Digi International, který je volně dostupný.

Po spuštění programu se přes příslušný COM port připojíme k Xbee modulu. Jako první krok je potřeba vybrat vhodný firmware. Firmwarem se rozumí, jakou funkci bude zařízení v síti zastávat (koordinátor, router, koncové zařízení) a v jaké módu bude pracovat.

Xbee podporuje dva typy módu:

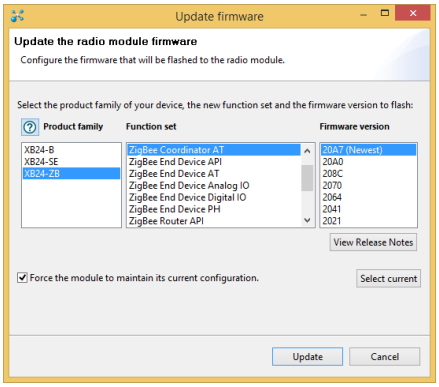
- API (Application Programming Interface) mód
- AT (Transparent) mód

API mód je velkou výhodou modulů XBee. API mód umožňuje jednomu centrálnímu počítači či mikroprocesoru dotazovat se na služby poskytující XBee moduly bez mikroprocesoru. Jak bylo řečeno v kapitole 10.2.1, Xbee moduly jsou vybaveny i speciálními piny. Takže pokud je potřeba například zjišťovat stav log. 1 (sepnuto) nebo log. 0 (rozepnuto) na určitém pinu, zažádáme o to vzdálené XBee z centrálního bodu a to nás informuje o stavu. Tak nám tedy odpadá nutnost použití dalšího mikroprocesoru na příslušném senzoru. V našem případě, kdy je požadováno přídavné šifrování AES256, je mikroprocesor pro zašifrování dat nepostradatelný. Proto API módu nebude využívat.

V AT módu nakonfigurujeme zařízení na trvalé nastavení a již není možné například na vstupně/výstupním pinu měnit hodnotu. Tento mód je vhodnější, pokud využíváme pouze vysílač a přijímač modulu a kontrolní piny.

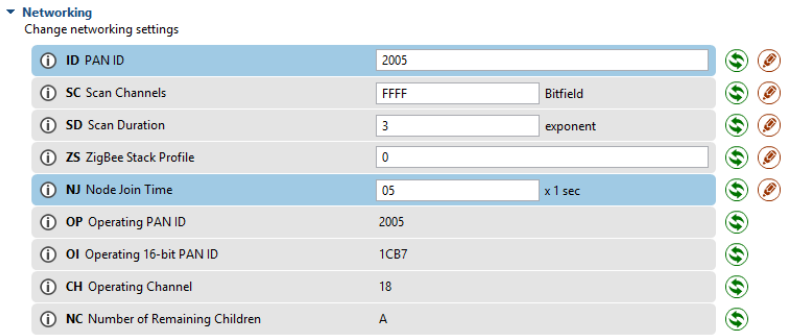
Konfiguraci je možné provádět přes grafické rozhraní nebo AT příkazy. V katalogovém listu je možné všechny AT příkazy nalézt. Pohodlnější a přehlednější je použít grafické prostřední programu X-CTU. Celý postup konfigurace modulu si ukážeme na koordinátorovi, jehož konfigurace je přímo v práci použita. Konfigurace na routeru je velice podobná, pouze s méně parametry. Zabývat se budeme pouze parametry důležitými pro naši práci. Vynechané parametry jsou většinou automaticky správně nastavené a nemá smysl je měnit.

Prvním krokem je vybrat firmware (obrázek 9-3). Product family vyčteme přímo na zadní straně modulu. Dále volíme roli zařízení v síti a mód, ve kterém bude pracovat. Zpravidla se volí nejnovější verze firmwaru. Firmware zapíšeme do zařízení tlačítkem update.



Obrázek 10-5: Volba firmwaru pro Xbee modul

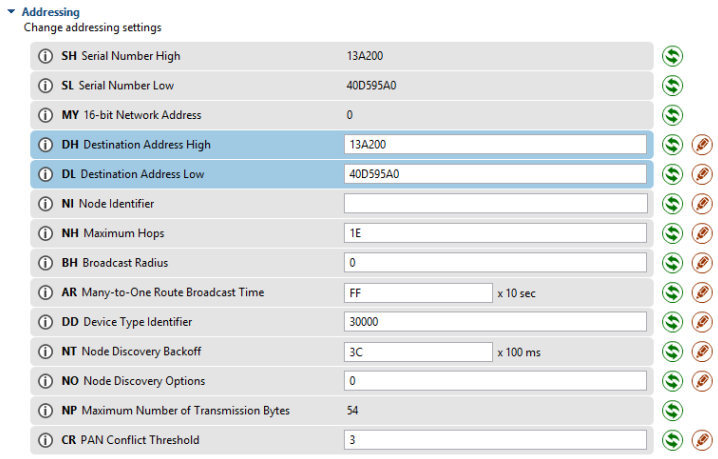
V části Networking se nastavuje PAN ID, SC (Scan Channels) pro skenování energetického zatížení jednotlivých kanálů. Třetím parametrem je nastavení exponentu do rovnice, kde je určeno, jak dlouho má SC trvat. Parametr Node Join Time slouží pro nastavení času, po který mají přihlašující se nody do sítě vygenerovat síťový klíč a odpovědět na požadavek.



Obrázek 10-6: Nastavení Networking části

Další částí, kterou nastavujeme je Addressing (adresování). První nastavitelný parametr je DH a DL, což je 8 horních a 8 spodních bytů adresy cílového zařízení. Protože koordinátor slouží pouze pro přijímání dat, můžeme mu nastavit jako cílovou adresu samé jedničky a pokud bude potřeba, aby vysílal, pošle zprávu typu broadcast.

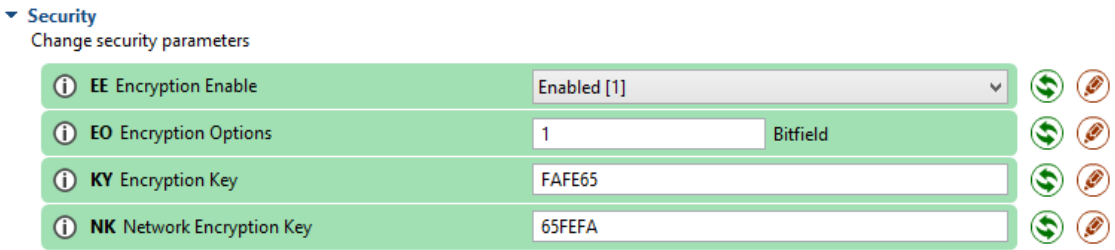
Parametr Node Identifier slouží pro vložení názvu zařízení, pro snazší identifikaci v síti. Maximum Hops slouží pro nastavení maximálního počtu skoků v síti. Parametr Node Discovery Backoff určuje dobu, po kterou musí připojující se zařízení odeslat do sítě svou síťovou identifikaci.



Obrázek 10-7: Nastavení Addressing části

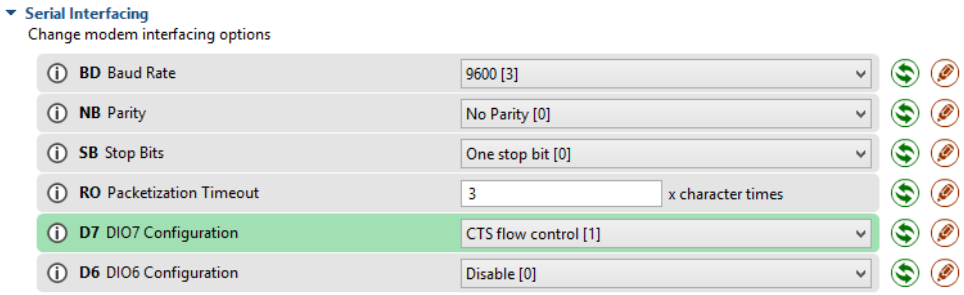
V části nastavení vysílače jsou nastaveny nejvyšší možné hodnoty. Vysílací výkon je 2 dBm.

V části Security (zabezpečení) se nastavuje šifrování AES128 a jeho parametry. Nejprve ho musíme aktivovat parametrem EE (Encryption Enable). Parametrem EO (Encryption Option) volíme mezi: 0 – předání nezabezpečeného síťového klíče při připojování a 1 – je využito Trust centrum. V našem případě je využito centrum důvěry. KY (Enryption Key) a NK (Network Enryption Key) jsou 128 - bitové klíče. KY slouží přímo šifrování dat, zatímco NK pro přístup do sítě. Po zapsání parametrů již není možné KY a NK vyčíst.



Obrázek 10-8: Nastavení Security části

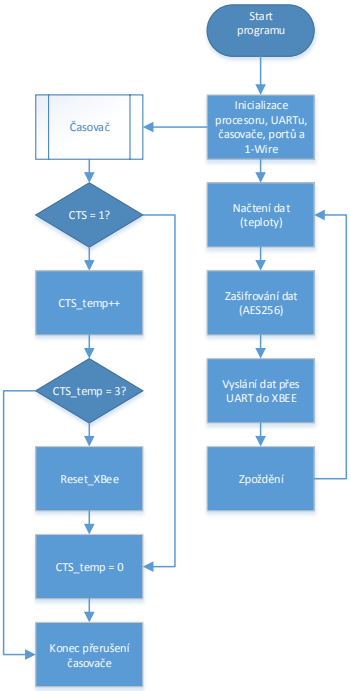
Další částí je nastavení sériové linky pro komunikaci s mikroprocesorem. Nakonfigurované parametry se musí shodovat s parametry nakonfigurovanými na mikroprocesoru. Dále je nastaven parametr na pinu D7. Parametrem je CTS flow control. Přes tento pin tedy budeme zjišťovat, zda je buffer Xbee modulu volný a zda jsme tedy schopni vysílat.



Obrázek 10-9: Nastavení sériové komunikace

10.3 Algoritmus programu v mikroprocesoru

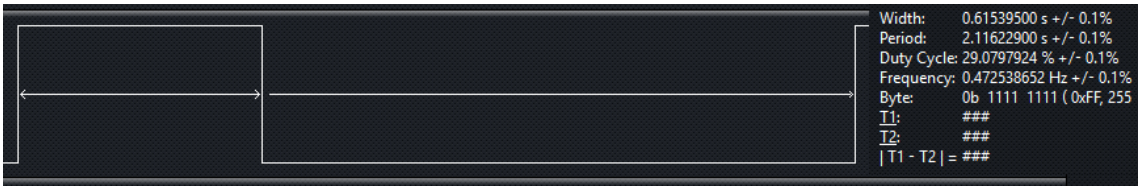
Mikroprocesor slouží k načtení dat z teplotního čidla a následné zpracování dat do odeslaného rámce. K tomuto rámci jsou přidána data jako ID zařízení a typ přenášených dat. Poté je celý rámec zašifrován pomocí AES256 a data jsou dále předávána přes UART do Xbee modulu. Mikroprocesor se také stará pomocí časovače o stav bufferu Xbee modulu a o případný reset. Proti zacyklení programu v mikroprocesoru je využit watchdog. Celý program je napsán v jazyce C.



Obrázek 10-10: Vývojový diagram Algoritmu programu v mikroprocesoru

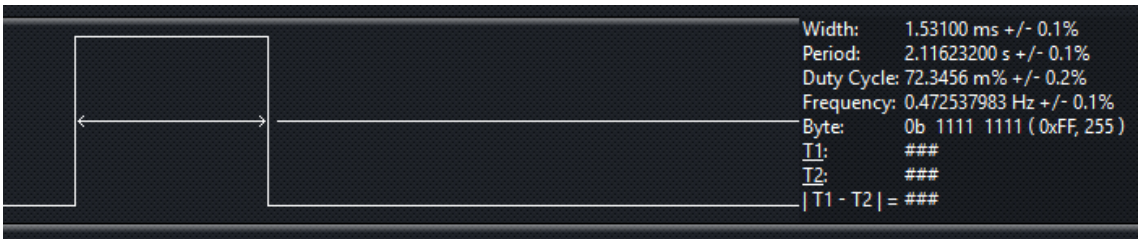
Změřený čas jednoho cyklu programu je 615 ms. Jeden cyklus obsahuje vyčištění bufferu, načtení teploty, sestavení rámce, zašifrování rámce a následné odeslání.

Čas byl měřen při taktu mikroprocesoru 16 MHz. Logická jednička na obrázku 10-11 je naměřený čas jednoho cyklu.



Obrázek 10-11: Doba trvání jednoho cyklu programu

Téměř 90% času trvá vyčtení a zpracování dat z teplotního čidla. Samotné zašifrování dat trvá kolem 1,5 ms.



Obrázek 10-12: Doba trvání zašifrování dat pomocí AES256

11 PŘIJÍMACÍ STRANA PŘENOSOVÉHO ŘETĚZCE

Přijímací strana přenosového řetězce je tvořena koordinátorem a počítačem. Přijímací strana má za úkol přijmout data a dešifrovat. Dešifrování dat AES128 je prováděno v Xbee modulu a následně předáno přes UART do PC. V PC jsou data dešifrována AES256 a vytisknuta do konzole.

11.1 Koordinátor

Koordinátor je tvořen modulem Xbee a Xbee Explorer USB vývojovou deskou.

Obrázek 11-1: Koordinátor složen z Xbee modulu a Xbee Explorer USB, převzato z [13]

Jelikož síť má sloužit pro ověření principů standardu ZigBee, je toto řešení koordinátora dostačující. Při realizaci sítě by se místo tohoto řešení využilo jedné z nabízených Xbee gateway. Ty jsou vybaveny lepšími parametry u přijímače a vysílače, vyšší rychlost zpracování a předání dat. Navíc je Xbee gateway vybaven i dalšími standardy jako Wi-Fi nebo Ethernet. Tím jsou data snadněji předávána a zpracovávána. Na obrázku 11-2 je ukázka gateway Xbee

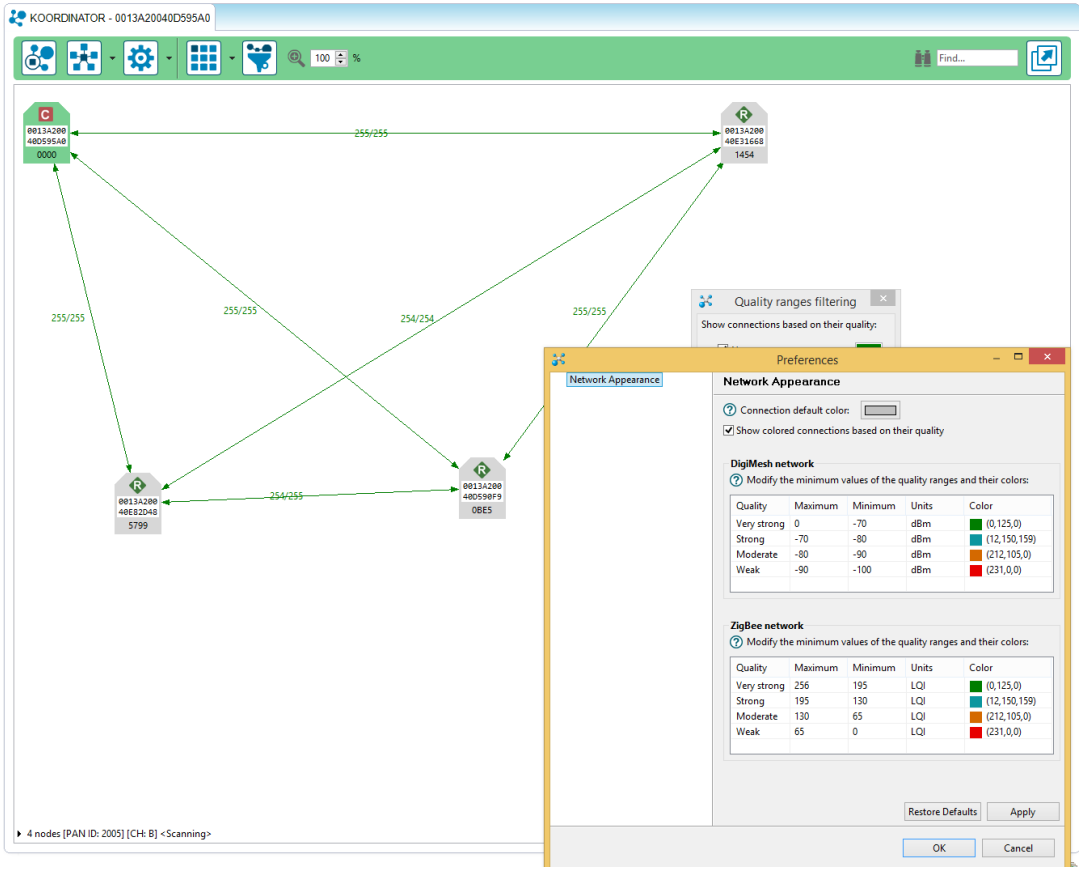
Obrázek 11-2: Gateway Xbee, převzato z [13]

11.2 Algoritmus programu v PC

Hlavní funkcí algoritmu v PC je dešifrovat data. Data jsou nejprve dešifrována AES 256. Dešifrovaná data jsou poté rozparsována podle předem navrženého protokolu na ID zařízeni, typ paketu a data. Poté jsou data převedena na řetězec a ten je vytisknut do konzole.

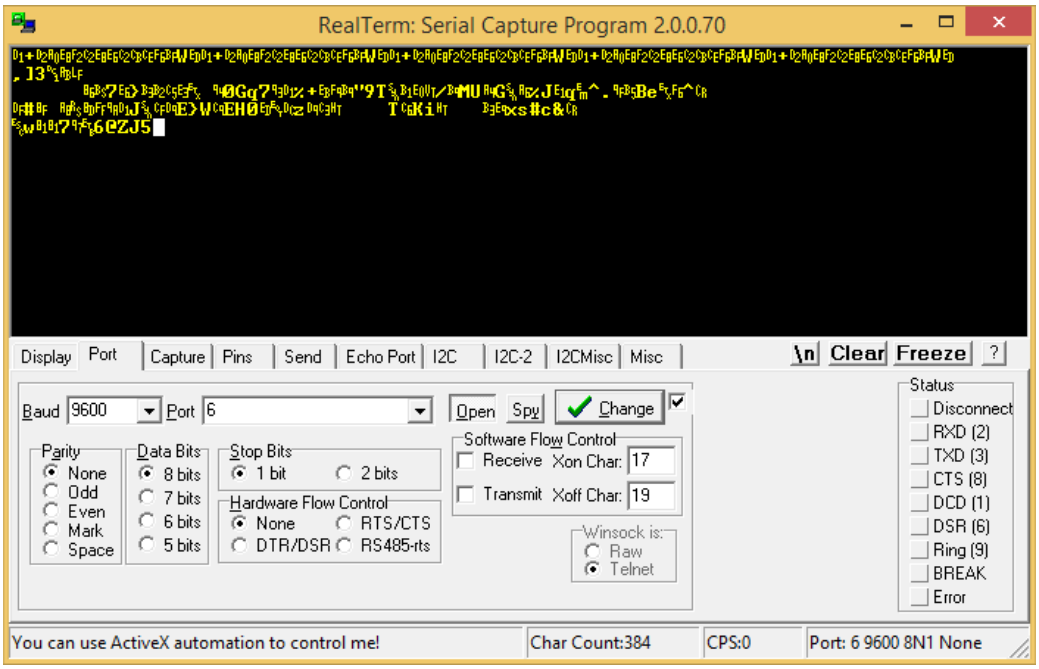
12 VÝSLEDNÁ FUNKCE SÍTĚ

Logická topologie sítě je na obrázku 12-1. Celá síť je navzájem propojená, což odpovídá topologii typu Mesh. Z obrázku je také patrná síla signálu jednotlivých spojů. Moduly od sebe byly vzdáleny zhruba 10 metrů.



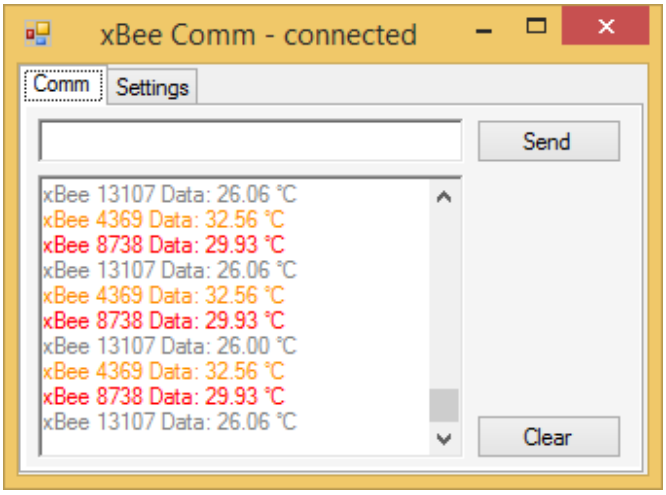
Obrázek 12-1: Logická topologie vytvořené sítě a síla jednotlivých linek

Výsledný výpis dat z čidel je na obrázku 12-2. Data jsou zobrazena v běžném terminálu, takže je vidíme zašifrována.



Obrázek 12-2: Výpis zašifrovaných dat v terminálu

Pokud data zobrazíme v našem terminálu, který data z AES 256 dešifruje, dostaneme výpis z obrázku 12-3: Výpisy jsou pro snadnou identifikaci barevně odděleny a to podle barev LED diod na jednotlivých modulech. Data je možné uložit do textového souboru.



Obrázek 12-3: Výpis dešifrovaných dat

ZÁVĚR

V první části bakalářské práce bylo uvedeno několik standardů pro bezdrátovou komunikaci. Na základě jejich parametrů bylo potřeba provést srovnání s parametry zadanými a zvolit nejvhodnější standard. Zvolené parametry nejlépe splňoval standard ZigBee, který podporuje topologii typu Mesh, umožňuje implementaci šifrování AES128 a který by měl být odolný proti průmyslovému rušení.

Dále bylo potřeba se s ZigBee standardem důkladně seznámit, jelikož se nejedná o příliš známý standard. V teoretické části byl velice důkladně popsán celý standard ZigBee, byl uveden referenční model, typy zařízení, která můžeme v síti najít, všechny topologie, které tento standard podporuje a také zde bylo probráno adresování a zabezpečení.

V další části práce byla uvedena analýza trhu. Jelikož moduly jsou distribuovány velkou řadou výrobců, bylo potřeba prozkoumat různé výrobky. V této části práce byly uvedeny jednotlivé ZigBee moduly a jejich základní parametry. V závěru 8. kapitoly pak byly jednotlivé moduly porovnány i cenově. Na základě všech zjištěných parametrů byly zvoleny moduly Xbee S2. Hlavními důvody pro tuto volbu byly nejpřívětivější konfigurace modulů, poměr cena/výkon, velké množství informací o modulech, například v podobě datasheetu.

V poslední části práce pak byla popsána praktická realizace sítě. Síť je složena z přijímací a vysílací strany. Vysílací strana je složena z 3 hlavních částí: Xbee modulu, mikroprocesoru a teplotního senzoru DS18B20. DS18B20 slouží ke snímání teploty. Mikroprocesor se může jevit jako nadbytečný, jelikož Xbee modul dokáže na svých pinech vyčítat hodnoty. Protože bylo potřeba posílit šifrování dat, jelikož šifrování v Xbee modulech AES128 je již nedostačující, bylo potřeba vyřešit implementaci šifrování AES256 do 8 – bitového mikroprocesoru. Po zašifrování dat v mikroprocesoru jsou data přes UART předána Xbee modulu, který je ještě zašifruje AES128 a poté jsou bezpečně odeslána ke koordinátorovi. Na přijímací straně jsou data z AES128 dešifrována koordinátorem a přes UART přeposlána do PC. Z AES 256 jsou dešifrována až v PC. Nejprve bylo zkoušeno dešifrovat data dešifrovat v mikroprocesoru na přijímací straně a až poté byla data předávána do PC. Tato metoda se ukázala jako méně výhodná, jelikož dešifrování dat trvá 1,5 ms, což by při větším množství čidel byl příliš vysoký čas. Navíc v případě dešifrování dat v PC jsou data chráněna i při přenosu z koordinátora do PC. Za tímto účelem byla napsána konzolová aplikace v jazyce C#.

Zadání práce bylo zcela splněno. Síť je plně funkční pro sběr dat a bezpečný přenos. Do budoucna by bylo vhodné konzolovou aplikaci rozšířit na přehlednější zpracování dat, například zobrazení dat v grafu. Při realizace sítě by bylo také vhodné použít vyšší řadu Xbee modulů Pro, které mají lepší parametry. Další možností sítě by mohlo být zavedení zpětné vazby na jednotlivé podněty, která by sloužila například pro regulaci teploty.

LITERATURA

[1] ZigBee - novinka na poli bezdrátové komunikace. *Hardware.cz* [online]. 2005 [cit. 2015-12-12]. Dostupné z: http://vyvoj.hw.cz/navrh-obvodu/rozhrani/zigbee-novinka-na-poli-bezdratove-komunikace.html

[2] XBee/XBee-PRO moduly Digi. *Hardware.cz* [online]. 2009 [cit. 2015-12-12]. Dostupné z: http://www.hw.cz/embedded/xbeexbee-pro-moduly-digi.html

[3] ZigBee PRO - nová vylepšená verze bezdrátové komunikace ZigBee. *Www.hw.cz* [online]. 2008 [cit. 2015-12-12]. Dostupné z: http://automatizace.hw.cz/zigbee-pro-nova-vylepsena-verze-bezdratove-komunikace-zigbee.

[4] *ZigBee Security* [online]. 2009 [cit. 2015-12-12]. Dostupné z: https://docs.zigbee.org/zigbee-docs/dcn/09-5378.pdf.

[5] *XBee ZigBee Route Discovery and Network Address Discovery* [online]. [cit. 2015-12-12]. Dostupné z: http://knowledge.digi.com/articles/Knowledge_Base_Article/XBee-ZigBee-Route-Discovery-and-Network-Address-Discovery.

[6] ATZB-X0-256-3-0-C: DATASHEET. *Http://www.atmel.com/* [online]. [cit. 2015-12-12]. Dostupné z: http://www.atmel.com/Images/Atmel-42172-Wireless-ZigBit-ATZB-X0-256-3-0-C_Datasheet.pdf

[7] ATZB-S1-256-3-0-C: DATASHEET. *Http://www.atmel.com/* [online]. [cit. 2015-12-12]. Dostupné z: http://www.atmel.com/Images/Atmel-42191-Wireless-ZigBit-ATZB-S1-256-3-0-C_Datasheet.pdf

[8] MRF24J40MD/ME: DATASHEET. *Http://www.microchip.com/* [online]. [cit. 2015-12-12]. Dostupné z: http://ww1.microchip.com/downloads/en/DeviceDoc/70005173A.pdf

[9] Xbee types antennas: Moduls. *Http://www.microchip.com/* [online]. [cit. 2015-12-12]. Dostupné z: http://www.digi.com/products/xbee-rf-solutions

[10] BERAN, L. Bezdrátové sítě ZigBee: bakalářská práce. Pardubice: Univerzita Pardubice, Fakulta elektrotechniky a informatiky, 2011. 65s. Vedoucí bakalářské práce Ing. Martin Hájek

[11] FARAHANI, Shahin. *ZigBee wireless networks and transceivers*. Boston: Newnes/Elsevier, 2008, xxiv, 339 p. ISBN 0750683937.

[12] FALUDI, Robert. *Building wireless sensor networks*. 1st ed. Sebastopol: O'Reilly, 2010, xviii, 300 s. ISBN 978-0-596-80773-3.

[13] Sparkfun. *Sparkfun.com* [online]. [cit. 2016-05-18]. Dostupné z: https://www.sparkfun.com/

[14] Pyroelectro. *Www.pyroelectro.com* [online]. [cit. 2016-05-18]. Dostupné z: http://www.pyroelectro.com/tutorials/xbee_pan_tilt_servo/xbee_theory.html

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

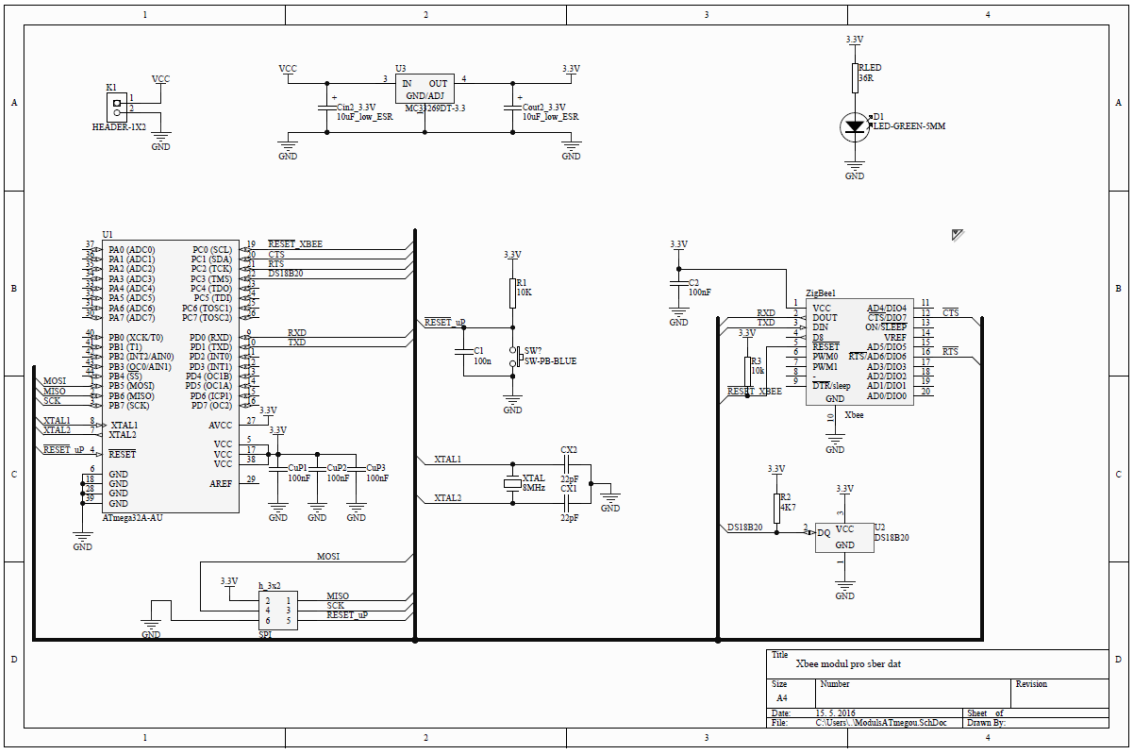
C	Cena linky.
H	Hertz
Pl	Pravděpodobnost úspěšného doručení zprávy.
ms	Milisekunda
°C	Stupeň Celsia

AES	Advanced Encryption Standard
API	Application Programming Interface
APS	Application support
CAP	Contention Access Period
CCA	Clear Channel Assessment
CFP	Contention-Free Period
CS	Carrier Sense
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance, Přístupová metoda CSMA-CA
CRC	Cyclic Redundancy Check, Cyklický redundantní kód
CTS	Clear To Send
IEEE	Institute of Electrical and Electronics Engineers, Institut pro elektrotechnické a elektronické inženýrství
ED	Energy Detection, Detekce hladiny signálu
EE	Encryption Enable
EO	Encryption Option
FFD	Full-Function Device, Plně funkční zařízení
GTS	Guaranteed Time Slot, Garantovaný časový slot
ISM	Industrial, Scientific, and Medical, Průmyslové, vědecké a zdravotnické pásmo
KY	Enryption Key
KZ	Koncové Zařízení
LQI	Link Quality Indicator, Indikátor kvality linky
MAC	Medium Access Control, Vrstva přístupu k médiu
MFR	MAC Footer

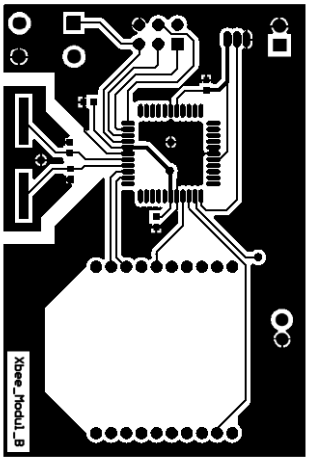
MHR	MAC Header
MIC	Message Integrity Code
NK	Network Enryption Key
NWK	Network Layer, Síťová vrstva
PAN	Personal Area Network, Osobní lokální síť
PC	Personal Computer, Osobní počítač
PHY	Physical Layer, Fyzická vrstva
R	Router
RFD	Reduced Function Device, Zařízení se sníženou funkčností
RSS	Received Signal Strength, Úroveň přijatého signálu
RTS	Request To Send
SC	Scan Channels
SPI	Serial Peripheral Interface, Sériové periferní rozhraní
SNR	Signal-to-Noise Ratio, Poměr signál-šum
I2C	Inter-Integrated Circuit, Počítačová sériová sběrnice
UART	Universal Asynchronous Receiver and Transmitter, Univerzální sériové vysílání a přijímání
WPAN	Wireless Personal Area Network, Bezdrátová osobní lokální síť
ZigBee	Bezdrátový standard typu IEEE802.15.4
ZDO	ZigBee Device Object, ZigBee zařízení

A NÁVRH ZAŘÍZENÍ

A.1 Obvodové zapojení Modulu pro sběr a přenos dat

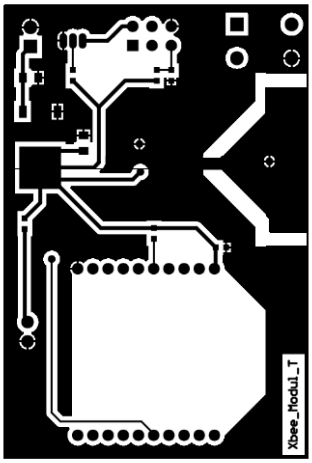


A.2 Deska plošného spoje Modulu pro sběr dat – bottom



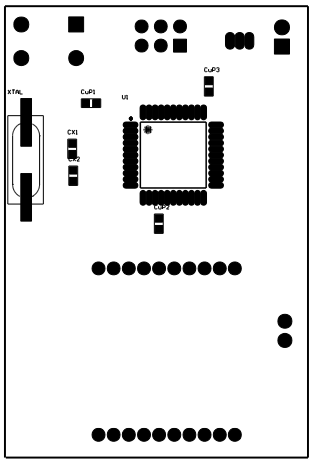
Rozměr desky 40 x 60 [mm], měřítko M1:1

A.3 Deska plošného spoje Modulu pro sběr dat – top



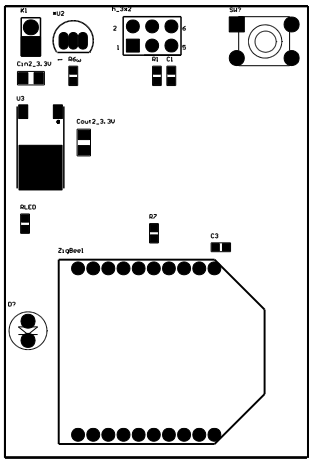
Rozměr desky 40 x 60 [mm], měřítko M1:1

A.4 Osazovací plán Modulu pro sběr dat – bottom



Rozměr desky 40 x 60 [mm], měřítko M1:1

A.5 Osazovací plán Modulu pro sběr dat – top



Rozměr desky 40 x 60 [mm], měřítko M1:1

B SEZNAM SOUČÁSTEK PRO DESKU PLOŠNÝCH SPOJŮ MODULU PRO SBĚR DAT

Comment	Description	Designator	Quantity
100nF	CAPACITOR 0603 CERAMIC	C1,C2, CuP1, CuP2, CuP	5
10uF_low_ESR	CAPACITOR 0805 CERAMIC	Cin2_3.3V, Cout2_3.3V	2
22pF	CAPACITOR 0603 CERAMIC	CX1, CX2	2
LED-GREEN-5MM	LED-GREEN-5MM	D1	1
SPI	Header, 3-Pin, Dual row	h_3x2	1
HEADER-1X2		K1	1
10K	GENERIC RESISTOR 0603	R1	1
4K7	GENERIC RESISTOR 0603	R2	1
10k	GENERIC RESISTOR 0603	R3	1
36R	GENERIC RESISTOR 0603	RLED	1
SW-PB-BLUE	SW-D6-R / SW-DS-S / SW-14X14 / SW-7X7	SW?	1
ATmega32A-AU	8-bit AVR Microcontroller, 32KB Flash, 1KB EEPROM, 2KB SRAM, 44-pin TQFP, Industrial Grade (-40°C to 85°C)	U1	1
DS18B20		U2	1
MC33269DT-3.3	Low Dropout Positive Fixed Voltage Regulator	U3	1
8MHz	8MHZ CRSYTAL HC49US	XTAL	1
Xbee	Xbee_S2_model	ZigBee1	1