VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

ENERGETICKÁ NÁROČNOST IPV6 V BEZDRÁTOVÝCH SENZOROVÝCH SÍTÍCH

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

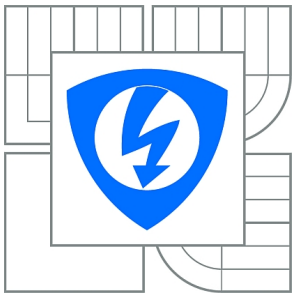
AUTOR PRÁCE
AUTHOR

ROMAN KLADIVA

BRNO 2011

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

ENERGETICKÁ NÁROČNOST IPV6 V BEZDRÁTOVÝCH SENZOROVÝCH SÍTÍCH

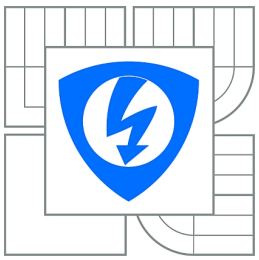
IPV6 AND POWER EFFICIENCY IN WIRELESS SENSOR NETWORKS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — ROMAN KLADIVA
AUTHOR

VEDOUCÍ PRÁCE — Ing. VLADIMÍR ČERVENKA
SUPERVISOR

BRNO 2011



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Roman Kladiva	***ID:***	119477
Ročník:	3	***Akademický rok:***	2010/2011

NÁZEV TÉMATU:

Energetická náročnost IPv6 v bezdrátových senzorových sítích

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je zhodnotit energetickou náročnost protokolů vrstev 6LowPAN. Poukázat na možné způsoby snížení spotřeby pro jednotlivé implementace a provést návrh přípravku na měření spotřeby dané platformy.

DOPORUČENÁ LITERATURA:

[1] DUNKELS, Adam; VASSEUR, Jean-Philippe. Interconnecting Smart Objects with IP : The Next Internet . California : Morgan Kaufmann, 2010. 432 s. ISBN 0123751659.

[2] SHELBY , Zach; BORMANN, Carsten. 6LoWPAN : The Wireless Embedded Internet . [s.l.] : Wiley, 2010. 244 s. ISBN 0470747994.

Termín zadání:	7.2.2011	***Termín odevzdání:***	2.6.2011

Vedoucí práce: Ing. Vladimír Červenka

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

ABSTRAKT

Tato bakalářská práce se zabývá bezdrátovými senzorovými sítěmi z pohledu energetické náročnosti IPv6. Obsahuje popis bezdrátových senzorových sítí, rozbor senzorového uzlu a protokolů 6LoWPAN a IPv6. Další část se zaměřuje na adaptační vrstvu 6LoWPAN a nástroje, které používá k minimalizaci přenosové jednotky a tedy i ke snížení energetické náročnosti. V práci je popsána problematika spotřeby energie v bezdrátových senzorových sítích a její možné řešení na úrovni fyzické a linkové vrstvy. Jsou zde podrobně rozebrány možnosti režimu spánku a jednotlivé protokoly MAC vrstvy. Následuje charakteristika měření spotřeby senzorového uzlu a vlastní návrh na zlepšení měřící metody.

KLÍČOVÁ SLOVA

bezdrátové senzorové sítě, WSN, senzor, 6LoWPAN, IPv6, spotřeba energie, MAC protokoly, měření spotřeby

ABSTRACT

This bachelor's thesis deals with wireless sensor networks in terms of energy performance of IPv6. It contains a description of wireless sensor networks, sensor node analysis and 6LoWPAN and IPv6 protocols. The another part of the thesis is focused on adaptation layer 6LoWPAN and tools, which used to minimize the transmission unit, and thus to reduce energy consumption. Problems of energy consumption in wireless sensor networks is discribed in the thesis and its possible solutions at the physical and link layers. There are analyzed in detail possibilities of sleep mode and various MAC layer protocols are analyzed in detail. The measuremenr overview of the sensor node and own proposal to improve the measurement method are discribed following in the thesis.

KEYWORDS

wireless sensor networks, WSN, sensor, 6LoWPAN, IPv6, energy consumption, MAC protocols, metering energy consumption

KLADIVA, Roman *Energetická náročnost IPv6 v bezdrátových senzorových sítích*: bakalářská práce. BRNO: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2011. 71 s. Vedoucí práce byl Ing. Vladimír Červenka

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Energetická náročnost IPv6 v bezdrátových senzorových sítích“ 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 jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

BRNO ....

(podpis autora)

Poděkování

Děkuji vedoucímu bakalářské práce Ing. Vladimíru Červenkovi za užitečnou metodickou, odbornou pomoc a další cenné rady při zpracování mé bakalářské práce. Také bych chtěl poděkovat své rodině za podporu při studiu.

V Brně dne ....

podpis autora

OBSAH

Úvod **11**

1 Bezdrátové senzorové sítě **12**
1.1 Úvod do bezdrátových senzorových sítí 12
1.2 Standard IEEE 802.15.4 13
1.2.1 Fyzická vrstva 15
1.2.2 Linková vrstva 17
1.2.3 Vyšší vrstvy 18
1.2.4 Senzorový uzel 18

2 Protokol 6LoWPAN **20**
2.1 Vrstvy 6LoWPANu 22
2.2 IPv6 23
2.3 Adaptační vrstva 6LoWPAN 25
2.3.1 Zapouzdření formátu hlavičky 26
2.3.2 Fragmentace záhlaví 27
2.3.3 Mesh záhlaví 28
2.3.4 Komprese záhlaví IPv6 dle RFC 4944 29
2.4 Implementace 30
2.4.1 Contiki OS 30
2.4.2 TinyOS 31

3 Spotřeba energie v sítích WSN **32**
3.1 Spotřeba energie komunikačního bloku 32
3.1.1 Spotřeba energie přijímací části 33
3.1.2 Spotřeba energie vysílací části 33

4 Snížení spotřeby energie v sítích WSN **35**
4.1 Snížení spotřeby energie z hlediska fyzické vrstvy 35
4.1.1 Druhy baterií 36
4.2 Snížení spotřeby energie z hlediska linkové vrstvy 39
4.2.1 Režim spánku 39
4.2.2 MAC protokoly 42

5 Praktická část **49**
5.1 Experimentální měření 49
5.1.1 Použité přístroje a součástky 49
5.1.2 Schéma zapojení 49

5.1.3 Výsledky měření 50
5.1.4 Srovnání spotřeby s ostatními bezdrátovými technologiemi . . 52
5.2 Návrh měření 53
5.2.1 Vybrané měřicí přístroje a součástky 53
5.2.2 Schéma zapojení 56

6 Závěr **58**

Literatura **60**

Seznam symbolů, veličin a zkratek **65**

Seznam příloh **67**

A Naměřené průběhy zobrazené na osciloskopu **68**
A.1 Zobrazený průběh odběru proudu při zapnutí senzorového uzlu . . . 68
A.2 Přiblížený průběh odběru proudu při zapnutí senzorového uzlu . . . 69
A.3 Zobrazený průběh odběru proudu při komunikaci senzorových uzlů . 70
A.4 Přiblížený průběh odběru proudu při komunikaci senzorových uzlů . 71

SEZNAM OBRÁZKŮ

1.1 Bezdrátový přenos nasbíraných dat k základní stanici 12
1.2 Struktura PAN sítě standardu 802.15.4 14
1.3 Topologie a) hvězda b) peer to peer 15
1.4 Kmitočtové rozložení kanálů 16
1.5 Překrytí kanálů standardem 802.11 17
1.6 Schéma senzorového uzlu 18
2.1 Příklad komunikace koncových bodů se základní stanicí 21
2.2 Porovnání vrstvového 6LoWPAN modelu s modelem TCP/IP 22
2.3 Zapouzdření hlavičky adaptační vrstvou 6LoWPAN 27
2.4 Fragmentované záhlaví adaptační vrstvou 6LoWPAN 28
2.5 Mesh záhlaví protokolu 6LoWPAN 28
2.6 Komprese záhlaví IPv6 dle RFC 4944 29
3.1 Blokové schéma komunikačních obvodů 33
4.1 Blokové schéma napájení transceiveru 35
4.2 Procesy MAC protokolu s asynchronním pracovním cyklem 43
4.3 Procesy MAC protokolu se synch. pracovním cyklem 45
4.4 Struktura superrámce 47
5.1 Schéma zapojení kitu TI INA210-214EVM 50
5.2 Naměřený průběh odběru proudu při zapnutí senzorového uzlu 51
5.3 Naměřený průběh odběru proudu při komunikaci 52
5.4 Navržené schéma zapojení 56
A.1 Zobrazený průběh odběru proudu při zapnutí senzorového uzlu 68
A.2 Přiblížený průběh odběru proudu při zapnutí senzorového uzlu 69
A.3 Zobrazený průběh odběru proudu při komunikaci senzorových uzlů . . 70
A.4 Přiblížený průběh odběru proudu při komunikaci senzorových uzlů . . 71

SEZNAM TABULEK

4.1 Porovnání typu baterií používaných v sítích WSN 38
4.2 Spotřeba jednotlivých částí senzorového uzlu 40
4.3 Přehled metod režimu spánku a jejich využití 41
4.4 Tabulka srovnání MAC protokolů pro sítě WSN 48
5.1 Porovnání technologií bezdrátového přenosu dat 52
5.2 Porovnání operačních zesilovačů 53
5.3 Porovnání osciloskopů 54
5.4 Porovnání napájecích zdrojů 55

ÚVOD

Bezdrátové senzorové sítě neboli Wireless Sensor Network se v dnešní době stávají stále populárnějšími. Velkou roli zastávají v systémech pro sbírání informací z fyzického prostředí v celé řadě sledování a pozorování od zabezpečovacích systémů, po lesní požáry, zvířata v zemědělství nebo řízení průmyslového monitorování. S pokročilejšími technologiemi se vývojáři WSN sítí snaží o rozšíření oblastí využitelnosti těchto sítí a také, o jejich co možná nejlepší spolehlivost a co nejdelší životnost, která úzce souvisí se spotřebou. Od spotřeby se odvíjí vývoj v oblasti energetické účinnosti komunikačních protokolů, směrovacích protokolů, hardwaru apod. Pokrok zaznamenaly i možnosti napájení senzorových uzlů, které v současné době častěji využívají napájení a dobíjení napájecích článků alternativními zdroji, tedy pomoci solární energie a energie vibračních dějů.

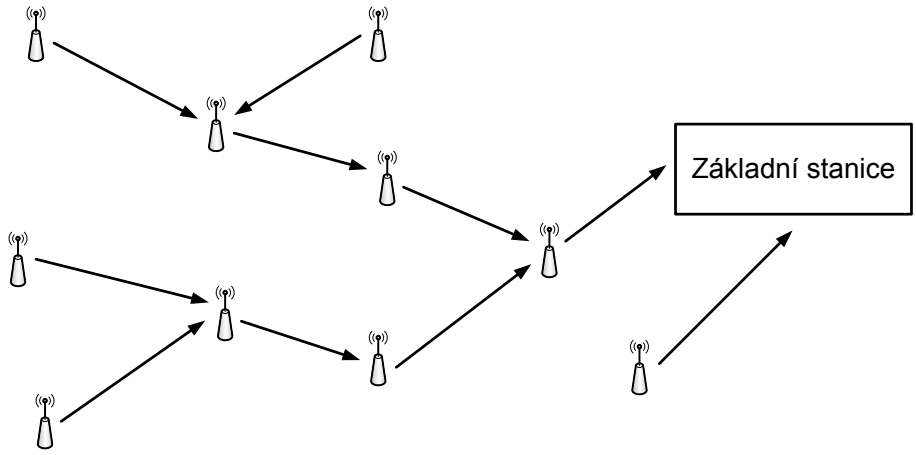
Tato práce se zaměřuje na problematiku energetické náročnosti IPv6 v bezdrátových senzorových sítích. Řeší jednotlivé vrstvy standardu IEEE 802.15.4, na jehož základě jsou WSN sítě postaveny. Bude se zabývat energetickou náročností jednotlivých vrstev právě standardu 802.15.4 při přenosu v rámci protokolu IPv6. Budou zde rozebrány možné způsoby snížení spotřeby senzorových uzlů z hlediska fyzické a linkové vrstvy. Ve fyzické vrstvě je nejdůležitější výběr vhodného způsobu čerpání energie a zdroje napájení. Linková vrstva v dnešní době definuje velké množství synchronních a asynchronních MAC protokolů, jejichž vlastnosti budou v práci popsány. Z hlediska úspory energie na linkové vrstvě je důležitý režim spánku a právě výběr vhodného MAC protokolu.

Cílem práce je nastudování a zhodnocení možných řešení snížení energetické náročnosti standardu 6LoWPAN, dále pak měření spotřeby senzorového uzlu a vlastní návrh na zlepšení měřící metody, který zahrnuje výběr operačního zesilovače, měřícího přístroje, napájecího zdroje, sestavení schématu a sepsání postupu měření.

1 BEZDRÁTOVÉ SENZOROVÉ SÍTĚ

1.1 Úvod do bezdrátových senzorových sítí

Vývoj bezdrátových senzorových sítí, neboli Wireless Sensor Networks (WSN), začal po roce 2000 a vzešel z myšlenky, že malé bezdrátové senzory mohou být využity pro sbírání informací z fyzického prostředí v celé řadě sledování a pozorování od zabezpečovacích systémů, po lesní požáry, zvířata v zemědělství nebo řízení průmyslového monitorování [1]. Fungují na principu, že každý jednotlivý senzorový uzel bezdrátově přenáší nasbíraná data k základní stanici. Jednotlivé senzory spolu vzájemně kooperují, viz Obr. 1.1 [1].



Obr. 1.1: Bezdrátový přenos nasbíraných dat k základní stanici [1]

Jedním z prvních systémů realizovaných pomocí bezdrátových senzorových sítí byl systém zvaný „Smart dust“. Jednalo se o systém složený z velkého množství drobných elektronických komponentů, jež jsou vybaveny rádiovým vysílačem, malým mikroprocesorem a zdrojem energie, nejčastěji baterií. Jejich funkce je snímání, počítání a schopnost komunikovat [1]. Využívaly se v prostředí, kde měly být měřeny jevy jako je teplota, tlak, zvuk, vibrace nebo vlhkost. Jelikož elektronické komponenty byly tak malé, mohly být rozptýleny pomocí mechanismů, jako je proudění vzduchu [1]. Tento systém byl využíván zejména armádou, která jej používala k zapnutí alarmu, když byl zjištěn vetřelec v monitorovaném prostoru nebo ke zjištění přítomnosti vozidel. Kvůli malým rozměrům byla značně omezena schopnost komunikace a výpočetní schopnost uzlů a tedy i použitelnost. Místo toho se začaly stavět systémy s větší konstrukcí, které umožňovaly snadnější simulaci a zkoumaní jejich chování v provozních podmínkách [1] [2].

Za léta výzkumu v oblasti bezdrátových senzorových sítích bylo vytvořeno velké množství důležitých mechanismů a algoritmů. Vzhledem k tomu, že bezdrátové senzory obvykle používají baterie s dlouhodobou životností, je zde velmi důležité řešit problém spotřeby energie jednotlivých uzlů. V praxi to vypadá tak, že jednotlivé uzly jsou z hlediska spotřeby zkoumány v simulačních programech, simulující reálné podmínky, a na základě jejich hodnocení jsou navrhovány opatření pro co nejnižší spotřebu energie a co nejdelší životnost. V dnešní době jsou tyto sítě vnímány jako sítě s velmi dlouhou životností (několik měsíců až let) [1].

Velký význam mají v oblasti technologií pro průmyslovou automatizaci a monitorování. Mnohé, z již existujících norem v průmyslových bezdrátových sítí, jako je WirelessHART a ISA100a, mají své kořeny v komunitě bezdrátových senzorů sítí [1].

Jedním z hojných využití WSN v současné době jsou sociální aplikace, jako je řízení domácnosti, které jsou typickým příkladem sítí, jenž musí být řízeny samostatně, a vyžadují minimální konfiguraci od koncového uživatele [1].

S vývojem bezdrátových senzorových sítí je úzce spojen i vývoj inteligentních objektů (Smart objects). Bezdrátové senzorové sítě jsou složeny z malých uzlů, které jsou vybaveny bezdrátovým komunikačním zařízením, jenž se zcela samostatně připojí a nakonfiguruje do sítě, a jejichž prostřednictvím jsou pak nasbírána data posílána. Inteligentní objekty v síti nejsou zaměřeny čistě jenom na sběr dat, ale jsou určeny pro velké množství dalších úkolů, včetně ovládání a kontroly. Bezdrátové senzorové sítě jsou primárně určeny pro přenos dat přes bezdrátové zařízení rádiové komunikace, v kontrastu s tím nejsou inteligentní objekty vázány na konkrétní mechanismus komunikace, ale naopak mohou běžet přes kabelové i bezdrátové sítě [1], [2].

1.2 Standard IEEE 802.15.4

Standard IEEE 802.15.4 je určený pro bezdrátové technologie o malém výkonu a malé přenosové rychlosti. Norma byla vypracována v rámci standardu 802.15 používaný pro místní Osobní sítě PAN (Personal Area Network). IEEE 802.15.4 má maximální přenosovou rychlost 250 kbit/s [1] a maximální výstupní výkon 1 mW [1]. Zařízení pracující na tomto standardu zajišťují dosah běžně na několik desítek až tisíc metrů, byl již však odzkoušen i na dosah několik km [1]. Hlavní význam IEEE 802.15.4 je zajistit co nejjednodušší a nejméně nákladné transceivery (vysílač s přijímačem) používané pro inteligentní objekty. Velký zájem o tuto technologii zapříčinil značný rozmach ve výrobě zařízení kompatibilních s tímto standardem [1].

Vzhledem k velkému rozšíření IEEE 802.15.4 a dostupnosti IEEE 802.15.4 kom-

patibilních transceiverů bylo na tomto standardu postaveno mnoho nově vzniklých nízkonapěťových přenosových norem [3].

Standard IEEE 802.15.4 specifikuje dvě vrstvy:

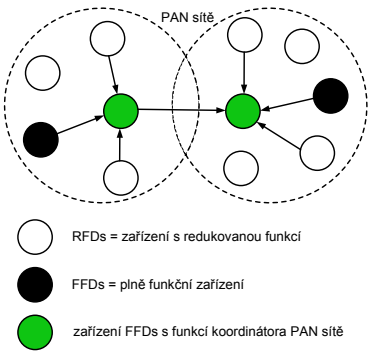
- Fyzická vrstva - PHY (Physical Layer).
- Linková vrstva - MAC (Medium Access Controll).

Ačkoliv IEEE 802.15.4 norma specifikuje několik mechanismů ve fyzické a MAC vrstvě, nejsou všechny části této specifikace vždy využity. Například standardní WirelessHART používá fyzickou vrstvu specifikace a MAC vrstvu, ale pouze v omezené míře. Místo MAC vrstvou nadefinovaného formátu přidá svůj vlastní formát hlavičce paketu [3].

Maximální velikost paketu v 802.15.4 je 127 oktetů [1]. Pakety jsou malé, protože standard IEEE 802.15.4 je určen výhradně pro zařízení o nízkém výkonu přenosu dat s nízkou přenosovou rychlostí. Protože MAC vrstva přidává hlavičku ke každému paketu, je množství dat určené pro vyšší vrstvy protokolu nebo aplikace v rozmezí 86 až 116 bajtů. Horní vrstvy protokolu proto často využívají fragmentaci [3].

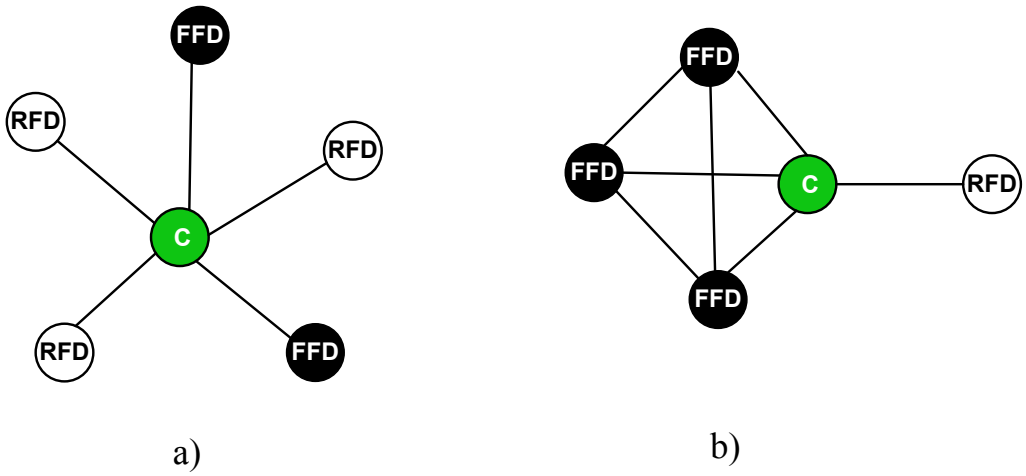
Typická realizace standardu 802.15.4 je prováděna pomocí kombinace hardwaru a softwaru. Nízké úrovně částí fyzické vrstvy a částí zpracování MAC jsou realizovány pomocí hardwaru, zatímco částí vyšší úrovně, jako je logická vrstva MAC, jsou implementovány v softwaru.

IEEE 802.15.4 sítě jsou rozděleny do osobních sítí, viz Obr. 1.2 [3]. Každá osobní síť má PAN koordinátora a skupinu PAN členů. Pakety odeslané přes PAN sítě prochází přes PAN identifikátor, který určuje do jaké PAN sítě je paket určen. Jedno zařízení může působit v jedné PAN síti jako koordinátor a zároveň v další síti působit jako člen PAN sítě [3].



Obr. 1.2: Struktura PAN sítě standardu 802.15.4 [3]

IEEE 802.15.4 specifikuje dva typy zařízení: plně funkční zařízení FFD (Full-Function Device) a zařízení s redukovanou funkcí RFD (Reduced-Function Device). FFD zařízení jsou schopnější než zařízení RFD a mohou působit jako koordinátoři v sítích PAN. Oproti tomu RFD zařízení jsou jednodušší, snadněji realizovatelné a díky tomu také méně nákladné z hlediska výroby. RFD může komunikovat pouze se zařízeními FFD, FFD mohou komunikovat s oběma typy [3].

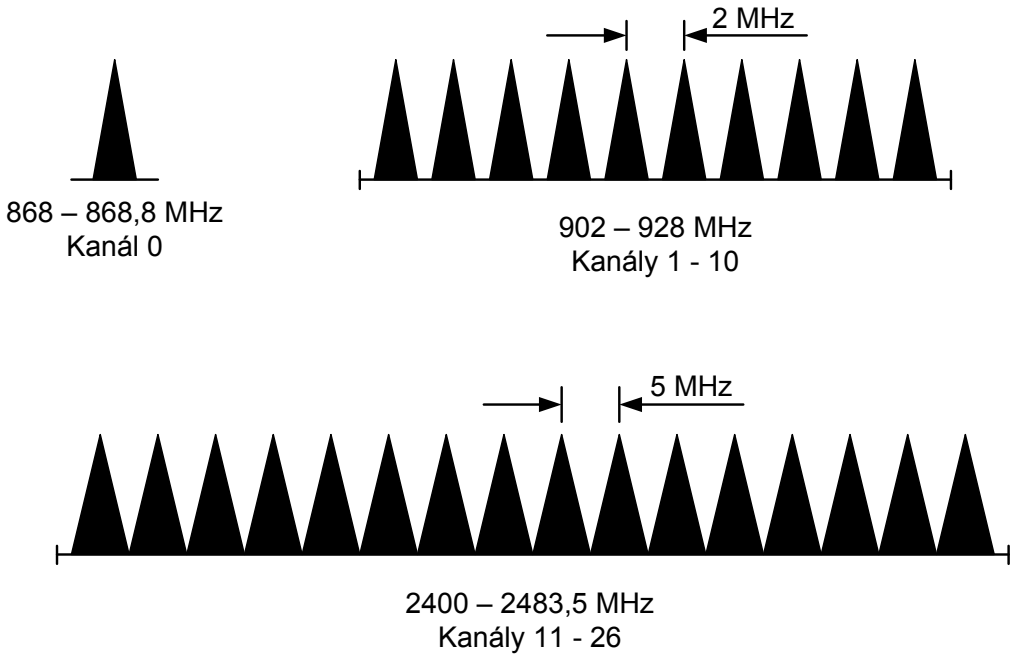


Obr. 1.3: Topologie a) hvězda b) peer to peer [3]

Ačkoli 802.15.4 definuje dva typy síťových struktur topologii hvězda a peer to peer (komunikace každý s každým) [1] viz Obr. 1.3 [3], většina protokolů, které fungují na vrcholu 802.15.4, nepoužívají 802.15.4 topologie. Místo toho si budují vlastní topologii sítě [1] [3].

1.2.1 Fyzická vrstva

Všechna zařízení v bezdrátových osobních místních sítích (PAN) s malým dosahem obsahují fyzickou vrstvu. Fyzická vrstva zodpovídá za přenos a příjem dat a definuje parametry bezdrátového přenosu. Jedním z těchto parametrů je modulační kmitočet. Standard IEEE 802.15.4 pracuje na třech kmitočtových pásmech. Vzhledem k odlišným normám platí na různých částech světa jiná frekvenční pásma. V USA využívá IEEE 802.15.4 pásmo $902 \div 928\,\mathrm{MHz}$ [3]. V Evropě je to $868 \div 868,8\,\mathrm{MHz}$ [3], ve zbytku světa se používá pásmo $2400 \div 2483,5\,\mathrm{MHz}$ [3].

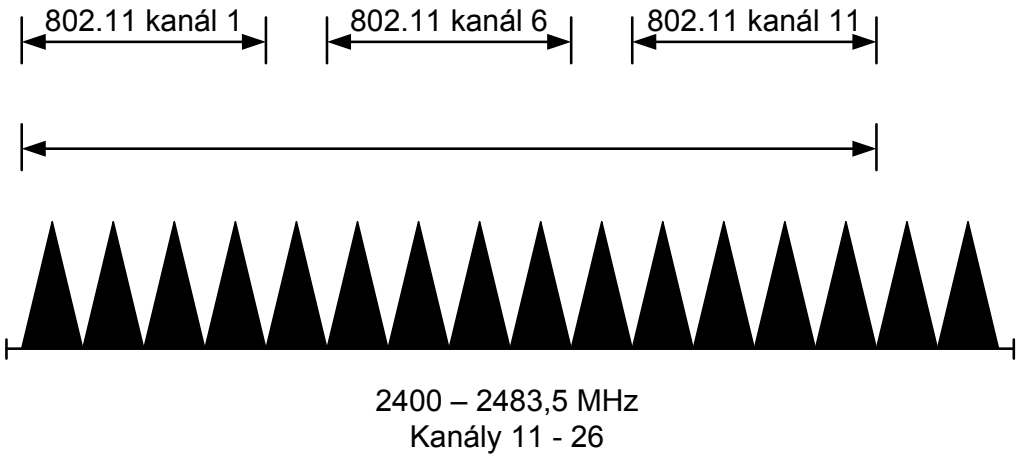


Obr. 1.4: Kmitočtové rozložení kanálů [3]

Dalším parametrem je počet kanálů v různých frekvenčních pásmech viz Obr. 1.4 [3]. IEEE 802.15.4 definuje 26 provozních kanálů. Kanál 0, který je definován v Evropě, pracuje ve frekvenčním pásmu 868 MHz [3]. V USA jsou definovány kanály $1 \div 10$ na frekvenci $902 \div 928$ MHz s odstupem kanálů 2 MHz [3]. Kanály $11 \div 26$ jsou v pásmu 2,4 GHz, což z nich dělá kanály dostupné po celém světě všude s odstupem kanálů 5 MHZ [3].

Různá pásma s různými kanály používají také odlišné modulace a přenosové rychlosti. Modulace Offset Quadrature Phase-Shift Keying (QPSK) se používá pro nelicencované pásmo 2,4 GHz [3] s 16 celosvětovými kanály při rychlosti 250 kbit/s [3]. V Americe na kmitočtu 915 MHz s deseti kanály je to modulace dvoustavového fázového klíčování Bi Phase-Shift Keying (BPSK) při rychlosti 40 kbit/s, v Evropě s jedním kanálem 0 o rychlosti 20 kbit/s a opět s modulací BPSK [3]. Na všech kanálech využívá IEEE 802.15.4 modulaci pro rozprostření spektra na základě přímé sekvence kódu Direct Sequence Spread Spectrum (DSSS) [4].

IEEE 802.15.4 stanice v pásmu 2,4 GHz se musí podělit o přenosové frekvence se standardem IEEE 802.11 (Wi-Fi) [3]. Protože má 802.11 výrazně vyšší výkon, dochází k překrývání kanálů, což má za následek rušení provozu stanic, pracujících na standardu IEEE 802.15.4. [3] Na Obr. 1.5 lze vidět, že všechny kanály 802.11 (kanály 1, 6 a 11) překrývá až na kanály číslo 15 a 20, které svým provozem neruší a kanály 25 a 26, na které se 802.11 nevztahuje [3].



Obr. 1.5: Překrytí kanálů standardem 802.11 [3]

Mezi další úlohy fyzické vrstvy patří posílání signálu o volnosti média CCA (Clear Channel Assessment) přístupové metodě MAC vrstvy [4].

1.2.2 Linková vrstva

Zajišťuje řízení přístupu k médiu, což znamená, že určuje, jak se zpracovávají data přijatá přes fyzickou vrstvu. Poskytuje přístupovou metodu CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), která se označuje jako metoda s vícenásobným přístupem a naslouchání nosné. Používá signál CCA a funguje tak, že před začátek vysílání paketu stanice naslouchá určitý čas (pevná + náhodně generovaná část čekací doby) médium, a pokud je médium volné k přenosu, začne vysílat. V opačném případě čeká stanice náhodně vygenerovanou dobu a po té opět zkontroluje médium, jestli je už možno vysílat. Veškerá komunikace touto metodou je zpětně potvrzována ACK (Acknowledgment) pakety. Když stanice obdrží data a jsou v pořádku, pošle vysílající stanici informaci, že obdržela data nepoškozena. V případě, že vysílající stanice toto potvrzení nedostane, předpokládá se, že došlo během přenosu ke ztrátě dat a přenos se po náhodně zvoleném čase opakuje. Tato přenosová metoda se snaží předcházet kolizím, avšak vzniklé kolize není schopna detekovat [1], [3], [4].

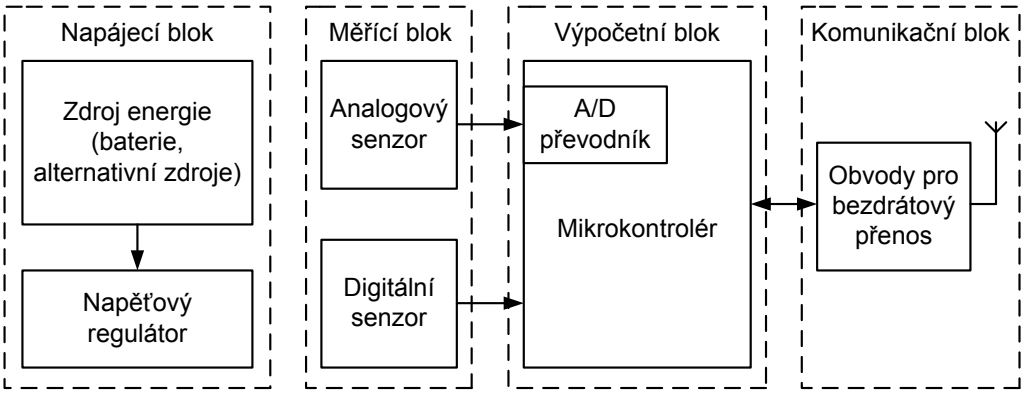
Kromě MAC vrstvy obsahuje linková vrstva ještě vrstvu LLC (Logical Link Control), která zajišťuje MAC adresaci, řízení toku dat, vytváření rámců a kontrolu chyb [1].

1.2.3 Vyšší vrstvy

K vyšším vrstvám se řadí síťová vrstva, která obstarává sestavení sítě, manipulaci s pakety a směrování paketů podle zvolené topologie, dále vrstva aplikační, u které se řeší energetická náročnost konkrétní aplikace [3].

1.2.4 Senzorový uzel

Senzorová síť se skládá z malých elektronických komponentů, obsahujících čtyři části viz Obr. 1.6 [5]:



Obr. 1.6: Schéma senzorového uzlu [5]

Komunikační blok

Komunikační blok (transceiver) se skládá z vysílací části (transmitter) a přijímací části (receiver). Bezdrátový přenos probíhá přes rádiové vlny nebo optické vlny (nižší energetická spotřeba, ale nutnost přímé viditelnosti) na frekvenčním pásmu $433 \div 2400\,\mathrm{Hz}$ [1].

Transceiver pracuje ve čtyřech režimech [5]:

- Režim vysílání.
- Režim příjmu.
- Režim nečinnosti (idle mode).
- Režim spánku (sleep mode).

Výpočetní blok

Výpočetní blok (programovatelný mikrokontrolér) obsahuje mikroprocesor, paměť, A/D převodník a vstupy/výstupy pro periferní zařízení. Zpracovává data, vykovává úkoly a dohlíží na správnou funkci ostatních součástí senzorového uzlu [5].

Typy pamětí mikrokontroléru:

- Programovací paměť FLASH.
- Datová paměť RAM.
- Paměť EEPROM.

Měřící blok

Měřící blok je složen z digitálních nebo analogových (potřeba A/D převodníku) senzorů, které nasbírají data a pomocí digitálního signálu je pošlou k dalšímu zpracování. Požadavky na senzory jsou malá velikost, nízká energetická náročnost, přizpůsobivost prostředí. Senzory jsou schopny monitorovat životní prostředí, teplotu, vlhkost, atmosferický tlak, pohyb, zvuk, atd [5].

Napájecí blok

Napájecí je blok se skládá ze zdroje energie a napěťového regulátoru. Důležitým požadavkem na napájecí zdroj je maximální proudový odběr, který musí pokrýt požadavky senzorového uzlu, zejména při komunikaci a zpracovávání nasbíraných dat. V dnešní době jsou nejčastějším zdrojem energie senzorového uzlu nabíjecí baterie, nebo energie získaná z alternativních zdrojů. Alternativní zdroje získávají energii z okolního prostředí, nejčastěji ze slunečního záření a vibračních dějů. Jako napěťové regulátory se používají buď přepínané regulátory, nebo lineární regulátory [5].

Rozdělení senzorových uzlů

Senzorové uzly se svou funkcí dělí na:

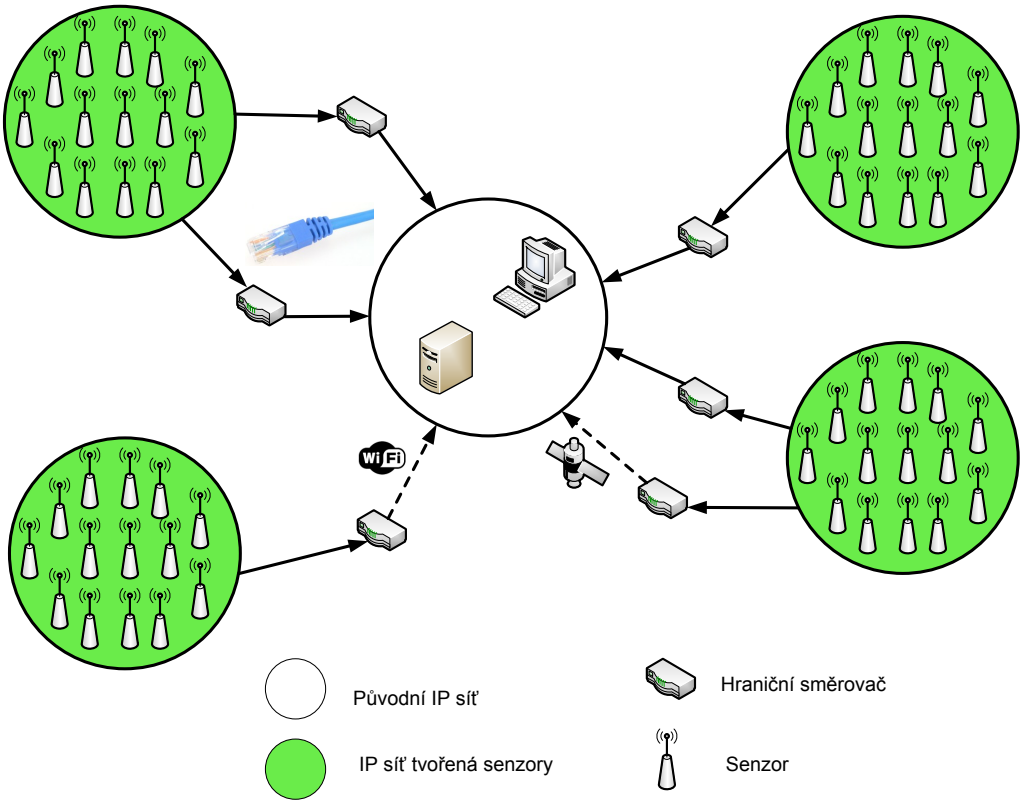
- Routery (směrovače ve WSN síti) – přeposílají data od senzorových uzlů k základní stanici, která je poté vyhodnocuje.
- Node (senzorové uzly pro sbírání dat) – sbírají data (sledování a monitorování), která pak přeposílají na router.

2 PROTOKOL 6LOWPAN

V dnešní době je velká snaha o co největší zařazení inteligentních objektů do sítí s funkcí, jako je například: sledování životního prostředí, nebo do sítí zabezpečovacích systémů a průmyslové kontroly. Aby bylo využití inteligentních objektů co největší, musí poskytnout více kontrolních bodů pro pokrytí co největší zeměpisné oblasti za nižší cenu. Tyto požadavky spolu ještě s požadavkem na mikrokontrolér MCU (Machine Control Unit) s nízkou spotřebou a dlouhodobou životností jednotlivých uzlů sítě, přiměly vymyslet nový standard pro tyto systémy. Stal se jím protokol 6LoWPAN, pracující se síťovým protokolem IPv6. Na rozdíl od jiných WPAN technologií, jako je Bluetoooth, určený zejména pro připojení sluchátek, herních ovladačů a osobních zařízení, má 6LoWPAN omezenější možnosti co se týká přenosové rychlosti a vysílajícího výkonu, ale také o mnoho nižší provozní náklady a dlouhou životnost [6] [7].

6LoWPAN radikálně mění současnou strukturu bezdrátových senzorových sítí zavedením adaptační vrstvy, která umožňuje komunikaci přes IPv6 aplikací standartu IEEE 802.15.4 na nízko-výkonové osobní bezdrátové sítě LoWPAN (Low power Wireless Personal Area Networks). Adaptační vrstva je IETF standardem a poskytuje kompresi hlaviček rámců pro snížení režie přenosu, fragmentaci na podporu IPv6, minimální požadované velikosti maximální přenosové jednotky Maximum Transmission Unit (MTU) a podporu pro druhou vrstvu při přenosu dat přes více stanic [6].

Senzory pracující na protokolu 6LoWPAN vytvářejí vlastní IP sítě a prostřednictvím jednoho či více hraničních směrovačů jsou připojeny k původní IP síti, ve které se také nachází základní stanice pro zpracování nasbíraných dat, jak je vidět na Obr. 2.1 [6]. Toto připojení může být realizováno různými technologiemi jako je např. Ethernet, Wi-Fi, GPRS, nebo satelit [6].



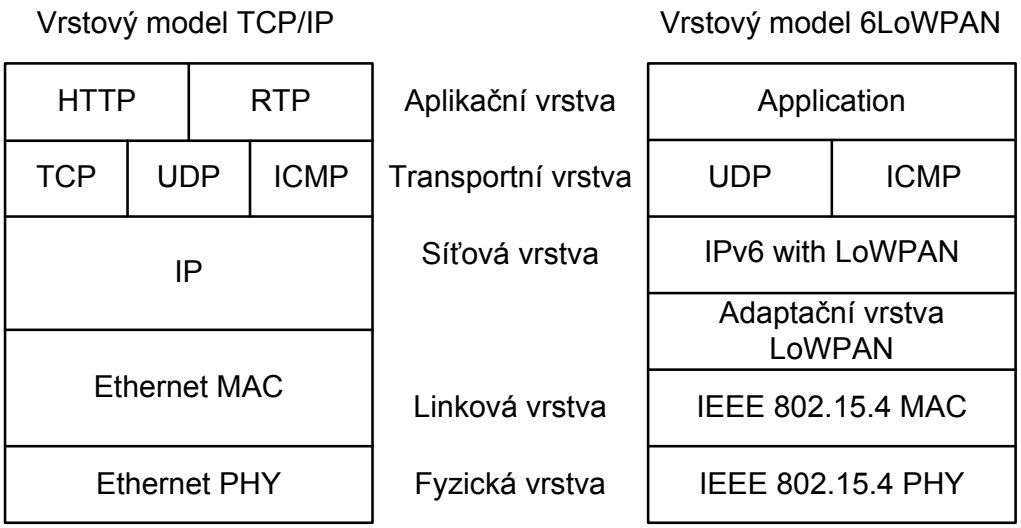
Obr. 2.1: Příklad komunikace koncových bodů se základní stanicí [6]

Vzhledem k tomu, že hraniční směrovače předávají IP diagramy na síťové vrstvě, nemusí brát ohled na aplikační vrstvu, na rozdíl od jiných architektur ad-hoc sítí (např. ZigBee), které využívají aplikační brány pro spojení LoWPAN sítí s ostatními IP sítěmi [6]. Aplikační brány, neboli také Proxy firewally, jsou zařízení, která slouží k oddělení jednotlivých sítí a poskytují překlad síťových adres NAT (Network Address Translation). Tyto aplikační brány se musí přizpůsobit nastavení LoWPAN sítě a veškeré změny v souvislosti s bezdrátovými uzly v aplikačním protokolu, musí být zaznamenány změnami v právě v těchto branách. Protokol 6LoWPAN aplikační brány nevyužívá, ale ve světě internetu jsou pro optimalizaci běžně využívány [6].

6LoWPAN společně se ZigBee patří k nejvíce využívaným standardům pro bezdrátové senzorové sítě [7]. ZigBee je oproti 6LoWPANu již poměrně starou, avšak neustále hojně využívanou, technologií. Je označována jako průkopnická technologie v oblasti bezdrátových senzorových sítí využívající prvky ke snížení spotřeby energie jako je režim spánku, apod [7].

2.1 Vrstvy 6LoWPANu

Vrstvový model 6LoWPANu je velmi podobný vrstvovému modelu TCP/IP. Porovnání těchto vrstvových modelů je na Obr. 2.2 [7].



Obr. 2.2: Porovnání vrstvového 6LoWPAN modelu s modelem TCP/IP [7]

Jednotlivé vrstvy 6LoWPAN [7]:

- **Fyzická vrstva** – je založena na standardu 802.15.4. Součástí fyzické vrstvy je transceiver, složený z transmitteru (vysílače) a receiveru (přijímače) sloužící k bezdrátovému přenosu. Rychlost přenosu je 250 kbit/s [1] v pásmu $2400 \div 2483,5$ MHz [1]. Maximální velikost paketu je 127 oktetů [1].

- **Linková vrstva** – pomocí MAC (Medium Acces Control)vrstvy zajišťuje přístup k médiu a vrstvu LLC (Logical Link Control), která zajišťuje MAC adresaci, řízení toku dat, opravu chyb a vytváření rámců. MAC vrstva určuje přístupovou metodu CSMA/CA. Určuje také jestli bude senzorový uzel přenášet v synchronizačním nebo asynchronním režimu.

- **Adaptační vrstva** – pomocí rámců standardu 802.15.4 definuje způsob komunikace sítě IPv6. Skládá se ze tří prvků (komprese hlaviček, fragmentace a přesměrování na síťovou vrstvu). Adaptační vrstva je velmi důležitou součástí, protože IPv6 pakety přizpůsobuje na rámce pro bezdrátové senzorové sítě.

- **Síťová vrstva** – zajišťuje správu sítě pomocí protokolu SNMP (Simple Network Management Protocol). Obsahuje směrovací protokoly: Route Over (směrování v síťové vrstvě 6LoWPAN), které se dále dělí na LOAD – 6LoWPAN Ad-hoc On-Demand Distance Vector, DYMO-LOW – Dynamic MANET On-demand for 6LoWPAN Routing a HiLow –Hierarchical Routing. Síťová vrstva sestavuje spojení od začátku až po jeho konec.

- **Transportní vrstva** – zajišťuje samotný přenos dat. Využívá zejména protokol nespolehlivého přenosu dat UDP (User Datagram Protocol) a protokol ICMP (Internet Control Message Protocol), který slouží pro odesílání chybových zpráv, dotazování např. na ping apod. Je zodpovědná za poskytování údajů příslušnému procesu aplikace běžící na hostitelském počítači.

- **Aplikační vrstva** – poskytuje přístup aplikacím ke komunikačnímu systému, obstarává jejich spolupráci. Mezi aplikace využívající 6LoWPAN patří: monitorování životního prostředí, bezpečnostní systémy, systémy pro sledování zdraví, automatizace budov a další.

2.2 IPv6

Protokol IPv6 byl navržen jako nástupce protokolu IPv4 a hraje zásadní roli v IP sítích s inteligentními objekty. Striktně dodržuje architektonické principy IP, v podstatě je to další řešení některých omezení starší verze protokolu IPv4, avšak protokol IPv4 znamenal průlom v technologii internetu a je v provozu už 25 let a nepochybně zůstane v provozu i nadcházející roky. Autoři protokolu IPv6 vyvinuli nepřeberné množství mechanismů, jež by měl usnadnit přechod z IPv4 na IPv6 [6].

Klíčové funkce protokolu IPv6 [6]:

- **Větší adresní prostor potřebný pro sítě ve velkém měřítku** – Ačkoliv se některé nízko-energetické a nízko-ztrátové sítě LLN (Low-power and Lossy Networks), jako jsou sítě domácí automatizace, mohou skládat z několika desítek uzlů, v mnoha jiných případech může být počet těchto uzlů řádově větší než v běžných sítích IP. Například městské sítě, nebo inteligentní sítě pro průmyslovou automatizaci budou zahrnovat stovky až tisíce uzlů. Protokol IPv4 má omezený počet adres a předpokládá se, že k vyčerpání jeho kapacity dojde kolem roku 2012. Protokol IPv6 rozšiřuje adresní prostor z 32 bitů na 128 bitů [1], čímž zajišťuje výrazně větší počet adresovatelných uzlů, stejně jako mnoho dalších úrovní hierarchie adresování a automatickou konfiguraci funkce [1] [6].

- **Automatická konfigurace** – Využívá se zejména u sítí velkého rozsahu, jako jsou městské sítě, nebo sítě pro průmyslovou automatizaci. Jejích úkolem je konfigurace zařízení, automatické přidělování adres, detekce chyb, analýza výkonnosti apod. V praxi to znamená, že sítě IPv6 oproti IPv4 nepotřebují překlad adres (IPv4 potřebuje bránu). Tyto vlastnosti přispívají k tomu, že IPv6 se stává velmi oblíbeným protokolem pro bezdrátové senzorové sítě [6].

- **Úprava záhlaví** – Nevyužitá pole v záhlaví rámců protokolu IPv4 jako fragmentace, kontrolní součet, atd. byly odstraněny. Byla vytvořena jednodušší konstrukce s pevnou hlavičkou.

- **Ověřování a ochrana soukromí** – Oproti IPv4 je zde rozšířená podpora autentizace, integrity a důvěryhodnosti.

- **Zabezpečení** – Zatímco IPSec (IP Security = bezpečnostní rozšíření IP protokolu) bylo u protokolu IPv4 pouze volitelné, u IPv6 je bezpodmínečně požadované.

IPv6 také odráží pokroky v technologiích v oblasti internetu. Dominantní vazbou se postupem času stal Ethernet, jehož výkon velice vzrostl. Velké využití mají také aktuální WLAN (Wireless Local Area Network) technologie. Asi nejpoužívanější je standard Wi-Fi (Wireless Fidelity), který stejně jako Ethernet podporuje vysoké velikosti MTU a poskytuje dostatečný výkon pro přenos dat. Dalším standardem, který pracuje v bezdrátové lokální síti je WPAN (Wireless Personal Area Network). Narozdíl od Wi-Fi má WPAN výrazně nižší výkon, na druhou stranu se vyznačuje dlouhodobou životností. Nízko-energetické nároky zaručuje např. protokol 6LoWPAN a mikroprocesory s nízkou spotřebou. Propustnost je omezena na 250 kbit/s [6], velikost MTU na 127 bajtů [6]. Je zde poměrně vysoká chybovost během přenosu, způsobená omezenou schopností ukládání dat do vyrovnávací pamětí používaných mikroprocesorů, kdy se paket při vysílání poškodí. Standard 802.15.4 definuje kromě IEEE EUI-64 adresy (6 bitový rozšířený identifikátor), také krátké 16 bitové adresy, aby se snížila velikost záhlaví a požadavky na paměť. Na rozdíl od většiny typických WPAN a WLAN zařízení, umí LoWPAN komunikovat přes více skoků (hopů). Mikroprocesory používané v u zařízení LoWPAN mají obvykle okolo 8 KB paměti RAM a 64 KB paměti ROM [1] [6].

Vzhledem k omezení hopů při přenosu v LoWPAN sítí, představuje podpora IPv6 v sítích LoWPAN několik problémů:

- Datagramy (datagram = datový paket posílání v sítí IP) posílané sítí s protokolem IPv6, nejsou přizpůsobené k přenosu sítí LoWPAN. Kvůli nízké propustnosti, omezenému ukládání dat do vyrovnávací paměti mikroprocesoru a sníženému MTU požadavku na jednu desetinu musí být IPv6 datagramy pro efektivní přenos fragmentovány nebo komprimovány. Realizuje se to úpravou záhlaví hlavičky. Maximální velikost záhlaví hlavičky je 81 bajtů [6], což znamená: protokol IPv6 (40 bajtů) [6], protokol UDP - User Datagram Protocol (8 bajtů) [6] a protokol TCP - Transmission Control Protocol (20 bajtů) [6].

- Standard 802.15.4 má nízký výkon přenosu, malou propustnost a je náchylný na rušení, které má často za následek selhání spojení. Síťová vrstva IPv6 vyžaduje spolehlivost a předvídatelné chovaní. Nízko-energetické prvky v síti LoWPAN mají vliv na fragmentaci, kompresi, předávání a směrování dat v síti [6].

- Topologie používaná pro sítě LoWPAN je určená pro krátký dosah spojení, což nefunguje za předpokladu, že hlavní součásti IP architektury, jako je IPv6. IETF tento problém, týkající se pracovních skupin 6LoWPAN, řešila pomocí RFC 4944 [6] [8].

2.3 Adaptační vrstva 6LoWPAN

Protokol 6LoWPAN definuje způsob komunikaci přes IPv6 pomocí rámců standardu 802.15.4 a pomocí aplikační prvky upřesňuje klíčové prvky komunikace. 6LoWPAN má tři hlavní prvky: [6] [7]

- **Komprese hlaviček** – Komprese hlaviček: Záhlaví protokolu IPv6 jsou komprimována za předpokladu použití stejných hodnot. Záhlaví pole paketu jsou zmenšována a můžou obsahovat informace o změnách prováděných během přenosu na úrovni 802.15.4 rámce [6].

- **Fragmentace** – Z důvodu malé velikosti maximální přenosové jednotky (MTU) musí být IPv6 pakety rozděleny do více částí, ale obsah dat zůstává nezměněn [6].

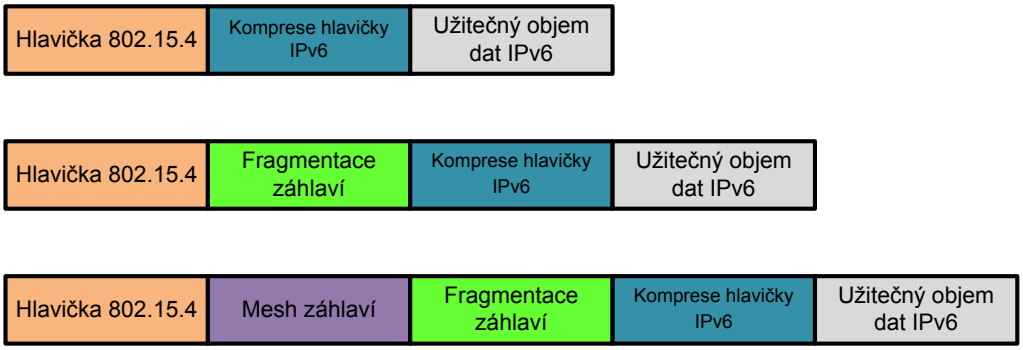
- **Přesměrování z linkové vrstvy na síťovou** – Adaptační vrstva může nést adresy odkazující na konec skoku v případě zasílání IPv6 datagramů linkovou vrstvou. Případně by IP stack (implementace souboru komunikačních protokolů) uvnitř sítě PAN mohl dosáhnout směrování přes síťovou vrstvu, ve které je každý 802.15.4 hop považován za IP hop [6].

Důležitou součástí celé adaptační vrstvy 6LoWPAN je použití fragmentace a komprese záhlaví paketů na úrovni všech tří vrstev, z důvodu různé velkosti minimálního MTU u různých typů sítí (např. Ethernet, WLAN, atd.). IPv6 často při přenosu využívá UDP, TCP a ICMPv6, které mají záhlaví protokolu IPv6 stejnou velikost a mohou být komprimována. 6LoWPAN také zmenšuje počet redundantních informací v hlavičce [6].

Tradiční IP technika komprese hlaviček je stavová a obecně se zaměřuje na optimalizaci jednolitých paketů. Tyto metody předpokládají, že kompresor a dekompresor jsou v přímé cestě přenosu a kompresi síťové hlavičky na úrovni transportní vrstvy. Optimalizace probíhá určitý čas, během něhož se propouští postupně pakety, což vyžaduje, aby koncové body zpočátku posílaly nekomprimované pakety. Průtok paketů vychází z techniky komprese a je nevyhovující pro sítě LoWPAN. Komunikace vyžadující kompresi a dekompresi paketů při přenosu přes každý uzel sítě, má za následek nárůst hopů při přenosu informace. Mnoho směrovacích protokolů, využívaných v sítích LoWPAN, používá přijímání informací pomocí přesměrování v závislosti na předchozím stavu a kompresi. Oproti tomu sítě 6LoWPAN nevyžadují stejný způsob komprese a nechá směrovací protokoly zvolit trasu přenosu bez ovlivnění účinnosti komprese [6].

2.3.1 Zapouzdření formátu hlavičky

Protokol 6LoWPAN upravuje formát hlavičky pomocí síťového adresování, fragmentace a komprese hlaviček, jak je popsáno v následujících kapitolách. Síťová adresace se provádí na linkové vrstvě, fragmentace podporuje minimální velikost požadovaného MTU u IPv6. 6LoWPAN identifikuje všechny formáty hlavičky pomocí typů záhlaví pole, umístěného na začátku každého záhlaví. 6LoWPAN umožňuje koexistovat s jinými protokoly, které přímo operují v dané síti. Fragmentací je hlavička zmenšována na malé datagramy, což znamená, že je obsah rozdělen do více rámců. Velikost těchto rámců pak následně musí odpovídat maximální velikosti MTU sítě, v které jsou data přenášena. Podobně, je zmenšováno také Mesh záhlaví. V případě, že jsou pole zdrojové a cílové adresy shodná se záhlavím v linkové vrstvě, jsou 6LoWPAN rámce přenášeny během jediného hopu. Na Obr. 2.3 je vidět typické úprava formátu hlavičky [1], [6].



Obr. 2.3: Zapouzdření hlavičky adaptační vrstvou 6LoWPAN [6]

2.3.2 Fragmentace záhlaví

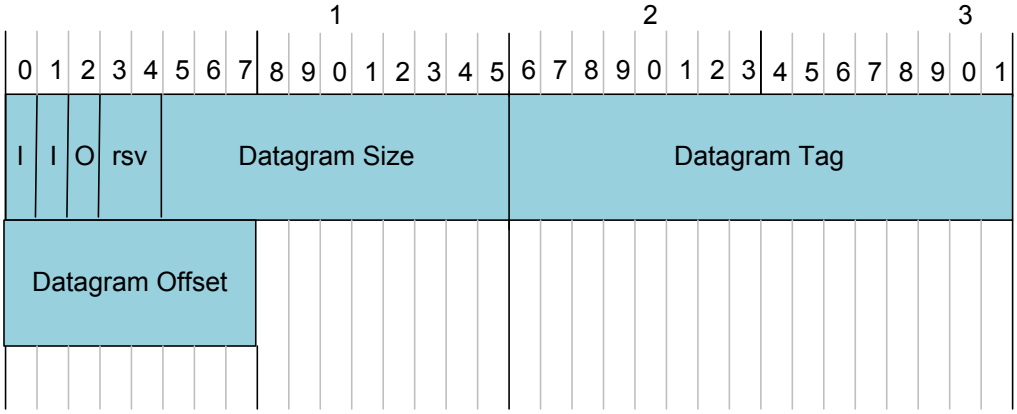
Fragmentace záhlaví se používá, když užitečný objem dat je tak velký, že se nevejde do jednoho IEEE 802.15.4 rámce. Fragmentace zahrnuje tři oblasti [6]:

- Datagram velikosti (Datagram Size) - určuje celkovou velikost nefragmentovaného užitečného objemu dat a je součástí každé fragmentace, kdy má za úkol zjednodušení přidělování vyrovnávací paměti na straně přijímače v okamžiku, kdy se fragmentace přeruší.

- Datagram označení (Datagram Tag) - ve fragmentovaných souborech identifikuje části nesoucí daný objem dat, a je používán k porovnání stejných obsahů užitečných dat.

- Datagram vyrovnání (Datagram Offset) - identifikuje fragmenty Offset (vyrovnává velikost posledního datagramu, aby odpovídala požadované velikosti MTU) uvnitř rámce s nefragmentovaným užitečným objemem dat a jeho velikost je 8 bitů [6]. Povolení libovolného bitu offset by vyžadovalo 11 bitů [6] pro podporu minimální velikosti MTU 1280 bajtů [6], ale 8 bajtové [6] vyrovnání vyžaduje pouze 8 bitů [6] pro Offset.

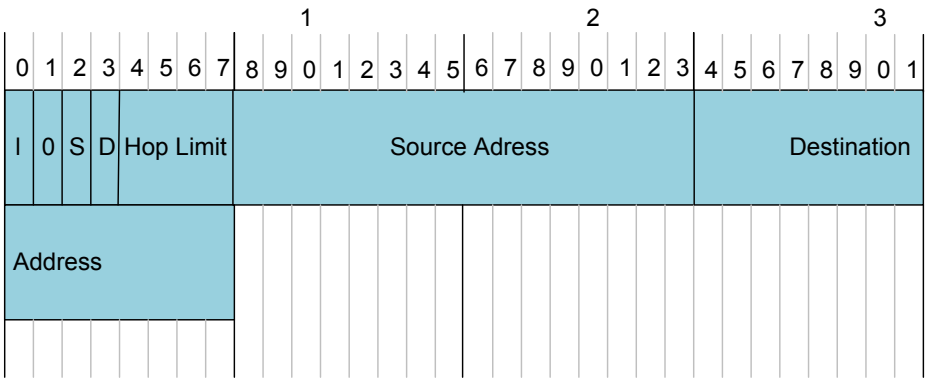
Formát fragmentovaného záhlaví je vyobrazen na Obr. 2.4 [6]. První dva bity určují typ záhlaví. Třetí bit určuje kompresi datagramu vyrovnání, první fragment je vždy na nule. Velikost záhlaví prvního fragmentu je 4 bity [6] a následujících fragmentů 5 bitů [6].



Obr. 2.4: Fragmentované záhlaví adaptační vrstvou 6LoWPAN [6]

2.3.3 Mesh záhlaví

Mesh záhlaví se používá pro předání dat přes druhou vrstvu. Skládá se z oblastí: Hop Limit (limit počtu hopů), Sourcess Address (zdrojová adresa) a Destination Address (cílová adresa). Pole Hop Limit omezuje počet hopů pro přesměrování. Pole je postupně zmenšováno každým spedičním uzle, a pokud se jeho hodnota dostane na nulu, je rámec vynechán. Zdrojové a cílové adresy jsou koncovými body hopu. Řešení Mesh záhlaví je zobrazeno na Obr. 2.5 [6].

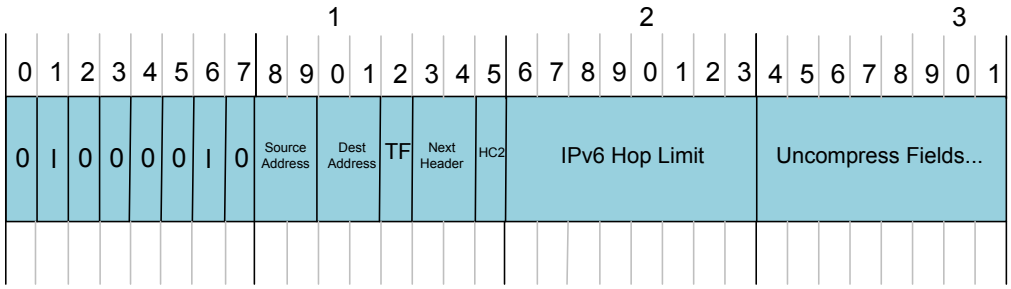


Obr. 2.5: Mesh záhlaví protokolu 6LoWPAN [6]

Typ záhlaví je zapsán pouze v prvních dvou bitech. Třetí a čtvrtý bit určují režim pro použití zdrojové a cílové adresy. Následující bity nesou pole Hop Limit a adresní pole. Velikost síťové adresovací hlavičky se pohybuje mezi 5 až 17bity [6], v závislosti na zvoleném způsobu adresování. [6]

2.3.4 Komprese záhlaví IPv6 dle RFC 4944

RFC 4944 definuje HC1, což je kompresní schéma optimalizované pro lokální komunikaci v sítích IPv6 [8]. Kompresní schéma HC1 je identifikováno v prvním odeslaném bajtu. 6LoWPAN v některých oblastech zmenšuje běžně používané hodnoty, např. v sítí komprimuje prefix (binární předpona) zdrojové a cílové adresy do jediného bitu [6]. Pokud se k přenosu paketu používá protokol UDP, TCP nebo ICMPv6, komprimuje 6LoWPAN pole hlavičky Next Header (udává, jaká data budou následovat za IP hlavičkou)do dvou bitů. Kromě toho také komprimuje Traffic Class (Třída Dat značí pole v hlavičce, ve kterém se specifikuje podle priority, které IP-datagramy je možné zahodit dříve než jiné) a Flow Label (Identifikace toku dat = spolu s adresou odesílatele jednoznačně identifikuje jeden dílčí tok dat v Internetu) do jediného bitu, pokud je jejich hodnota 0. 6LoWPAN redukuje ostatní oblasti, což je možné odvodit pomocí Payload Length (pole udávající celkovou délku datové části paketu) v 802.15.4 rámci, nebo v hlavičce fragmentovaného 6LoWPAN paketu. 64 bitový identifikátor IID (Interface Identifier) je zmenšen při odvození zdrojové a cílové adresy z adresy linkové vrstvy při komunikaci v síti standardu IEEE 802.15.4 nebo hlavičky síťové adresace. Aby 6LoWPAN mohl komunikovat, musí vždy komprimovat záhlaví IPv6 paketů [6] [8]. Na Obr. 2.6 [6] je vidět komprimovací schéma HC1.



Obr. 2.6: Komprese záhlaví IPv6 dle RFC 4944 v adaptační vrstvě 6LoWPAN [6]

První odeslaný bajt poukazuje na použití HC1 kódování. Po odeslání prvního bajtu určuje následující bajt tj. bitů, jak jsou komprimovány pole v hlavičce IPv6 paketu. Jeden bit označuje adresy v případě, že jejich prefix je komprimovaný, druhý bit se používá k označení v případě, že IID lze odvodit a adresy linkové vrstvy při komunikaci v síti standardu IEEE 802.15.4. Bit TF označuje, zda mají pole Traffic Class a Flow Label hodnotu 0 a jsou tedy komprimována. Další dva bity záhlaví uvádějí, zda je Next Header komprimované a jaký protokol se k přenosu používá (UDP, TCP IMCPv6), nebo jestli se data posílají v řadě za sebou. HC2 bit udává, jestli je následující záhlaví také komprimováno. Při plné komprimaci pomocí HC1

kódování je záhlaví IPv6 paketu zmenšeno na 3 bajty, včetně odeslání hlavičky [6] [8].

Adaptační vrstva 6LoWPAN má za úkol optimalizovat IPv6 pakety pro přenos v rámci standardu IEEE 802.15.4. Umožňuje podporu nezbytných součástí s ohledem na omezenou velikost MTU. Kromě přizpůsobení poskytuje adaptační vrstva 6LoWPAN dostatečně účinné mechanismy komprese hlaviček ke snížení režie IP hlavičky pouze na několik bitů, což je velmi podstatné právě pro sítě s přenosem rámců malých velikostí. [6] [8]

2.4 Implementace

Vývoj protokolu 6LoWPAN také směřuje k vývoji softwarových implementací pro snížení náročnosti softwaru. Snížení náročnosti implementovaného softwaru má za následek snížení požadavků na paměťovou kapacitu a v konečném důsledku snížení energetické náročnosti. Vývoj a implementace vhodného operačního systému, může výrazně prodloužit životnost jednotlivých senzorů v bezdrátových senzorových sítích (WSN). K nejpoužívanějším implementacím z hlediska vývoje, experimentů, ale i běžného provozu jsou operační systémy Contiki a TinyOS.

2.4.1 Contiki OS

Contiki je malý, účinný, implementovaný v jazyce C a tedy vysoce přenosný, víceúlohový operační systém, open-source software (software s otevřeným zdrojovým kódem), vyvinutý pro vestavěná zařízení, síťové systémy inteligentní objekty s omezenou pamětí. Je vyvíjen týmem akademických vývojářů, pod vedením Adama Dunkelse[1] a první verze byla spuštěna roku 2003. Contiki byl první operační systém vyvinutý pro inteligentní objekty, které pracují na principu IP komunikace pomocí TCP/IP stacků. Typická konfigurace Contiki spotřebuje 2KB paměti RAM a 40 KB paměti ROM [1]. Contiki také nabízí standardní funkce, jako je časovač, generátor náhodných čísel, hodiny, souborový systém a příkazový řádek shellu a navíc ještě sadu simulátorů, umožňujících simulaci při vývoji a experimentování s inteligentními objekty sítě. Contiki byl portovaný na více než dvanáct různých mikroprocesorů a mikrokontrolérů [1] [9].

V sítích fungujících na 6LoWPAN se od roku 2008 používá Contiki protokol μIPv6. μIPv6 je svazek protokolů pro sítě IPv6 využívající velmi krátký open-sourcový kód, umožňující komunikaci pomocí nejmenších IPv6 stacků. Díky tomuto řešení mohou i zařízení s omezenou kapacitou paměti získat IP adresu [1]. Tento

[1] Adam Dunkels autor knih, zabývajících se problematikou WSN

systém se využívá k např. v monitorování životního prostředí, automatizace budov, řízení energetických toků apod. S příchodem technologie μIPv6 a jeho nízkoenergetickému řídícímu mechanismu a minimálních nároků na paměťovou kapacitu můžou využívat IP platformu také zařízení, která dosud nemohla [1] [9].

Pro nízko-energetické sítě využívající 6LoWPAN byla vyvinuta implementace ContikiRPL, která používá nový směrovací protokol. Je velmi flexibilní při stavbě topologie sítě, což je velmi výhodné z hlediska metriky (počet hopů) [10].

2.4.2 TinyOS

Stejně jako Contiky je operační systém TinyOS open-source, využívá se pro inteligentní objekty a senzorové sítě. Byl původně vytvořen University of California v Berkeley, ale v současné době na jeho vývoji pracuje tým ze Stanford University. Původní operační systém TinyOS byl vytvořen v roce 2000. Je primárně používám pro výzkum a vývoj bezdrátových senzorových sítí WSN a má velkou uživatelskou podporu v akademické sféře. Vývoj TinyOS se zaměřuje na vytváření komunikačních mechanismů pro sítě WSN. TinyOS je implementován v programovacím jazyce nesC (dialekt jazyku C). Tento jazyk umožňuje statickou analýzu některých druhů chyb v časování, které lze tímto způsobem nalézt už během kompilace. TinyOS je portovaný na celou řadu systémů a prototypů desek.

Součástí TinyOS je také Blip Tutorial, který popisuje sestavení a konfiguraci podsítě využívající protokol 6LoWPAN. [1]

3 SPOTŘEBA ENERGIE V SÍTÍCH WSN

Spotřeba energie v bezdrátových senzorových sítích je dána spotřebou senzorových uzlů uvnitř sítě. Většinu energie spotřebovává hardware, proto se v nízkoenergetických systémech dosahuje největší úspory energie při návrhu senzorového uzlu. Spotřeba energie každého prvku WSN se skládá ze součtu spotřeb při provádění jednotlivých úkonů uvnitř uzlu [11]:

- Sbírání dat – u sběru dat záleží na typu senzoru, na veličině, která má být snímána a na způsobu jejího snímání. Senzory musí být nejprve aktivovány pro snímání a pro sběr dat z okolního prostředí. Různé typy senzorů spotřebovávají různé množství energie.

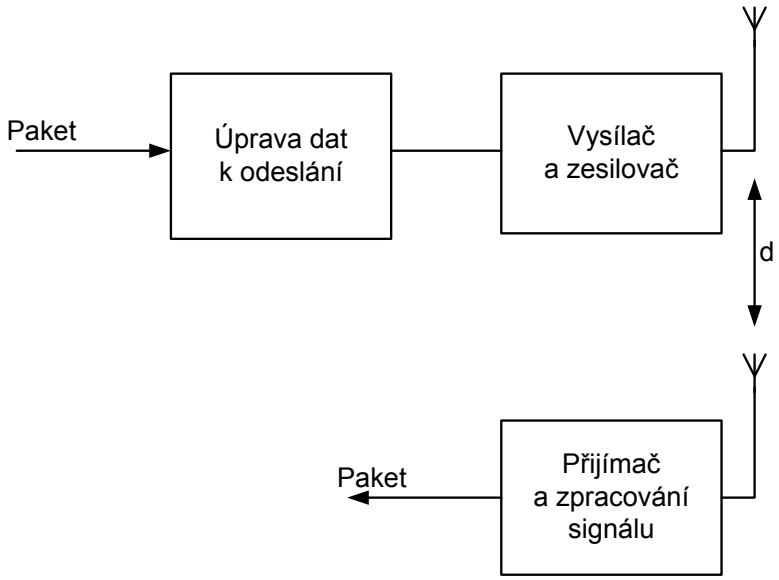
- Komunikace – spotřeba senzorového uzlu v bezdrátové senzorové síti při komunikaci se skládá ze spotřeby při přijímání paketů (R_x power) a při odesílání paketů (T_x power). Velkou roli zde hraje maximální dosah přijímací a vysílací části.

- Výpočetní úkony – spotřeba při výpočetních úkonech se odvíjí od spotřeby výpočetního bloku, tedy od mikrokontroléru, obsahujícího mikroprocesor, paměti, A/D převodník. Výpočetní blok pracuje při každé činnosti, kterou uzel provádí, zejména pak při sběru dat a jejich následném zpracování.

Spotřeba energie bezdrátových senzorových sítí závisí na spotřebě při jednotlivých činnostech senzorového uzlu. Největší spotřebu uzel zaznamenává při komunikaci, tedy při přijímání a odesílání nasbíraných dat. Na rozdíl od komunikace je energetická náročnost výpočetního bloku, který pracuje při každém úkonu, jenž uzel provádí, výrazně nižší. Spotřeba energie se řeší především na fyzické a linkové vrstvě [11].

3.1 Spotřeba energie komunikačního bloku

Spotřeba energie rádiového přenosu se skládá ze spotřeby obvodů, zajišťující samotný bezdrátový přenos a obvodů, které zpracovávají a upravují data pro jejich transport. Na Obr. 3.1 je blokové schéma komunikačních obvodů.



Obr. 3.1: Blokové schéma komunikačních obvodů [11]

3.1.1 Spotřeba energie přijímací části

Spotřeba energie přijímací části závisí na na spotřebě obvodů pro zpracování přijímaného signálu a na počtu přijímaných bitů. Energetická náročnost přijímací části se pak vypočítá: [11]

$$E_{rx} = E_d \cdot n, \qquad [\mathrm{J}] \tag{3.1}$$

kde $\mathrm{E_{rx}}$ je energie pro příjem paketu o n bitech a $\mathrm{E_d}$ spotřeba obvodů pro zpracování signálu na 1 bit.

3.1.2 Spotřeba energie vysílací části

Spotřebu energie vysílací části ovlivňuje hned několik faktorů – velikost odesílaného paketu, vzájemná vzdálenost komunikujících uzlů, použitá modulace a na vysílacím výkonu zesilovače. Energetická náročnost vysílací části se vypočítá: [11]

$$E_{tx} = E_m \cdot n + E_z \cdot n \cdot d^2, \qquad [\mathrm{J}] \tag{3.2}$$

kde $\mathrm{E_{tx}}$ je spotřebovaná energie při vysíláni paketu o n bitech na vzdálenost d metrů, $\mathrm{E_m}$ je energie spotřebovaná při modulaci jednoho bitu a $\mathrm{E_z}$ je energie spotřebovaná zesilovačem.

Energetickou náročnost senzorových uzlů mohou výrazně ovlivnit elektronické obvody a součástí, ze kterých se uzel skládá. Při návrhu bezdrátových senzorových

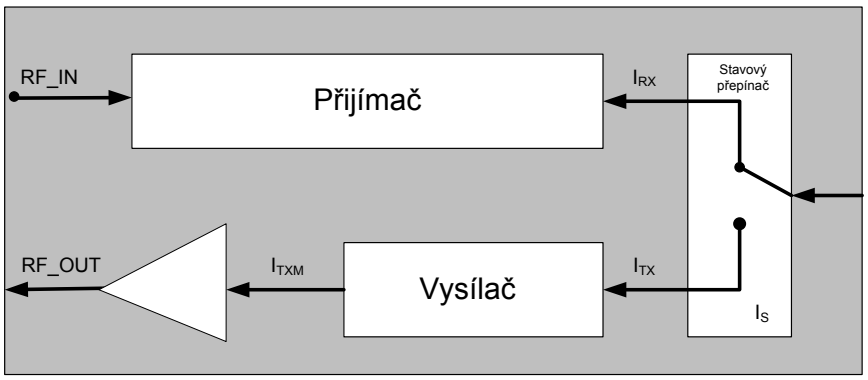
sítí, je proto nutné dbát během výběru zařízení na některé parametry – spotřeba mikrokontroléru s mikroprocesorem, spotřeba uzlu v aktivním režimu a v režimu spánku (uzel v něm tráví většinu času), energetická náročnost při vysílání a přijímání, apod. Energetickou náročnost lze také ovlivnit snížením vysílacího výkonu (omezení maximálního možného dosahu), způsobem přenosu, výběrem směrovacího protokolu a protokolu pro přenos dat .

4 SNÍŽENÍ SPOTŘEBY ENERGIE V SÍTÍCH WSN

Znalost aplikační domény spolu s funkcí fyzické vrstvy hardwaru sítě je klíčem k návrhu systému s nízkou energetickou náročností pro bezdrátové senzorové sítě WSN. Základ realizace takového systému je vybrání vhodné topologie WSN a komunikačních protokolů. Bylo již vytvořeno spoustu systémů, které se zabývají nízkoenergetickou problematikou (např. ZigBee, 6LoWPAN atd.) lišící se právě topologií a výběr různých komunikačních protokolů. Tato kapitola je věnována právě protokolu 6LoWPAN [12].

4.1 Snížení spotřeby energie z hlediska fyzické vrstvy

Snížení spotřeby energie v sítích WSN z hlediska fyzické vrstvy je řešeno především použitím vhodného způsobu čerpání energie při napájení senzorových uzlů. Jako napájecí zdroj se v bezdrátových senzorových sítích většinou používají bateriové články. Velký význam v úspoře energie zde má schéma napájení, které se skládá z několika módů provozu – přenos, příjem a spánek. Na Obr. 4.1 [7] je znázorněno blokové schéma napájení typického transceiveru (vysílač s přijímačem) [12].



Obr. 4.1: Blokové schéma napájení transceiveru [12]

Proud I_{TX} je celkový proud odebíraný, když je vysílač aktivní (režim vysílání). Proud I_{RX} je proud odebíraný transceiverem, ve stavu kdy přijímač je aktivní (režim příjmu). Proud I_S je odebíraný proud v režimu spánku = přijímací ani vysílací část není aktivní [12].

4.1.1 Druhy baterií

Hlavním napájecím zdrojem senzorů v bezdrátových senzorových sítích jsou baterie. V dnešní době je obrovské množství technologií a použitých materiálů při výrobě bateriových článků, což má za následek vznik velkého množství typů baterií. V sítích WSN se využívají pro senzory tyto typy baterií [13] [14] [15]:

a) Alkalické akumulátory

Alkalické akumulátory jsou již zastaralou technologií. Nahradili je modernější niklové a lithiové napájecí zdroje s možností opakovaného nabití. Oproti ostatním technologiím se vyznačují vysokým jmenovitým napětím a zanedbatelnou hodnotou samovybíjení [13] [14].

b) Niklové

- **Baterie Ni-Cd (Nikl-Kadmiové)** – tyto články se vyznačují dobrým výkonem v prostředí, které vyžaduje větší odběr proudu, nebo v prostředí s nízkou teplotou. Mají dlouhou životnost a při vhodném uchovávání dochází k velmi pomalému vybíjení, takže mají dlouhou výdrž. Ve srovnání s bateriemi Ni-Mh mají delší životnost a při uchovávání vydrží déle [15] [16].

- **Baterie Ni-Mh (Nikl-Metal-Hydridové)** – patří k novější generaci oproti bateriím Ni-Cd a v současné době se staly nejpopulárnějším typem bateriových článků na našem trhu, především díky rozvoji digitálních přístrojů a mp3/mp4 přehrávačů. Oproti staršímu typu Ni-Cd se vyznačují rychlejším samovybíjením a kratší životností, na druhou stranu dosahují o cca 30 % vyšší kapacity [15]. Charakterizují se také větší hustotou energie (teoretická hodnota až 50 %, [15] reálná hodnota cca 25 %) [15] a výhodnější cenou. Kvůli vlivu paměťového efektu, který zkracuje životnost baterií, je nabíjení těchto akumulátorů možné až po jejich úplném vybití [15].

- **Baterie Ni-Mh nové generace** – u těchto Ni-Mh článků byla použita zdokonalená technologie při jejich výrobě, která umožnila zminimalizování efektu samovybíjení. Výsledkem jsou univerzální baterie, jež mohou úspěšně nahrazovat alkalické baterie a jsou okamžitě připravené k užívání (nemusí se hned nabíjet) [15].

Paměťový efekt je jev, vznikající opětovným dobíjením neúplně vybité baterie. Při opakovaném vybíjení (řádově desítky až stovky cyklů) článků na např. pouze

50 % [17] jejich kapacity dochází k postupnému snižování jejich kapacity. V podstatě si jakoby „pamatovaly“ kolik kapacity jim stačí, k jejich vytížení a následkem toho postupně ztrácí schopnost udržet původní množství energie a jejich kapacita se výrazně zmenšuje až k úplnému znehodnocení baterie. Paměťový efekt se projevuje hlavně u Ni-Cd článků, u typu Ni-Mh má vliv jen částečně [17].

c) Lithiové

- **Baterie Li-Ion (Lithium-Iontové)** – nabíjecí baterie běžně využívaná ve spotřebitelské elektronice. Vyznačuje se až 3x větší kapacitou než baterie niklové a velmi nízkou hodnotou samovybíjení. Na rozdíl od baterií typu Ni-Cd nebo Ni-Mh má vysoké nominální napětí až 3,6 V [15]. Lithiové články mají vyšší životnost, ovšem jsou výrazně citlivé na pokles napětí pod minimální hodnotu (okolo 2,8 V) [15]. Baterie Li-Ion lze kdykoliv dobíjet, není u nich vliv paměťového efektu, ale jsou výrazně dražší oproti bateriím niklovým [13] [15].

- **Baterie Li-Pol (Lithium-Polymerové)** – jsou to nejnovější typy akumulátorů a mají podobné vlastnosti jako baterie Li-Ion. Používají se v mobilních telefonech, kamerách, fotoaparátech, noteboocích a dalších přenosných zařízení. Technologie Li-Pol článků byla vyvinuta z technologie Li-Ion. Stejně jako baterie Lithium-Iontové mají jmenovité napětí jedno článku 3,6 V [15]. Jejich výhodou je malá hmotnost, vysoká kapacita, velká výkonnost a velmi malé samovybíjení. Díky svým vlastnostem se stále více rozšiřují, jsou neustále vyvíjeny, přičemž je zvyšována jejich kapacita a výkonnost. Nevýhodou u těchto akumulátorů je nutnost používání elektronické ochrany jednotlivých článků při nabíjení a vybíjení. Při jejich vybíjení a nabíjení nesmí být překročeny hodnoty stanovené výrobcem, v opačném případě může dojít k poškození článků. Další jejich nevýhodou je jejich citlivost na mechanické poškození. V budoucnu by technologie Li-Pol baterií měla nahradit, dnes již starší niklové baterie a také Li-Ion akumulátory [13] [15].

Porovnání parametrů jednotlivých typů baterií používaných ve WSN je v Tab. 4.1.

Tab. 4.1: Porovnání typu baterií používaných v sítích WSN [14]

Parametr	Typ baterie				
	Alkalické baterie	Ni-Cd	Ni-Mh	Li-Ion	Li-Pol
Jmenovité napětí [V]	1,5	1,2	1,2	3,6	3,6
Kapacita [mAh]	až 2400	500 – 800	1500 – 3200	800 – 5000	800 – 5000
Trvanlivost [počet cyklů]	1	200 – 500	200 – 500	500 – 1000	500 – 1000
Paměťový efekt	NE	ANO	minimální	NE	NE
Samovybíjení/ měsíc	$< 10\,\%$	30 %	30 %	10 %	10 %
Doba rychlo--nabíjení [hod]	–	2 – 4	2 – 4	2 – 4	2 – 4
Min. hodnota napětí/článek	–	0,8	0,8	2,8	2,8
Tolerance přebíjení	–	nízká	nízká	velmi nízká	nízká
Okamžitě použitelné	ANO	NE	NE	ANO	ANO
Poznámka: mAh (miliampérhodina) = jednotka udávající kapacitu článků					

Základem pro snížení spotřeby energie z hlediska fyzické vrstvy je zvolení vhodného způsobu čerpání energie senzorového uzlu z akumulátorů, kdy se používá nelineární vybíjecí charakteristika. Vybíjení tedy není konstantní, ale uzel čerpá energii po impulsech. Důležité je také správně zvolené napájecí schéma s napěťovým regulátorem (přepínaný regulátor nebo lineární regulátor). Napájecí schéma se skládá z několika módů, které v případě neaktivního vysílače nebo přijímače sníží pomocí napěťového regulátoru odběr senzoru na minimum. U zdroje napájení je velmi důležité co nejmenší procento samovybíjení. Jelikož žádný z akumulátorů nevydrží požadovanou dobu, skládají se zdroje s použitím více článků, kdy je např. senzorový uzel napájen nejdříve nějakou dobu (pár ms) z prvního článku, poté přejde na

napájení z článku druhého apod.

Jako alternativní zdroje energie slouží zdroje z okolního prostředí. Mezi nejpoužívanější patří využívání solární energie a energie vibračních dějů. Solární energie se čerpá pomocí solárního panelu, který se skládá ze solárních buněk na křemíkové bázi zapojených do série.

Všechny tyto aspekty se podílí na celkovém snížení spotřeby energie a jsou předmětem budoucí snahy o jejich vývoj a vylepšení.

4.2 Snížení spotřeby energie z hlediska linkové vrstvy

Energetická účinnost, je základním tématem při vývoji komunikačních protokolů, směrování a protokolů MAC vrstvy pro bezdrátové senzorové sítě WSN. Jedním z primárních mechanismů pro dosažení nízké energetické náročnosti v oblasti energetiky jsou protokoly se synchronizovaným nebo asynchronním nízko-výkonovým režimem. Každý senzorový uzel může být buď v aktivním stavu, nebo ve stavu spánku. Klíčovým parametrem charakterizující jednotlivé stavy je doba spánku, čas probuzení a energie spotřebovaná během aktivního stavu a stavu spánku. Vzhledem k regulaci odběru proudu, řeší vývojáři komunikačních protokolů pro sítě WSN, jak dosáhnout vysoké propustnosti a zároveň nízkého zpoždění a co nejmenší energetické náročnosti ve stavu bdění a spánku senzorů. Řešení poskytuje vhodné zvolení typu MAC protokolu.

4.2.1 Režim spánku

Režim spánku, neboli sleeping mode, je režim snížené spotřeby. Senzorový uzel přejde z aktivního stavu do stavu spánku, během kterého nevysílá ani nepřijímá žádné pakety. Z režimu spánku se senzorový uzel probudí do aktivního režimu vždy po nějaké době, odešle a přijme data a zase usne. Celý proces se periodicky opakuje. Uzel v režimu spánku stráví 99 % času [18]. Režim spánku je základní nástroj pro snížení spotřeby energie. V Tab. 4.2 je uvedena spotřeba jednotlivých částí senzorového uzlu. [18]

Tab. 4.2: Spotřeba jednotlivých částí senzorového uzlu [18]

Součásti senzorového uzlu	Spotřeba energie $[mW]$	Povolená činnost [%]
Komunikační modul (příjem)	50 – 100	0,1 – 1
Komunikační modul (odesílání)	25 – 50	0,1 – 1
MCU	1 – 5	1 – 5
Senzory	0,5 – 10	0,01 – 1
Všechny součásti v režimu spánku	5 – 100 μ	100

Způsoby režimu spánku

- **RFID (Radio Frequency Identification) impulzy** – pracují na principu identifikace doby přechodu do aktivního režimu přes rádiovou frekvenci. V režimu spánku mají všechny uzly vypnutý komunikační modul, regulátor napětí,oscilátor a také MCU přechází do stavu nečinnosti. Když chce nějaký uzel vysílat data jinému uzlu musí nejdříve vygenerovat RFID tag, který pošle do vzdálené správy WSN sítě. Ta probudí jednotku MCU cílového uzlu a během pár ms aktivuje jeho komunikační modul, regulátor napětí i oscilátor. Pokud probuzení proběhlo v pořádku vyšle cílový uzel zpět k vysílajícímu uzlu zprávu, že je již připraven a může začít vysílání. Po skončení přenosu přejdou opět všechny části uzlu do spánkového režimu. V případě že vysílající uzel neobdrží potvrzovací zprávu, předpokládá se, že probuzení proběhlo neúspěšně a vyšle další RFID tag. Maximální počet pokusů o probuzení jsou tři. [19]

- **Predikce (odhad trajektorie přenosu)** – metoda je založená na odhadu cíle a trajektorie přenosu vedoucí právě k tomuto cíli pomocí matematického algoritmu. Základní myšlenka predikce je, že se pomocí algoritmu předpoví uzel, který bude v budoucnu tvořit hranici monitorované oblasti. To umožňuje všem uzlům v síti zůstat v režimu spánku, v aktivním stavu jsou pouze uzly tvořící hranici. Tato metoda se využívá v sítích, které monitorují území o velké rozloze s neustále se pohybující hranicí, kterou tvoří sousedící senzorové uzly. Všechny uzly jsou tedy ve stavu spánku a probouzejí se jen ty uzly,

které budou tvořit hraniční linii. Metoda predikce definuje 5 možných stavů senzorového uzlu [20]:

Bílý režim spánku – uzel zůstává ve stavu spánku. Čidlo udržuje klidový režim a pravidelně se probouzí, aby zjistilo zda v dosahu není cílový uzel (predikcí vybraný uzel, který tvoří hranici).

Bílý aktivní režim – snímač uzlu je v aktivním režimu a sleduje pohyb predikovaných cílů. Při zjištění cílového uzlu v okolí, přechází celý uzel do aktivního režimu.

Režim aktivního testování – do tohoto stavu se dostává uzel z bílého nebo černého aktivního režimu, když zjistí možný cílový uzel v okolí. Uzel v tomto režimu vybere další senzorový uzel, se kterým bude tvořit hranici a také předpoví budoucí podobu hranice pro aktivaci spících uzlů.

Černý režim spánku – do toho stavu režimu přechází uzel v případě, že je detekován jako budoucí cílový uzel. V režimu spánku zůstává dokud není hranice pro snímání blízko, poté přejde do aktivního stavu.

Černý aktivní režim – uzel je v tomto stavu, když již informoval další uzel, že bude budoucím cílovým uzlem. Uzel poté přejde do režimu aktivního testování a nakonec do bílého režimu spánku.

Využití metod režimu spánku

Pro jednotlivé aplikace je lepší jiný princip režimu spánku viz Tab. 4.3.

Tab. 4.3: Přehled metod režimu spánku a jejich využití [19] [20]

Princip režimu spánku	Využití
RFID impulzy	monitorování kvality vody měření teploty, tlaku, monitorování dopravy, sledování zdravotního stavu, zabezpečovací systémy, atd.
Predikce	území o veliké rozloze s pohyblivými hranicemi např. lesní požáry, chemické katastrofy, ropné skvrny, atd.

4.2.2 MAC protokoly

S vývojem bezdrátových senzorových sítí jsou neustále vyvíjeny také MAC protokoly linkové vrstvy. MAC protokoly se mohou dělit na protokoly se soupeřením a protokoly bez soupeření. Podle soupeření protokolu soutěží uzly o přenos přes sdílený kanál, přičemž se snaží vyhnout kolizím rámců. Tyto protokoly často vychází ze skoro zapomenutého protokolu ALOHA nebo z metody CSMA/CA [18].

Protokol ALOHA snižuje počet kolizí rozdělením času do slotů a předáváním dat pouze mezi těmito sloty. Metoda CSMA/CA je modifikací metody CSMA, která dále snižuje počet kolizí tím, že zlepšuje dosažitelnou propustnost kanálu. Propust kanálu zlepšuje kontrolní činností před začátkem přenosu a zabraňuje stanici, aby začala vysílat, pokud je médium již obsazené. Metoda CSMA/CA navíc při přetížení kanálu odloží přenos na náhodně zvolený interval a poté opět zkontroluje médium, zda je již volné k přenosu. Přesto však může dojít k problému v důsledku skryté kolize – uzly odděleny dvěma hopy se nemusí navzájem detekovat a jejich přenosy se mohou setkat ve stejném okamžiku na přijímačích jejich dílčích uzlů. Vícenásobný přístup s vyhýbáním kolizí MACA (Multiple Access with Collision Avoidance) snižuje hrozbu skryté kolize uzlů, posláním požadavku RTS (Request to Send) a CTS (Clear to Send), před přenosem dat. Tato domluva je také definována jako možnost metody CSMA/CA. Zatímco protokoly se soupeřením pracují dobře při nízkém přenosovém zatížení, jejich výkon a spolehlivost výrazně klesá při vyšším zatížení, protože narůstá počet kolizí a v jeho důsledku také počet opakovaný přenosů [18].

Protokoly bez soupeření jsou v podstatě metody vícenásobného přístupu v sítích WLAN. Pomocí časového multiplexu TDMA (Time Division Multiple Access), frekvenčního multiplexu FDMA (Frequency Division Multiple Access) a datového multiplexu CDMA (Code Division Multiple Access) rozdělují pásmo mezi jednotlivé uzly v síti. Nejčastěji se pracuje s časovým multiplexem, ale některé systémy využívají i kombinace frekvenčního a časového multiplexu (počet kanálů je ale vždy omezen) [18].

TDMA rozdělí čas do mnoha slotů a vždy pouze jeden uzel má povoleno předávat data ze slotu na slot. FDMA poskytují protokolům bez soupeření samostatné frekvenční kanály a CDMA šíření kódů [18].

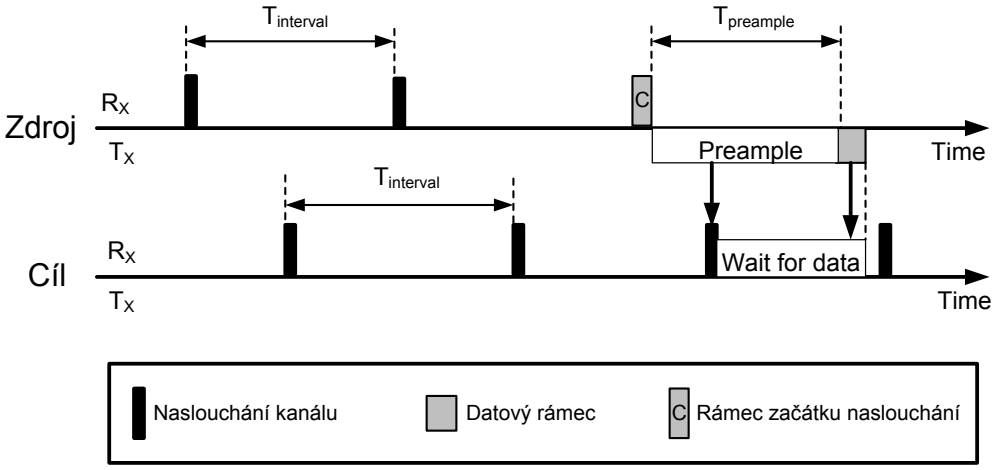
Protokoly bez soupeření dosahují vysokého výkonu a spolehlivosti bez ohledu na zatížení. Přesto by se měla šířka pásma předem rezervovat, což ale zvyšuje režijní náklady na řízení provozu [18].

Vzhledem ke spotřebě proudu nízko-výkonových senzorových uzlů v pohotovostním režimu, není energetická účinnost běžných MAC přístupů dostačující pro nízko-energetické sítě WSN. Další úspory energie lze dosáhnout použitím nízkovýkonového režimu, kdy čas je rozdělen na krátkou aktivní dobu a dlouho dobu

spánku, které se střídají. Podle těchto nízko-výkonových režimů se MAC protokoly dělí na asynchronní a synchronizované protokoly, v závislosti na synchronizaci výměny dat [18].

a) MAC protokoly s asynchronním pracovním cyklem

MAC protokoly s asynchronním pracovním (Unsynchronized low duty-cycle MAC protocols) jsou založeny na mechanismu nízko-energetického poslechu LPL (Low Power Listening), kde uzly dělají asynchronní test na volnost kanálu pro přenos viz Obr. 4.2 [18]. Přenosům předchází preambule ($T_{preample}$), která je delší než doba zjišťování volnosti kanálu ($T_{interval}$). Proto preambule funguje jako budící signál, který převede uzly z režimu spánku do aktivního režimu. Po převedení do aktivního režimu musí zdrojový uzel začít posílat data dříve, než bude kanál obsazen [18].



Obr. 4.2: Procesy MAC protokolu s asynchronním pracovním cyklem [18]

Typy MAC protokolů s asynchronním pracovním cyklem:

- **B-MAC (Berkeley-MAC) protokol** – protokol byl vypracován University of Berkeley. Jedná se o jednoduchý LPL (Low Power Listening) protokol využívající metodu CSMA/CA. Když chce uzel zahájit přenos dat, musí nejdříve poslat paket s delším záhlavím pro přechod cílového uzlu z režimu spánku do aktivního režimu. Dlouhá preambule má za následek snížení energetické účinnosti. Kromě toho energetickou účinnost snižuje detekce rámců určených jiným uzlům a časté naslouchaní kanálu, aniž by uzel přenášel data. B-MAC má dobrou schopnost adaptace na měnící se přenosové podmínky [18].

- **Z-MAC protokol** – protokol Z-MAC operuje nad B-MAC, ale na rozdíl od něj využívá pro řízení přetížení multiplex TDMA. Každý uzel má vlastní slot, což má za následek snížení soupeření mezi uzly. Při nízkém soupeření se Z-MAC chová jako CSMA a při vysokém soupeření více jako TDMA. Využití slotů zvyšuje propustnost protokolu B-MAC. Přesto je zlepšení v oblasti energetické účinnosti omezené [18].

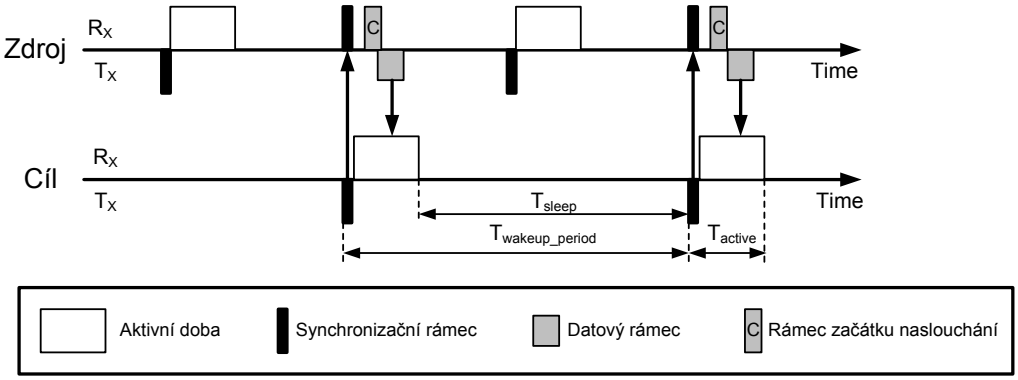
- **X-MAC protokol** – tento protokol navrhuje nové možnosti nízko-energetického naslouchaní. Využívá krátké preambule k dalšímu snížení spotřeby energie a ke snížení latence. První myšlenka byla vložení informace o cílové adrese, tak že přijímače, kterým nejsou data adresována, se mohou rychle vrátit do režimu spánku. Další možností, kterou protokol X-MAC přinesl je použití bleskového signálu, který umožní cílovému přijímači v případě, že zjistí, že je cílový přijímač, přerušení dlouhé preambule a to má za následek snížení doby a potřebné energie než se cílový přijímač probudí a je schopen přenosu. Protokol X-MAC obsahuje také automatizovaný algoritmus pro přizpůsobení pracovního cyklu uzlů tak, aby co nejlépe zvládaly přenosovou zátěž v síti [18] [21].

- **Protokol WiseMAC** – používá podobnou techniku jako protokol B-MAC s tím rozdílem, že zdrojový uzel určuje cílového uzlu, kdy má být v aktivním režimu a kdy v režimu spánku. K dosažení těchto záměrů posílají vysílače spolu s daty potvrzení. Při příštím přenosu tomuto přijímači, bude trvat jen krátký čas, než bude schopen přijímat data. Tím se snižuje energie potřebná k vyslání preambule. Při nízkém přenosovém zatížení je preambule delší než datový rámec. Přijímače zpracují datový rámec, a pokud nejsou určeny, jako příjemce vrátí se do režimu spánku. Pokud jsou příjemcem, zůstávají vzhůru až do konce přenosu a pošlou potvrzeni. Zatímco WiseMAC řeší mnoho věcí spojených s nízkou spotřebou při komunikaci, neposkytuje žádný mechanismus, který by přizpůsoboval uzly měnícímu se charakteru provozu [21].

Asynchronní protokoly jsou poměrně jednoduché a vyžadují malé množství paměti v porovnání se synchronizovanými protokoly. Nevýhodou je ovšem poměrně časté naslouchání kanálu bez další činnosti (přenos dat) předtím, než dostane uzel rámec pro uskutečnění přenosu dat. Asynchronní protokoly jsou vhodné pro bezdrátové senzorové sítě WSN s malými přenosovými rychlostmi. Umějí se přizpůsobit dynamickým podmínkám přenosu v síti, ale jejich energetické účinnost je omezena právě častým naslouchaním kanálu [18].

b) MAC protokoly se synchronizovaným pracovním cyklem

MAC protokoly se synchronizovaným pracovním cyklem (Synchronized low duty-cycle MAC protocols) využívají plánování stavu vysílačů a přijímačů, tak aby jim zajistili pravidelný přechod do aktivního režimu (T_{activ} – doba aktivního režimu), během kterého můžou přenášet data. Z aktivního režimu přecházejí senzorové uzly do režimu spánku (T_{sleep}), umožňující úsporu energie. Aktivní režim a režim spánku se opakují v pravidelných intervalech (T_{wakeup_period}), jak je znázorněno na Obr. 4.3 [18].



Obr. 4.3: Procesy MAC protokolu se synch. pracovním cyklem [18]

Doba aktivního stavu označována jako superrámec (superframe) je doba, kdy senzorový uzel vysílá jako první synchronizační rámec (beacon) pro signalizaci a zjištění stavu ostatních uzlů, a poté poslouchá až do konce doby aktivního režimu dění na kanálu pro možný přenos dat. Vzhledem k vzájemné synchronizaci režimů znají senzorové uzly předem dobu, po kterou budou aktivní, a tím se eliminuje potřeba dlouhé preambule. V rozsáhlých sítích je globální synchronizace režimů velmi obtížná, a proto se synchronizují senzorové uzly pouze lokálně se sousedními uzly [18]. Pro navázání synchronizace musí nejdříve uzly prohledat síť a najít sousední senzorové uzly. Hledání sousedních uzlů znamená dlouhodobý příjem frekvenčních kanálů pro příjem beacon rámců. Proces hledání je energeticky náročný, ale v konečném důsledku je synchronizace uzlů energeticky velmi výhodná [18].

V současné době je několik druhů MAC protokolů se synchronizovaným nízkovýkonovým režimem [18]:

- **S-MAC (Sensor-MAC) protokol** – je jedním z prvních MAC protokolů se synchronizovaným nízko-výkonovým režimem. Protokol využívá pevnou dobu

aktivního režimu a nastavitelnou dobu probuzení. Po probuzení uzlu a přechodu do aktivního režimu si uzly nejdříve vymění Synchronizační (SYNC) rámec. Poté uzel, který bude chtít přenášet data, vyšle požadavek RTS pro uskutečnění přenosu pomocí přístupové metody CSMA/CA. Cílový uzel podle přijaté zprávy vybere požadovaný uzel a odešle mu potvrzení o poskytnutí vyhrazeného pásma – zpráva CTS. Po té zdrojový uzel může začít přenášet data až do konce doby aktivního režimu. Bezchybně přijatá data jsou potvrzována ACK rámci. Energetická účinnost S-MAC protokolu se snižuje o proces synchronizace a posílání požadavku RTS, navíc délka doby aktivního režimu má za následek, že uzel po tuto dobu zbytečná naslouchá, i když nedochází k přenosu dat. Dalším problémem S-MAC protokolu je špatné přizpůsobení měnícím se přenosovým podmínkám [18] [21].

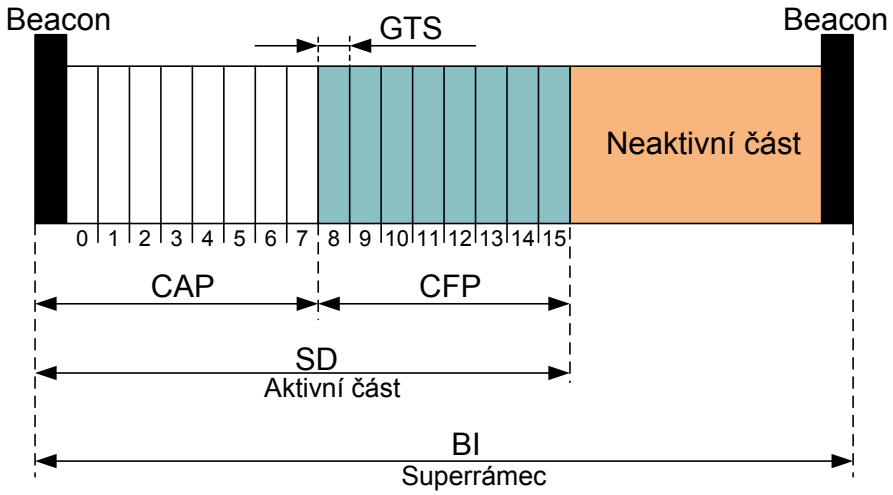
- **T-MAC (Timeout-MAC) protokol** – protokol T-MAC je v podstatě rozšíření protokolu S-MAC o zkrácení aktivního režimu, pokud je kanál nečinný. V S-MAC můžou uzly zůstat v aktivním režimu, i když neodesílají ani nepřijímají data. T-MAC poslouchá kanál jen po krátký čas, během něhož se synchronizuje a pokud nepřijme žádná data, přejde do režimu spánku. Pokud data obdrží, zůstane v aktivním režimu, do doby než jsou všechna data poslána a poté aktivní režim skončí. Pro proměnné zatížení využije T-MAC pouze jednu pětinu spotřebované energie protokolem S-MAC. Nevýhodou stejně jako u S-MAC je snížení energetické účinnosti o proces synchronizace a posílání požadavku RTS, ovšem doba zbytečného naslouchání je zde výrazně kratší než u protokolu S-MAC [18] [21].

- **D-MAC protokol** – je to varianta protokolu S-MAC měnící režimy uzlů aktivní/spánek stromové topologie. To umožňuje nízkou latenci přenosu paketů od vysílače zdrojového uzlu do přijímače cílového uzlu. Obsahuje mechanismy, oznamující uzlům, která data byla upravena a přizpůsobena pro nízko-výkonový režim [18].

Důležitou součástí MAC vrstvy standardu 802.15.4 je její podvrstva. Tato podvrstva řídí správu synchronizačních rámců Beacon, přístup ke kanálům, ověřuje platnost rámců, spravuje garantované časové úseky GTS (Guarenteed Time Slots), potvrzuje bezchybně přijatá data pomocí ACK paketů, spojuje a rozpojuje uzly. Obsahuje různé typy MAC protokolů podporující dva provozní režimy, které určuje PAN koordinátor [3] [18]:

- **Beacon-enabled mode (v synchronizačním režimu)** – signální rámce (beacon frames) periodicky generuje PAN koordinátor pro identifikaci sítě PAN, ve které se nachází. Pro synchronizaci uzlů ve své skupině a charak-

terizování superrámce (superframe) viz Obr. 4.4 [22]. Režimu Beacon-enabled dosáhne PAN koordinátor použití superrámce, který řídí komunikaci mezi uzly v sítích PAN. Když si PAN koordinátor vybere Beacon-enabled mode, docílí tím použití superrámce, který pak ovládá komunikaci mezi zařízeními, které patří do PAN. PAN koordinátor staví formát superrámce, který odpovídá signalizačnímu intervalu BI (Beacon Interval). Interval BI je definovaný časem mezi následnými signály a obsahuje aktivní periodu, jež může být následována periodou neaktivní. Aktivní perioda odpovídá délce superrámce SD (Superframe Duration) a je rozdělena na 16 shodných slotů, přes které se přenášejí data. V neaktivní periodě přechází uzel do režimu spánku. Každá aktivní perioda může být dále rozdělena na dobu soupeření o přístup CAP (Contention Access Period) a na dobu volného přístupu CFP (Contention Free Period). Doba soupeření o přístup funguje na základě přístupové metody CSMA/CA, doba volného přístupu se aktivuje u cílového uzlu poté, co zdrojový uzel požádá o jeho aktivaci PAN koordinátor. PAN koordinátor po přijetí žádosti o aktivaci zkontroluje, zda jsou dostatečné zdroje pro přenos a pokud je vše v pořádku, přidělí žádosti časový slot [22].



Obr. 4.4: Struktura superrámce [22]

- **Non Beacon-enabled mode (v asynchronním režimu)** – uzel může jednoduše posílat svá data prostřednictvím přístupové metody CSMA/CA. Režim Non Beacon-enabled nevyužívá superrámcovou strukturu. Jeho výhodou je snadná rozšiřitelnost a samo-organizace, na druhou stranu nemůže poskytnout službu GTS [22].

Na rozdíl od protokolů s asynchronním pracovním cyklem odpadá u protokolů se synchronizovaným pracovním cyklem doba, ve které je uzel aktivní, ale pouze naslouchá, aniž by přenášel data. Jsou tedy energeticky méně náročné. Jejich nevýhodou je požadovaná vetší velikost paměti oproti protokolům s asynchronním pracovním cyklem.

V Tab. 4.4 je srovnání synchronních a asynchronních MAC protokolů.

Tab. 4.4: Tabulka srovnání MAC protokolů pro sítě WSN [14]

	Asynchronní protokoly			
	B-MAC	Z-MAC	X-MAC	Protokol WiseMAC
Topologie	Mesh	Mesh	Mesh	Hvězda
Počet kanálů	1	1	1	1
Přístupová metoda	CSMA	TDMA/ CSMA	CSMA	Náhodný přístup
Zabránění neužit. naslouchání	LPL	LPL	LPL	LPL
Synchronizace	NE	ANO	NE	NE
Hlavní přínos	Kombinace CSMA s dlouhou preambulí	Učení LPL rozvrhu režimu	Mnohonásobně kratší preambule	Kombinace TDMA/CSMA nad B-MAC

	Synchronní protokoly		
	T-MAC	S-MAC	D-MAC
Topologie	Mesh	Mesh	Mesh
Počet kanálů	1	1	1
Přístupová metoda	CSMA	CSMA	CSMA
Zabránění neužitečného naslouchání	Periodický režim spánku	Periodický režim spánku	Periodický režim spánku
Synchronizace	NE	ANO	NE
Hlavní přínos	Režim aktivní/spánek	Adaptivní pracovní cyklus	Změny režimu aktivní/spánek

5 PRAKTICKÁ ČÁST

5.1 Experimentální měření

Před vlastním návrhem metody na měření energetické náročnosti jsem měl možnost vyzkoušet si měření již známou metodou. Měření bylo prováděno pomocí kitu od společnosti TI (Texas Instruments), díky nemuž jsem měl možnost ověřit si zapojení a nastavení vstupních parametrů. Z naměřených výsledků byla sestrojena grafická závislost odběru proudu na čase. V příloze A jsou naměřené průběhy zobrazené na osciloskopu.

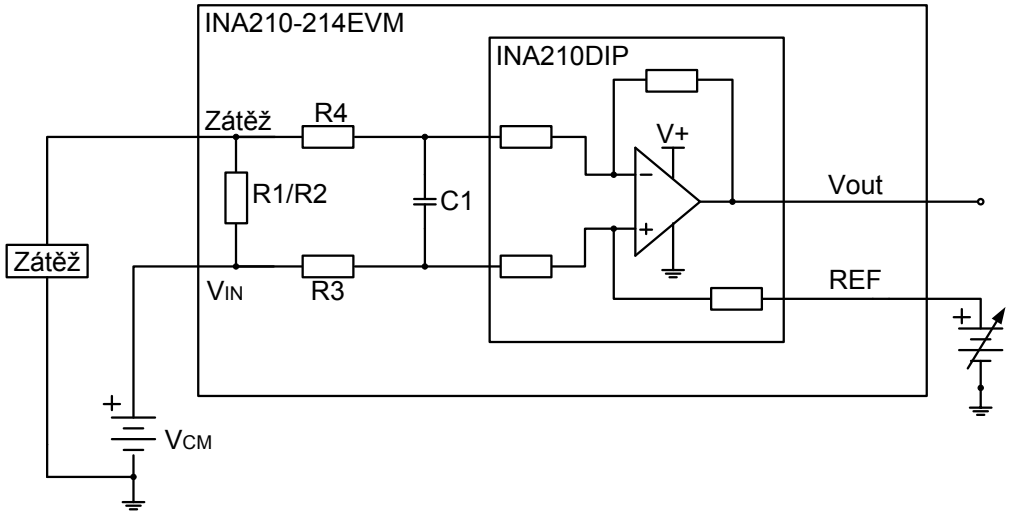
5.1.1 Použité přístroje a součástky

K experimentálnímu měření byly použity tyto přístroje a součástky [23] [24] [25]:

- kit Texas Instruments INA210-214EVM s oper. zesilovačem INA210AIDCKT (zisk $G_{INA210} = 200$),
- osciloskop Agilent Technologies DSO1012A,
- stejnosměrný zdroj Agilent Technologies E3620A,
- dva senzorové uzly IRIS XM 210 (jeden z nich byl router) s nainstalovaným softwarem od společnosti Atmel – Bitcloud, použitá technologie byla Zigbee Pro,
- rezistor $R_2 = 1\,\Omega$ s tolerancí 1 %,
- rezistory $R_3, R_4 = 0\,\Omega$, s tolerancí 5 % (řešeno metalickými propojkami,)
- filtrační kondenzátor $C_1 = 100\,\mathrm{nF}$,
- metalické vodiče.

5.1.2 Schéma zapojení

Na Obr. 5.1 [23] je schéma zapojení zátěže (senzorového uzlu IRIS XM 210) a kitu TI INA210-214EVM obsahující operační zesilovač INA210AIDCKT, boční rezistor R_2, rezistory R_3 a R_4 a také filtrační kondenzátor C_1 [23].



Obr. 5.1: Schéma zapojení kitu TI INA210-214EVM [23]

Nastavené parametry a hodnoty součástek [23]

Napětí operačního zesilovače $V_+ = 7{,}5\,\mathrm{V}$.
Napětí senzorového uzlu $V_{CM} = 3\,\mathrm{V}$.
Rezistor $R_2 = 1\,\Omega$, s tolerancí 1 %.
Rezistory $R_3, R_4 = 0\,\Omega$, s tolerancí 5 %.
Filtrační kondenzátor $C_1 = 100\,\mathrm{nF}$.

5.1.3 Výsledky měření

Naměřené hodnoty byly naměřeny jako úbytek napětí na bočním rezistoru (bočníku). Ze vzorce:

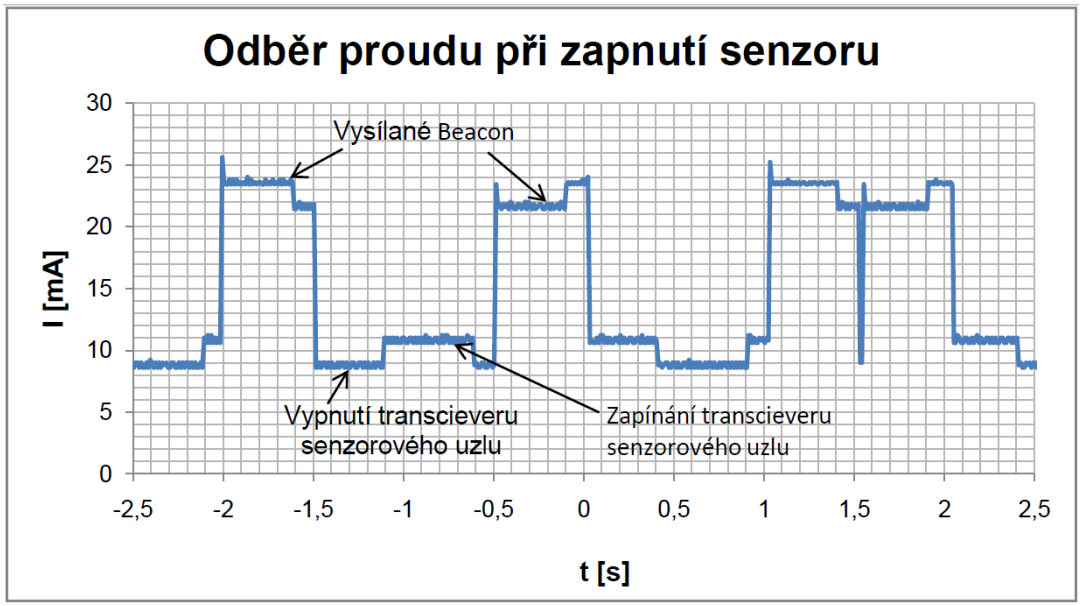
$$\Delta I = \frac{\Delta U}{R_2}, \tag{5.1}$$

vyplývá, že naměřené hodnoty úbytku napětí ΔU byly přímo úměrné proudovému odběru ΔI. Hodnoty bylo ještě nutné podělit hodnouto zesílení $G_{INA210} = 200$. Skutečný proudový odběr se tedy vypočítá:

$$I_{skut} = \frac{\Delta I}{G_{INA210}}. \tag{5.2}$$

Měření odběru proudu při zapnutí senzorového uzlu

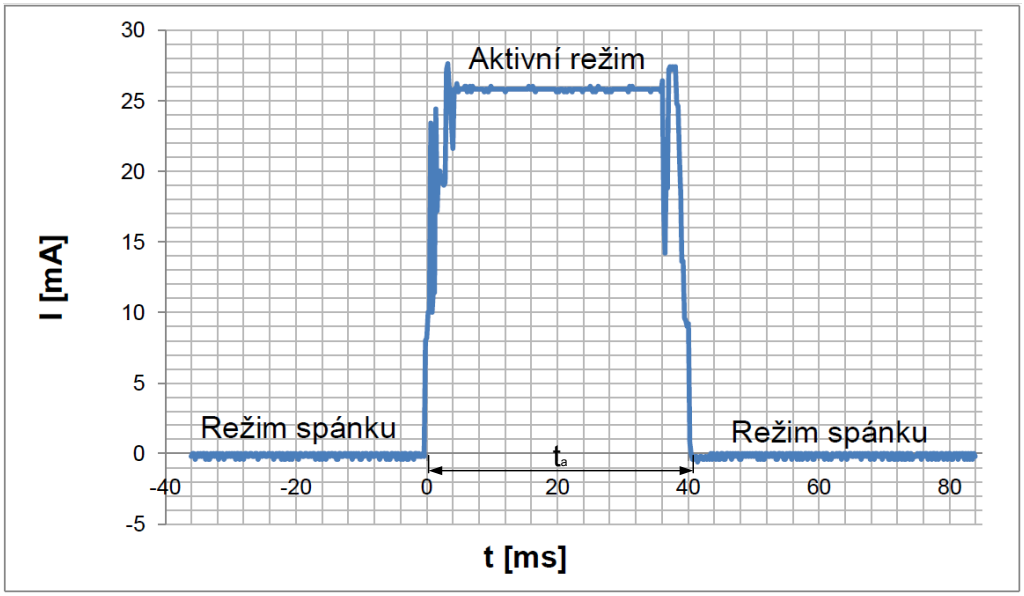
Senzor ihned po zapnutí vyhledává dostupnou síť. Při vyhledávání posílá vyhledávací Beacon pakety. Na Obr. 5.2 je naměřený průběh odběru proudu při posílání Beacon paketů. V příloze A.1 jsou zobrazené průběhy odběru proudu na osciloskopu při zapnutí senzoru.



Obr. 5.2: Naměřený průběh odběru proudu při zapnutí senzorového uzlu

Měření odběru proudu při komunikaci senzorových uzlů

Senzor se nejdříve připojí k již vytvořené síti, odešle data a přejde do režimu spánku. Z režimu spánku přejde po uplynutí 5s do aktivního režimu, ve kterém odešle data a poté znovu přejde do režimu spánku, viz Obr. 5.3. Doba aktivního režimu je $t_a = 40,4\,ms$. Toto řešení výrazně snižuje spotřebu senzorového uzlu a tím zásadně prodlužuje životnost energetického zdroje uzlu. V příloze A.3 jsou zobrazené průběhy odběru proudu na osciloskopu při komunikaci dvou senzorových uzlů.



Obr. 5.3: Naměřený průběh odběru proudu při komunikaci dvou senzorových uzlů

5.1.4 Srovnání spotřeby s ostatními bezdrátovými technologiemi

Technologie WSN se vyznačují nízko-výkonovým přenosem malého objemu dat. Tyto technologie jsou určeny pro aplikace s nízkou spotřebou, malou cenou a krátkou pracovní dobou přenosu. Zařízení je většinu času v režimu spánku, ze kterého se po určité době periodicky probouzí do aktivního stavu, ve kterém probíhá komunikace. V Tab. 5.1 je srovnání technologií bezdrátového přenosu dat [26].

Tab. 5.1: Porovnání technologií bezdrátového přenosu dat [26]

	Technologie bezdrátového přenosu		
	ZigBee PRO	Bluetooth	Wi-Fi
Typ sítě	WPAN	WPAN/WLAN	WLAN
Topologie	hvězda, strom, mesh	point to multi-point	point to multi-point
Rychlost	250 kbit/s	1 Mbit/s	> 54 Mbit/s
Odběr proudu při vysílání	28 mA	40 mA	> 400 mA
Aplikace	Sítě pro monitorování	Pro přenosy zvuků a souborů na krátké vzdálenosti	Koncový stupeň sítě Internet, propojení PC

5.2 Návrh měření

Vlastní návrh na měření energetické náročnosti vychází z experimentálního měření na kitu Texas Instruments INA 210-214EVM s operačním zesilovačem INA210AIDC. Při návrhu byl brán ohled na co největší zpřesnění měření pomocí vhodného výběru přístrojů a součástek.

5.2.1 Vybrané měřicí přístroje a součástky

Operační zesilovač

Při výběru vhodného operačního zesilovače bylo důležité, aby operační zesilovač splňoval požadavky na hodnoty některých parametrů: zisk (Gain), rozmezí vstupního napětí (Supply Voltage Rang), šířka pásma Bandwith), napájecí proud (Supply Current), poměr potlačení souhlasných signálů CMRR (Common Mode Rejection Ratio), rychlost přeběhu (Slew Rate), vstupní napěťové nesymetrie (Input Voltage Offset). V Tab. 5.2 jsou oper. zesilovače splňující dané požadavky.

Tab. 5.2: Porovnání zesilovačů [28] [29] [30] [31]

Model	LT6100CMS8	LT6106HS5	TSC101CILT	TSC101BILT
Výrobce	LINEAR TECHNOLOGY	LINEAR TECHNOLOGY	STMICROELECTRONICS	STMICROELECTRONICS
Zisk [V/V]	50	100	100	50
Rozmezí vstup. napětí [V]	2,7 – 3,6	2,7 – 3,6	4 – 24	4 – 24
Šířka pásma [kHz]	150	200	450	500
Napájecí proud [μA]	60	70	165	165
CMRR [dB]	120	120	105	105
Rychlost přeběhu [V/μs]	0,5	0,05	0,9	0,9
Vstupní napěťové nesymetrie [μV]	300	150	200	1500

Z dostupných operačních zesilovačů byl zvolen operační zesilovač LT6106HS5 od výrobce Linear Technology.

Osiloskop

U osciloskopu jsou důležitými parametry: vzorkovací kmitočet (Sampling Rate), šířka pásma (Bandwidth), vstupní impedance (Input Impedance), vstupní napětí (Input Voltage), doba náběhu (Rise Time) a rozlišení na svislé ose (Vertical Resolution). Měření proudového odběru senzorového uzlu spočívá v měření prudkých změn v charakteristice průběhu. K tomuto měření slouží nástroj Trigger. Pro kvalitnější měření je tedy nutné měřit s osciloskopem s co největší citlivostí nástroje Trigger (Trigger Sensantion). Srovnání použitelných osciloskopů je v Tab. 5.3.

Tab. 5.3: Porovnání osciloskopů [32] [33] [34]

Model	DSO5034A	TDS3034C	WAVESURFER 24MXS-A
Výrobce	AGILENT TECHNOLOGIES	TEXTRONIX	LECROY
Vzorkovací kmitočet [GSa/s]	2	2,5	50
Šířka pásma [MHz]	300	300	200
Vstupní impedance [MΩ]	1	1	1
Vstupní napětí [V]	400	150	400
Doba náběhu [ns]	1,17	1,2	1,75
Rozlišení na svislé ose [mV/div]	1 mV – 5 V	1 mV – 10 V	2 mV – 1 V

Jako měřící osciloskop byl vybrán Agilent Technologies typ DSO5034A z důvodu nejrychlejší doby náběhu a vysokého rozlišení na svislé ose.

Napájecí zdroj

Pro měření je důležitý také výběr kvalitního napájecího zdroje. Napájecí zdroj je určen výstupním napětím (Output Voltage) a výstupním proudem (Output Current). Důležitá je také plynulá regulace zátěže (Load Regulation). Porovnání napájecích zdrojů viz Tab. 5.4.

Tab. 5.4: Porovnání napájecích zdrojů [35] [36] [37]

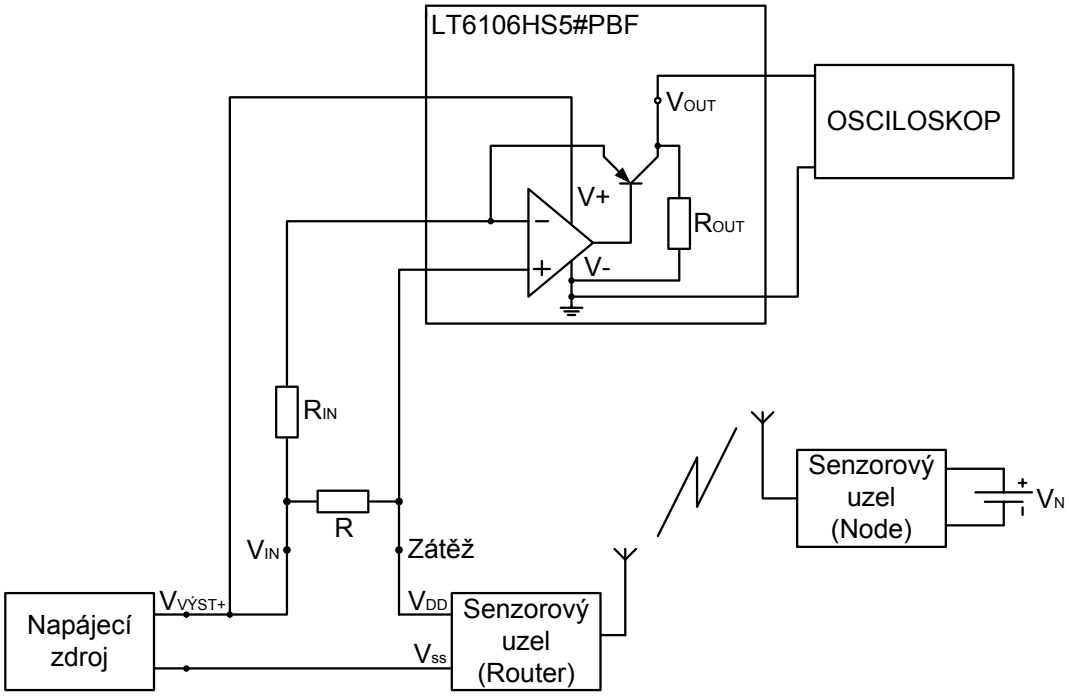
Model	72-7245	PL320QMD-E	E3649A
Výrobce	TENMA	AIM-TTI INSTRUMENTS	AGILENT TECHNOLOGIES
Výstupní napětí 1 [V]	30	32	35
Výstupní proud 1 [A]	3	2	2
Výstupní napětí 2 [V]	30	32	60
Výstupní proud 2 [A]	3	2,1	1,3
Výkon [W]	180	120	100
Regulace zátěže [%]	0,01	0,01	0,01

Z napájecích zdrojů byl vybrán zdroj E3649A od společnosti Agilent Technologies z důvodu dostatečného výkonu a plynulé regulace zátěže.

Senzorový uzel

Pro dosažení co nejvyšší přesnosti měření, byl senzorový uzel složen tak, aby byl komunikační modul oddělen od mikrokontroléru. Toto řešení nám umožňuje měřit zvlášť spotřebu energie mikrokontroléru a zvlášť spotřebu energie komunikačního modulu.

5.2.2 Schéma zapojení



Obr. 5.4: Navržené schéma zapojení [29]

Nastavení parametrů a hodnot součástek

Výstupní napětí napájecího zdroje $V_{VYST+} = 3{,}5\,V$
Napájecí napětí senzoru (node) $V_N = 3\,V$
Rezistor $R_{IN} = 100\,\Omega$, s tolerancí 1 %
Rezistor $R_{OUT} = 10\,k\Omega$, s tolerancí 1 %

Postup měření

Přístroje musí být zapojeny dle schématu na Obr. 5.4 [29]. Vstupní napětí přivedené na V_+ operačního zesilovače je 3,5 V,. Ke kladné napájecí svorce senzorového zdroje je připojen vstup In_+ operačního zesilovače, záporná svorka je přivedena na zem. Sonda osciloskopu je připojena na výstup V_{OUT}. Osciloskop musí mít nastavené horizontální rozlišení v řádu ms a vertikální rozlišení 1V/dílek. Pomocí nástroje Trigger, změříme skokové změny průběhu úbytku napětí na rezistoru R. U Triggeru

je nutné nastavit průběh Edge, aby reagoval na vzestupné a sestupné hrany průběhu a úroveň napětí, při kterém má Trigger na změny v charakteristice průběhu reagovat.

Nejdříve změříme průběh úbytku napětí na rezistoru R při zapnutí senzorového uzlu, kdy připojený uzel (router) zapneme a on začne vyhledávat síť a posílat vyhledávací Beacon pakety.

Poté změříme spotřebu senzorového uzlu (router) při komunikaci s jiným senzorovým uzlem (node). Uzel nejdříve zapneme a počkáme až se připojí do sítě, po přípojení vyšle senzorový uzel data a přejde do režimu spánku, ze kterého se po určité době probudí, opět odešle data a znovu usne. Celý proces se cyklicky opakuje.

Výsledný úbytek napětí ΔU je nutné přepočítat na odběr proudu ΔI na rezistoru R dle rovnice:

$$\Delta I = \frac{\Delta U}{R}. \tag{5.3}$$

Hodnota ΔI je ovšem zesílená, proto abychom dostali skutečnou hodnotu odběru proudu senzorového uzlu I_{skut}, je nutné ji ještě podělit hodnotou zisku operačního zesilovače $\mathrm{G_{LT6106HS5}}$:

$$I_{skut} = \frac{\Delta I}{\mathrm{G_{LT6106HS5}}}. \tag{5.4}$$

Výsledkem měření by měly být průběhy odběru proudu senzorového uzlu, podobné průběhům viz příloha A.

6 ZÁVĚR

Tato bakalářská práce se zabývá problematikou Energetické náročnosti IPv6 v bezdrátových senzorových sítích WSN. Bezdrátové senzorové sítě jsou v dnešní době terčem mnoha výzkumů, díky kterým se dostávají čím dál tím více do podvědomí a jejích možnosti uplatnění neustále narůstají. WSN mohou být použity v celé řadě aplikací pro sledování a monitorování od měření teploty, vlhkosti, tlaku, po zabezpečovací systémy a řízení průmyslového monitorování. Počet prvků, neboli senzorových uzlů WSN sítě se odvíjí od její rozlohy a jeho hodnota může dosahovat několika desítek, stovek i tisíců. Jedním z hlavních témat v oblastí vývoje bezdrátových senzorových sítích je spotřeba energie. Spotřebu energie lze snížit výběrem vhodných hardwarových součástí s pokud možno co nejmenší energetickou náročností. Jedná se především o výběr mikrokontroléru s mikroprocesorem, komunikačního bloku, senzorových obvodů. Volba vhodného zařízení značně snižuje spotřebu energie senzorového uzlu a výrazně tak vzrůstá životnost napájecího zdroje, kterým jsou ve WSN sítích většinou bateriové články. Spotřeba energie při komunikace je uváděna spotřebou energie pro příjem jednoho bytu R_x a spotřebou při vysílání jednoho bitu T_x v závislosti na vysílacím výkonu. Úspory energie při vysílání můžeme docílit redukcí počtu přenášených bitů a omezením maximálního dosahu vysílače. Omezení vysílacího výkonu bude mít za následek neschopnost senzorového uzlu komunikovat na delší vzdálenosti. Proto bude mít komunikace skokovou charakteristiku a do přenosu dat mezi dvěma vzdálenými uzly budou zapojeny i mezilehlé uzlu, které budou směrovat data od odesílatele k příjemci.

Energetická náročnost IPv6 byla řešena na úrovni fyzické a linkové vrstvy. U první vrstvy je pro snížení spotřeby důležité zvolení vhodného způsobu čerpání energie z napájecího zdroje. Využívá se nelineární vybíjecí charakteristika, kdy nejsou senzorové uzly napájeny konstantně, ale po impulsech. Jako napájecí zdroje se využívají bateriové články. V práci jsou rozebrány a porovnány používané typy akumulátorů viz Tab. 4.1. Jelikož žádný z akumulátorů nevydrží požadovanou dobu, skládají se zdroje s použitím více článků, kdy je např. senzorový uzel nejdříve nějakou dobu (pár ms) napájen z prvního článku, poté přejde na napájení z článku druhého apod. V současné době se také hojně využívá dobíjení bateriových článků alternativními zdroji z okolí, zejména pak solární energií a energií vibračních dějů. Linková vrstva definuje pro nižší spotřebu především režim spánku a řadu MAC protokolů. MAC protokoly se rozdělují na synchronní protokoly (S-MAC, T-MAC, D-MAC) a protokoly asynchronní (B-MAC, Z-MAC, X-MAC, WiseMAC). Protokoly mají odlišně řešenou přístupovou metodu, topologii, potlačení neužitečného naslouchání kanálu, synchronizaci a další parametry. Srovnání MAC protokolů je v Tab. 4.4.

Poslední část bakalářské práci je věnována měření energetické náročnosti senzorového uzlu. Nejdříve bylo provedeno experimentální měření pomocí kitu TEXAS INSTRUMENTS INA210-214EVM. Z naměřených hodnot byla sestrojena grafická závislost odběru proudu na čase při zapnutí senzorového uzlu a při komunikaci dvou uzlů. Na základě experimentálního měření byla navržena vlastní měřící metoda. Koncept spočíval ve operačního zesilovače, měřícího přístroje, zdroje napájení, sestrojení schématu zapojení a v sepsání popisu měření a zpracování získaných hodnot. Pří návrhu bylo hlavním kritériem zpřesnění měřící metody, které bylo dosaženo výběrem vhodných přístrojů a součástek a také oddělením výpočetního bloku od bloku komunikačního.

LITERATURA

[1] VASSEUR, Jean-Philippe; DUNKELS, Adam. *Interconnecting Smart Objects with IP: The Next Internet*. 30 Corporate Drive, Suite 400, Burlington, MA 01803, USA : Morgan Kaufmann Publishers is an Imprint of Elsevier, 2010. 432 s. ISBN 978-0-12-375165-2.

[2] [2] RAGHAVENDRA, C. S.; SIVALINGAM, Krishna M; ZNATI, Taieb. *Wireless Sensor Networks*. 233 Spring Street, New York, NY 10013, USA : Springer Science + Business Media, LLC, 2004. 442 s. ISBN 978-1-4020-7883-5.

[3] LEWIS, F. L. *Smart Environments: Technologies, Protocols, and Applications*. The University of Texas at Arlington, 7300 Jack Newell Blvd. S Ft. Worth, Texas 76118-7115 : WILEY-INTERSCIENCE, A John Wiley & Sons, INC., Publication, 2005. Wireless Sensor Networks1, s. 407. ISBN 0-471-54448-5.

[4] GUTIERREZ, Jose A. *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*. USA : Institute of Electrical and Electronics Engineers, Inc., 2003. 679 s. ISBN 0-7381-3677-5.

[5] MAURI, KUORILEHTO , et al. *Ultra-Low Energy Wireless Sensor Networks in Practice : Theory, Realization and Deployment*. Tampere University of Technology, Finland : A John Wiley & Sons, Ltd, 2007. 368 s. ISBN 978-0-470-05786-5.

[6] HUI, PHD, Jonathan; CULLER, PHD, David; HAKRABARTI, Samita. (IPSO) Alliance [online]. January 2009 [cit. 2010-11-26]. *6LoWPAN: Incorporating IEEE 802.15.4 into the IP architecture : Internet Protocol for Smart Objects*. Dostupné z WWW: <http://ipso-alliance.org/smart-metering-leader-itron-joins-ipso-alliance>.

[7] SHELBY, Zach; BORMANN, Carsten. *6LoWPAN : The wireless embedded internet*. The Atrium, Southern Gate, Chichester, West Sussex, PO 19 8SQ, United Kingdom : John Wiley & Sons Ltd, 2009. 219 s. ISBN 978-0-470-74799-5.

[8] N. KUSHALNAGAR, N. ; MONTENEGRO, G. ; SCHUMACHER, C. RFC4919 [online].August 2007 [cit. 2010-11-23]. *Network Working Group*. Dostupné z WWW: <http://tools.ietf.org/html/rfc4919>.

[9] SEHGAL, Anuj; SCHÖNWÄLDER, Jürgen. Jacobs University [online]. 2008 [cit. 2010-11-28]. *6lowpan with uIPv6 in Contiki*. Dostupné z WWW: <http://cnds.eecs.jacobs-university.de/courses/adsl-2009/presentation-3.pdf>.

[10] TSIFTES, Nicolas; ERIKSSON, Joakim; DUNKELS, Adam Kista. Sweden : Swedish Institute of Computer Science [online]. 2009 [cit. 2010-11-29]. *Poster Abstract: Low-Power Wireless IPv6 Routing with ContikiRPL. In Sss.* Dostupné z WWW: <http://www.sics.se/ adam/tsiftes10rpl.pdf>.

[11] CHIANG, Mu-Huan. *Energy Optimization in Wireless Sensor Networks.* North Carolina State University, 2007, USA : VDM Verlag Dr. Müller e.K., 100 s. ISBN 978-3-8364-6132-0.

[12] TIWARI, Ankit; BALLAL , Prasanna ; LEWIS , Frank L. ACM Digital Library [online]. 2007 [cit. 2010-11-27]. *Energy-efficient wireless sensor network design and implementation for condition-based maintenance.* Dostupné z WWW: <http://dl.acm.org/citation.cfm?id=1210670>.

[13] DOBREBATERIE.cz [online]. 2008 [cit. 2010-12-02]. *Vše o bateriích - druhy baterií.* Dostupné z WWW: <http://www.dobrebaterie.cz/inshop/scripts/show.asp?page=druhy-baterii.htm>.

[14] BLUEJAY, Michael. Michael Bluejay's.com [online]. 2002 [cit. 2010-12-03]. *Household Battery Types Compared (AAA, AA, C, D, and 9V).* Dostupné z WWW: <http://michaelbluejay.com/batteries>.

[15] Budget Batteries [online]. 2005 [cit. 2010-12-03]. *Battery Information.* Dostupné z WWW: <http://www.budgetbatteries.co.uk/batteries/>.

[16] TRNEČKA, Ivan. Mobil.cz [online]. 2001 [cit. 2010-12-03]. *Baterie a akumulátory pro PDA – Typy baterií.* Dostupné z WWW: <http://palmare.idnes.cz/pda.asp?r=pda&c=A010418_0029784_pda>.

[17] Cettra.cz [online]. 2004 [cit. 2010-12-03]. *Jak na baterie NiCd a NiMH.* Dostupné z WWW: <http://www.cettra.cz/vysilacky-radiostanice/MOTOROLA/Baterie-NiCd,-NiMH-.../Jak-na-baterie/20>.

[18] KOHVAKKA, Mikko. *Medium Access Control and Hardware Prototype Desings for Low-Energy Wireless Sensor Network.* Tampere University of Technology : Tampereen teknillinen yliopisto, Julkaisu 808, 2009. 2006 s. ISBN 978-952-15-2189-B.

[19] JURDAK, Raja, et al. *Radio Sleep Mode Optimization in Wireless Sensor Networks.* IEEE TRANSACTIONS ON MOBILE COMPUTING [online]. 2010, 7, [cit. 2011-04-27]. Dostupné z WWW:

<http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5432178&tag=1>. ISSN 1536-1233.

[20] SEUNG-WOO Hong, at al. FMC Technol. Team, ETRI, Daejeon, South Korea [online].September 2010 [cit. 2011-04-27]. *A Novel Continuous Object Tracking Scheme for Energy-constrained Wireless Sensor Networks*. Dostupné z WWW: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5594517&tag=1>.

[21] BUETTNER, Michael , et al. *X-MAC: A Short Preamble MAC Protocol For Duty-CycledWireless Sensor Networks*. Department of Computer Science. May 2006, Technical Report CU-CS-1008-06, 12 s.

[22] VOJÁČEK, A. HW server [online].[cit. 2010-12-05]. *ZigBee - novinka na poli bezdrátové komunikace*. Dostupné z WWW: <http://hw.cz/Rozhrani/ART1299- ZigBee—novinka-na-poli-bezdratove-komunikace.html>.

[23] TEXAS INSTRUMENTS *Manuál k INA210-214EVM*. [online] 2008 [cit.2011-05-21]. Dostupné z WWW: <http://focus.ti.com/lit/ug/sbou065/sbou065.pdf>.

[24] TEXAS INSTRUMENTS *Manuál k INA210*. [online] 2009[cit.2011-05-21]. Dostupné z WWW: <http://focus.ti.com/docs/prod/folders/print/ina210.html>.

[25] AGILENT TECHNOLOGIES *Manuál k DSO1012A*. [online] 2009[cit.2011-05-21]. Dostupné z WWW: <http://cp.literature.agilent.com/litweb/pdf/5989-9368EN.pdf>.

[26] Software Technology Group [online]. 2009 [cit. 2011-05-22]. *ZigBee compare with other wireless standards*. Dostupné z WWW: <http://www.stg.com/wireless/ZigBee_comp.html>.

[27] JIN-SHYAN, Lee; YU-WEI, Su; CHUNG-CHOU, Shen. Industrial Technology Research Institute (ITRI), Hsinchu, Taiwan [online]. 2007 [cit. 2011-5-23]. *A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi*. Dostupné z WWW: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04460126>.

[28] LINEAR TECHNOLOGY *Manuál k LT6100CMS8#PBF*. [online] 2005 [cit.2011-05-23]. Dostupné z WWW: <http://cds.linear.com/docs/Datasheet/6100fb.pdf>.

[29] LINEAR TECHNOLOGY *Manuál k LT6106HS5#PBF*. [online] 2007 [cit.2011-05-23]. Dostupné z WWW: <http://cds.linear.com/docs/Datasheet/6106fa.pdf>.

[30] STMICROELECTRONICS *Manuál k TSC101CILT*. [online] 2007 [cit.2011-05-23]. Dostupné z WWW: <http://www.st.com/stonline/books/pdf/docs/13313.pdf>.

[31] STMICROELECTRONICS *Manuál k TSC101BILT*. [online] 2007 [cit.2011-05-23]. Dostupné z WWW: <http://www.st.com/stonline/books/pdf/docs/13313.pdf>.

[32] AGILENT TECHNOLOGIES *Manuál k DSO5034A*. [online] 2010 [cit.2011-05-23]. Dostupné z WWW: <http://cp.literature.agilent.com/litweb/pdf/5989-6110EN.pdf>.

[33] TEKTRONIX *Manuál k TDS3034C*. [online] 2007 [cit.2011-05-23]. Dostupné z WWW: <http://www.farnell.com/datasheets/33538.pdf>.

[34] LECROY *Manuál k WAVESURFER 24MXS-A*. [online] 2010 [cit.2011-05-23]. Dostupné z WWW: <http://lecroycorp.com/files/pdf/LeCroy_WaveSurfer_XS-a_Datasheet.pdf>.

[35] TENMA *Manuál k TDS3034C*. [online] 2003 [cit.2011-05-23]. Dostupné z WWW: <http://www.farnell.com/datasheets/62454.pdf>.

[36] AIM-TTI INSTRUMENTS *Manuál k AIM-TTI INSTRUMENTS*. [online] 2008 [cit.2011-05-23]. Dostupné z WWW: <http://www.farnell.com/datasheets/99860.pdf>.

[37] AGILENT TECHNOLOGIES *Manuál k E3649A*. [online] 2008 [cit.2011-05-23]. Dostupné z WWW: <http://cp.literature.agilent.com/litweb/pdf/5968-7355EN.pdf>.

[38] CYPRESS SEMICONDUCTOR *Manuál k CY8C29566-24AXI*. [online] 2010 [cit.2011-05-23]. Dostupné z WWW: <http://www.cypress.com/?docID=24691>.

[39] MICROCHIP *Manuál k PIC18LF8720-I/PT*. [online] 2004 [cit.2011-05-23]. Dostupné z WWW: <http://www.farnell.com/datasheets/26259.pdf>.

[40] ATMEL *Manuál k ATMEGA88PV-10AU*. [online] 2010 [cit.2011-05-23]. Dostupné z WWW: <http://www.atmel.com/dyn/resources/prod_documents/8025s.pdf>.

[41] TEXAS INSTRUMENTS *Manuál k CC2520RHDT*. [online] 2007 [cit.2011-05-23]. Dostupné z WWW: <http://focus.ti.com/lit/ds/symlink/cc2520.pdf>.

[42] NORDIC SEMICONDUCTOR *Manuál k NRF24L01G*. [online] 2007 [cit.2011-05-23]. Dostupné z WWW: <http://www.farnell.com/datasheets/12195.pdf>.

[43] FREESCALE SEMICONDUCTOR *Manuál k MC13201FC*. [online] 2008 [cit.2011-05-23]. Dostupné z WWW: <http://www.freescale.com/files/rf_if/doc/data_sheet/MC13201.pdf>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

ACK	Acknowledgment
B-MAC	Berkeley-MAC
BI	Beacon Interval
BPSK	Bi. Phase-Shift Keying
CAP	Contention Access Period
CCA	Clear Channel Asessment
CFP	Contention Free Period
CRC	Cyclic Redundancy Check
CSMA	Carrier Sense Multiple Access
CSMA/CA	Carrier Sense Multiple Access with Colision Avoidance
CTS	Clear-To-Send
FFD	Direct Sequence Spread Spectrum
GPRS	General Packet Radio Service
GTS	Guaranteed Time Slot
ICMP	Internet Control Message Protocol
IEEE	Institue of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IID	Interface Identifier
IPSec	IP Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
Li-Ion	Lithium-Ion
Li-Pol	Lithium-ion Polymer
LoWPAN	Low power Wireless Personal Area Networks

LLN	Low-power and Lossy Networks
MAC	Medium Access Control
MACA	Multiple Access with Collision Avoidance
MCU	Machine Control Unit
MTU	Maximum Transmission Unit
Ni-Cd	Nickel-Cadmium
Ni-Mh	Nickel-Metal hydride
NAT	Network Address Translation
O-QPSK	Offset Quadrature Phase-Shift Keying
PAN	Personal Area Network
PHY	Physical
RFD	Reduced Function Device
RTS	Request-To-Send
S-MAC	Sensor-MAC
SD	Superframe Duration
T-MAC	Timeout-MAC
TCP	Transmission Control Protocol
TI	Texas Instruments
UDP	User Datagram Protocol
Wi-Fi	Wireless Fidelity
WiseMAC	Wireless Sensor MAC
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network

SEZNAM PŘÍLOH

A Naměřené průběhy zobrazené na osciloskopu **68**

A.1 Zobrazený průběh odběru proudu při zapnutí senzorového uzlu . . . 68

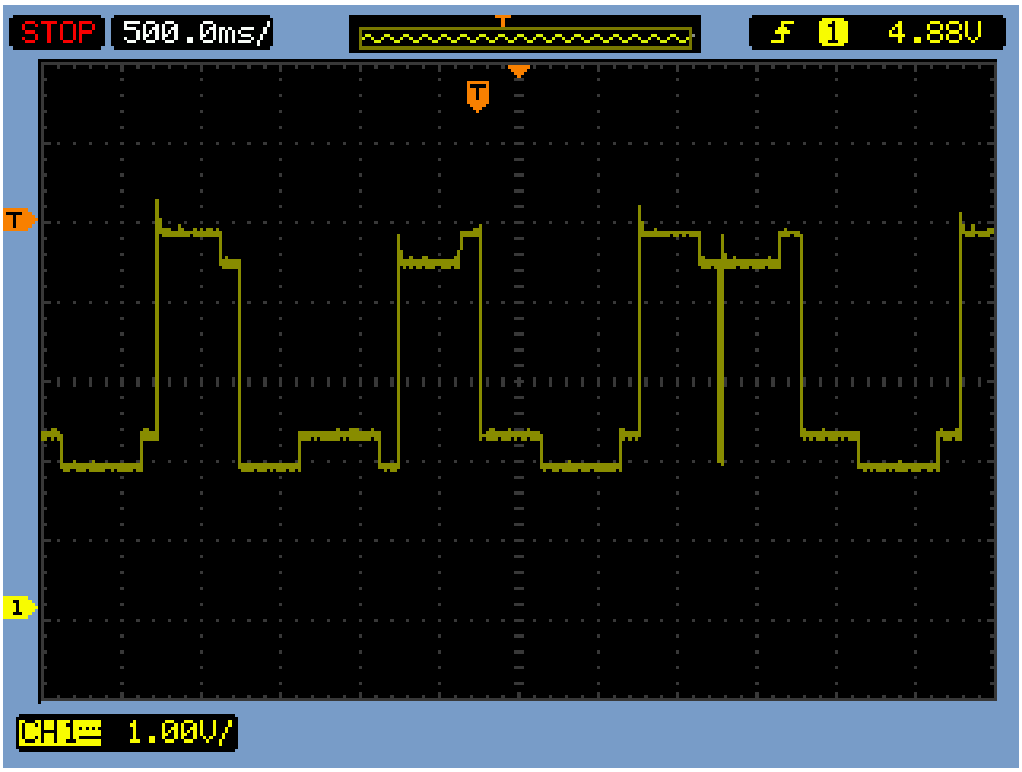
A.2 Přiblížený průběh odběru proudu při zapnutí senzorového uzlu . . . 69

A.3 Zobrazený průběh odběru proudu při komunikaci senzorových uzlů . 70

A.4 Přiblížený průběh odběru proudu při komunikaci senzorových uzlů . 71

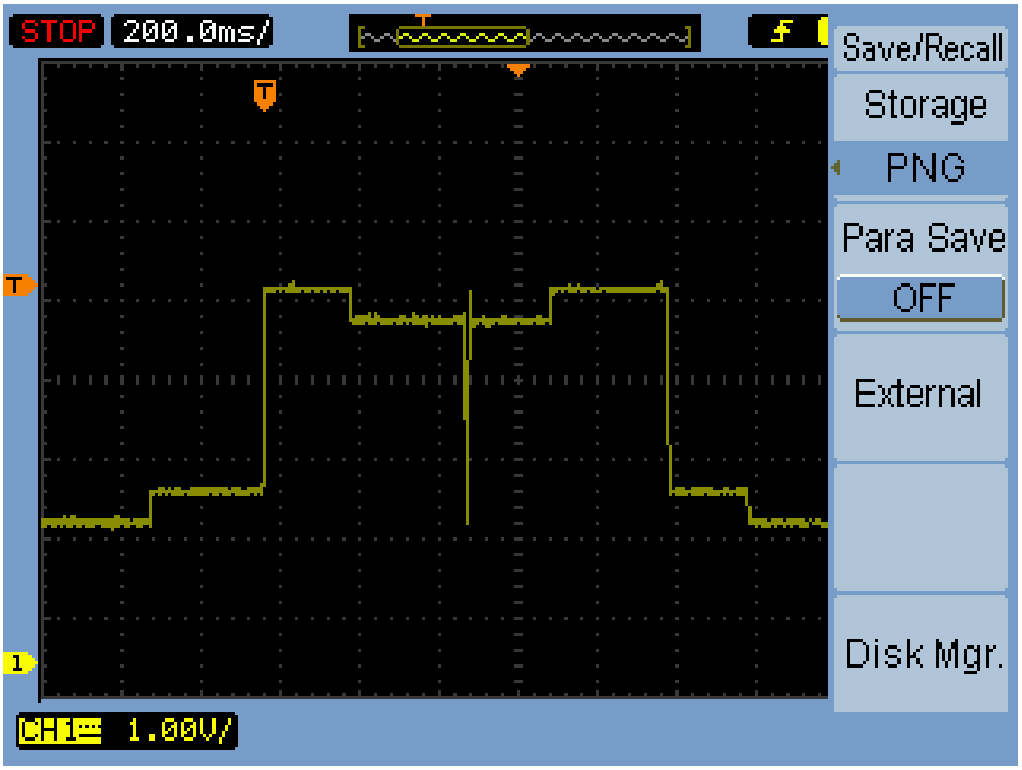
A NAMĚŘENÉ PRŮBĚHY ZOBRAZENÉ NA OSCILOSKOPU

A.1 Zobrazený průběh odběru proudu při zapnutí senzorového uzlu



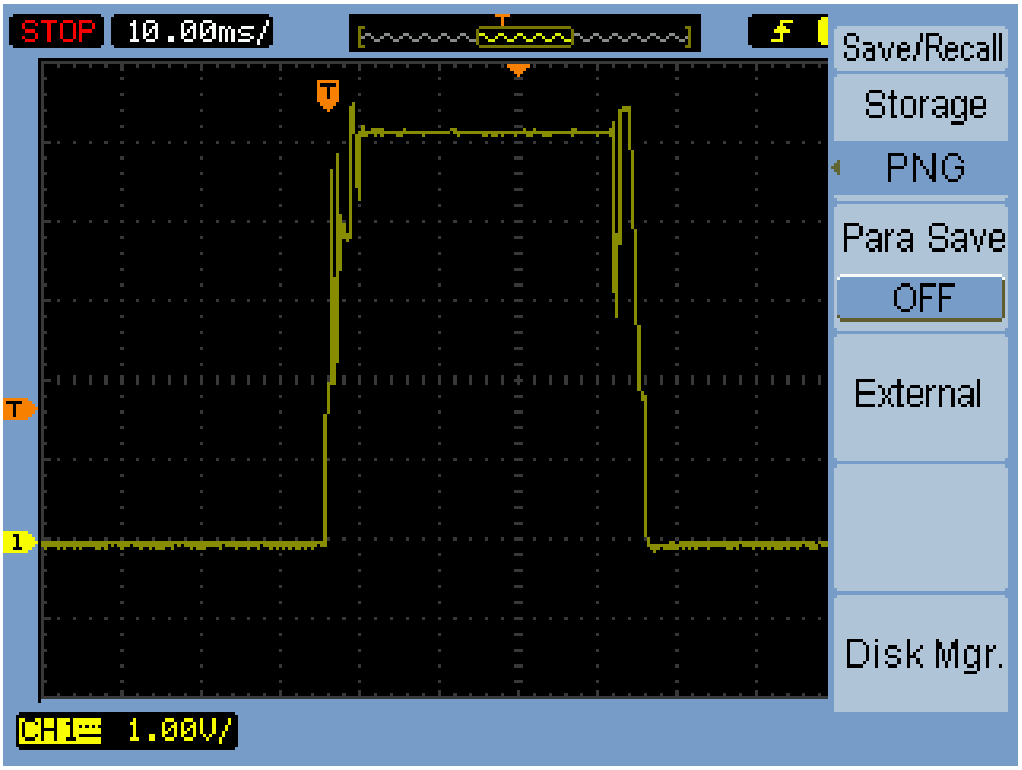
Obr. A.1: Zobrazený průběh odběru proudu při zapnutí senzorového uzlu

A.2 Přiblížený průběh odběru proudu při zapnutí senzorového uzlu



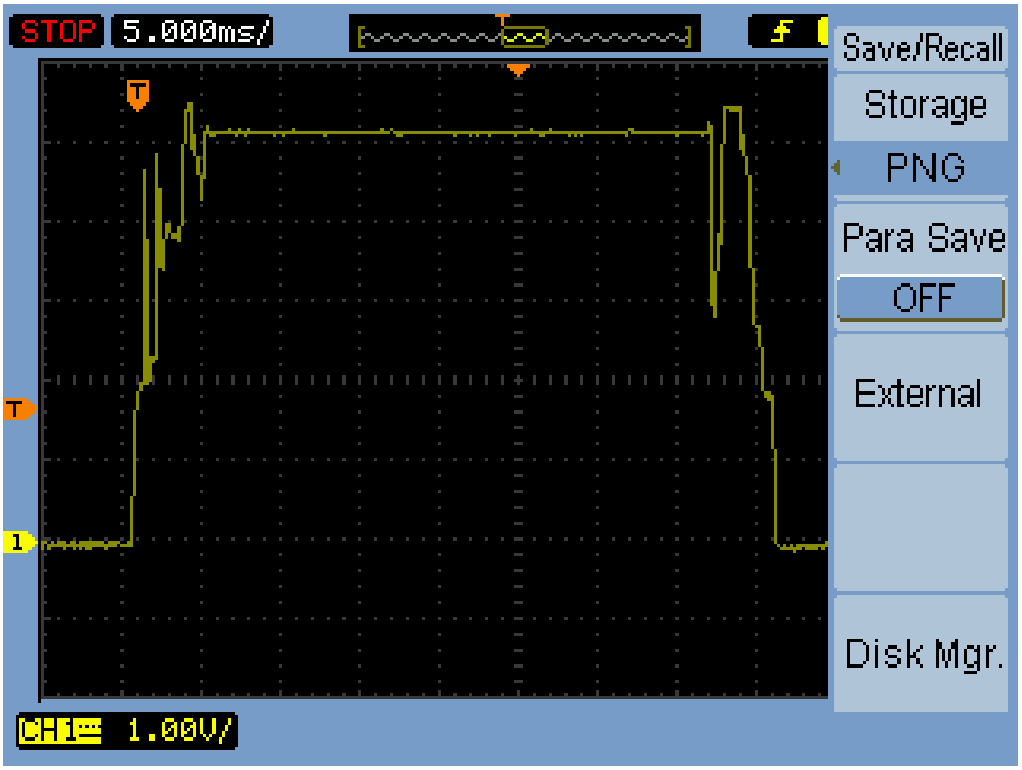
Obr. A.2: Přiblížený průběh odběru proudu při zapnutí senzorového uzlu

A.3 Zobrazený průběh odběru proudu při komunikaci senzorových uzlů



Obr. A.3: Zobrazený průběh odběru proudu při komunikaci senzorových uzlů

A.4 Přiblížený průběh odběru proudu při komunikaci senzorových uzlů



Obr. A.4: Přiblížený průběh odběru proudu při komunikaci senzorových uzlů