VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

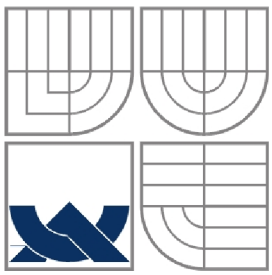
# BEZDRÁTOVÝ HLASOVACÍ SYSTÉM ZALOŽENÝ NA IEEE 802.15.4/ZIGBEE

SEMESTRÁLNÍ PROJEKT
SEMESTRAL PROJECT

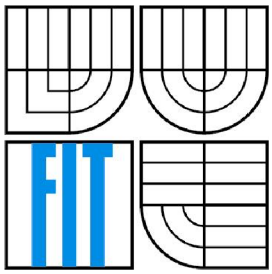
AUTOR PRÁCE
AUTHOR

Bc. PAVEL ALBRECHT

BRNO 2010



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

# BEZDRÁTOVÝ HLASOVACÍ SYSTÉM ZALOŽENÝ NA IEEE 802.15.4/ZIGBEE

WIRELESS VOTING SYSTÉM BASED ON IEEE 802.15.4/ZIGBEE

SEMESTRÁLNÍ PROJEKT
SEMESTRAL PROJECT

AUTOR PRÁCE
AUTHOR

Bc. PAVEL ALBRECHT

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. JOSEF STRNADEL, Ph.D.

BRNO 2010

# Abstrakt

Cílem práce je podrobně popsat bezdrátový protokol IEEE 802.15.4/ZigBee. Práce se dále zaměřuje na návrh architektury bezdrátového hlasovacího systému založeného na těchto standardech. Konkrétně na možnosti použití zapůjčeného vývojového kitu Freescale 1321xNSK-BDM k hlasování a identifikaci účastníků. Dále rozvádí problém zpracování přijatých hlasů z bezdrátové sítě ZigBee a jejich ukládání na server. Práce se zabývá i možností zobrazení výsledků hlasování na webovém rozhranní.

# Abstract

The goal of this work is to describe in detail the wireless protocol IEEE 802.15.4/ZigBee. This work also focuses on architecture design of wireless voting system based on these standards. Specifically, the possibility of using borrowed Freescale development kit 1321xNSK-BDM to vote and identification of participants. Further describe details the problem of processing the votes of ZigBee wireless networks and their storage on the server. The work is exploring options to display results of votes on the web interface.



# Klíčová slova

IEEE 802.15.4, ZigBee, hlasování, bezdrátový hlasovací systém, Freescale MC1321x, Java, RS232, RXTX, XML, JDOM, PHP.

# Keywords

IEEE 802.15.4, ZigBee, voting, wireless voting system, Freescale MC1321x, Java, RS232, RXTX, XML, JDOM, PHP.


# Citace

Albrecht Pavel: Bezdrátový hlasovací systém založený na IEEE 802.15.4/ZigBee, semestrální projekt, Brno, FIT VUT v Brně, 2010.

# Bezdrátový hlasovací systém založený na IEEE 802.15.4/ ZigBee

## Prohlášení

Prohlašuji, že jsem tento semestrální projekt vypracoval samostatně pod vedením pana Ing. Josefa Strnadela, Ph.D.
Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

……
Pavel Albrecht
6. ledna 2010

## Poděkování

Tímto bych chtěl poděkovat Ing. Josefu Strnadelovi, Ph.D. za poskytnuté konzultace, cenné rady a náměty a za zapůjčení vývojového kitu Freescale MC1321x.

# Obsah

# 1 Úvod

## 1.1 Slovo úvodem

Hlasování. Již v dávných dobách se jednalo o účinný a velmi jednoduchý způsob volby z možností ano či ne nebo z více navrhovaných možností. Jde v podstatě o demokratický rozhodovací proces. V dnešní době má hlasování stále stejné opodstatnění a význam. Je důležité v řadě odvětví a značně ovlivňuje i dění kolem nás.

Co se ovšem mění je způsob zpracovaní hlasů od jednotlivých účastníků. Stále používanou, v některých oblastech již nahrazenou, metodou hlasování je pomocí zvednuté ruky, vyřčeného slova nebo útržku papíru, na který je napsána odpověď.

V dnešní moderní době bývá tento systém nahrazován takzvaným elektronickým hlasovacím systémem. Kdy pro získání hlasu se používá elektronické zařízení. Tím může být klasický osobní počítač nebo speciální konzole, které obsahuje pouze pár ovládacích prvků, jako je vypínač, hlasovací tlačítka nebo i informační displej.

Obrovskou výhodou elektronických systémů je efektivní a okamžitý sběr hlasů, zabezpečení, jednoduchost, průhlednost, možnost archivace nebo přímého exportu výsledků na výstupní periferii nebo rozhranní. V některých případech i mobilita a dostupnost. Nevýhodou pak náklady na zřízení elektronického hlasovacího systému, jeho údržbu a provoz.

## 1.2 Cíl práce

Cílem práce je podrobně popsat bezdrátový protokol IEEE 802.15.4/ZigBee. Práce se dále zaměřuje na návrh architektury bezdrátového hlasovacího systému založeného na těchto standardech. Konkrétně na možnosti použití zapůjčeného vývojového kitu Freescale 1321xNSK-BDM k hlasování a identifikaci účastníků. Dále rozvádí problém zpracování přijatých hlasů z bezdrátové sítě ZigBee a jejich ukládání na server. Práce se zabývá i možností zobrazení výsledků hlasování na webovém rozhranní.

## 1.3 Obsah kapitol

První kapitola podrobně popisuje protokol IEEE 802.15.4/ZigBee. Stručně uvádí jeho historii, detailně rozebírá jednotlivé vrstvy a jejich vlastnosti. Rovněž uvádí funkci těchto vrstev a technologie použité na nich. V závěru se kapitola zabývá bezpečností v senzorových sítích ZigBee.

Druhá kapitola obsahuje úvod do problematiky hlasování a rozdělení hlasování. Dále se zabývá návrhem architektury bezdrátového hlasovacího systému založeného na IEEE 802.15.4/ZigBee.

# 2 Protokol IEEE 802.15.4/ZigBee

Bezdrátová komunikační technologie IEEE 802.15.4/ZigBee je poměrně nová technologie (2009). Jedná se o mezinárodní otevřený bezdrátový standard spravovaný nadnárodní organizací ZigBee Alliance a postavený na standardu IEEE 802.15.4, schváleným standardizační organizací IEEE.

ZigBee začalo být koncipováno v roce 1998, jelikož bezdrátové technologie Wi-Fi nebo Bluetooth byly pro některé aplikace z mnoha hledisek nevhodné. ZigBee bylo dokončen v květnu 2003 a schválen následující rok v prosinci. V roce 2005 uvolnila ZigBee Alliance veřejně dostupnou specifikaci známou jako ZigBee 2004. Poté následovala, podle roku vydání, specifikace ZigBee 2006 a poslední specifikace, zvaná ZigBee 2007.

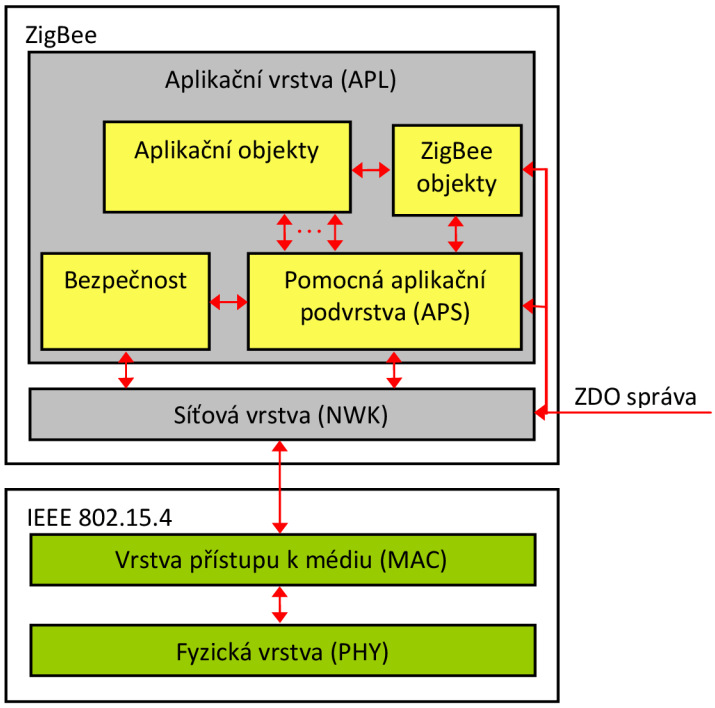
Tato bezdrátová technologie nemá působit, jako přímý konkurent Wi-Fi nebo Bluetooth, nýbrž jako doplněk, který má rozšířit oblasti nasazení bezdrátových sítí. ZigBee je vhodné především pro obor automatizace a řídící techniky. Uplatňuje se pro automatizaci budov, spotřební elektroniku, monitorování a diagnostiku prostředí a zařízení, pro počítačové periferie, dálkové ovládání nebo například ve zdravotnictví. Vyznačuje se především svou jednoduchostí, spolehlivostí, energetickou nenáročností, příznivou cenou a možností vytvářet libovolnou síťovou strukturu [5], [6].

Následující podkapitoly a jejich obsah se zabývají podrobným popisem protokolu IEEE 802.15.4/ZigBee.

## 2.1 Základní popis protokolu

Referenční model IEEE 802.15.4/ZigBee vychází ze sedmivrstvého modelu ISO/OSI (International Standards Organization/ Open System Interconnection). Ke své činnosti ovšem využívá pouze ty vrstvy, které jsou důležité pro dosažení požadované funkce a vlastností. Podrobný model ilustruje obrázek 2.1.

Struktura je navržena maximálně úsporně kvůli předpokládané implementaci do 8 bitových mikrokontrolérů s omezenou velikostí paměti. Nároky na systémovou paměť jsou okolo 30 kB [6], [7]. Protokol IEEE 802.15.4/ZigBee je postaven na dvou standardech. IEEE 802.15.4 a ZigBee. Každý z těchto standardů je definován jinou organizací a spravuje patřičné vrstvy.




*Obr. 2.1 Struktura protokolu IEEE 802.15.4/ZigBee.*

## 2.2 Standard IEEE 802.15.4

Definuje dvě nejnižší vrstvy. Jde o fyzickou vrstvu (PHY) a vrstvu přístupu k médiu (MAC) pro LR-WPAN (Low-Rate Wireless Private Area Network). Přestože tento standard nebyl vyvinut speciálně pro senzorové sítě, je pro ně vhodný. Standard IEEE 802.15.4 je použit kvůli své nízké bitové chybovosti u zařízení s velkým šumem. Dále je charakterizován malým datovým přenosem, energetickou nenáročností a nízkou cenou [8].

### 2.2.1 Typy zařízení

Úvodem do standardu IEEE 802.15.4, LR-WPAN podporují dva typy zařízení [8].

**Plně funkční zařízení (FFD – Full Function Device)**. Je zařízení, které podporuje tři operační módy:

1. **PAN (Personal Area Network) koordinátor** – pracuje jako hlavní koordinátor PAN sítě, do které se mohou připojovat ostatní zařízení. V každé PAN síti se může nacházet pouze jedno FFD zařízení, které na sebe přebírá úlohu PAN koordinátora. Účelem tohoto zařízení je monitoring a správa dané sítě. Dále má na starost příjem dat od ostatních zařízení. Ty může zpracovávat nebo dále přeposílat.
2. **Koordinátor** – je zařízení, které nevytváří vlastní síť, ale slouží jako mezičlánek pro komunikaci mezi koncovým zařízením a koordinátorem PAN nebo jiným koordinátorem. Tedy pro přeposílání dat. Vzhledem ke své funkci je také často označován jako směrovač. Dovoluje možnost sestavit libovolnou strukturu PAN. Rovněž může pracovat ve funkci koncového zařízení.
3. **Koncové zařízení** – je zařízení typu RFD. Popsáno viz níže.

**Redukované funkční zařízení (RFD – Reduced Function Device)**. RFD je zařízení, které pracuje s minimální implementací protokolu IEEE 802.15.4. Je určeno pro velmi jednoduché aplikace, jako je vypínač nebo pasivní infračervený senzor. RFD nemá potřebu zasílat velké objemy dat, vzhledem k požadované úspoře energie a dokáže komunikovat pouze s plně funkčním zařízením.

### 2.2.2 Fyzická vrstva (PHY)

Funkcí fyzické vrstvy je umožnit přístup k přenosovému médiu vyšším vrstvám architektury ZigBee. Fyzická vrstva obsahuje základní mechanizmy řízení vysokofrekvenční části. Je zodpovědná za správné zaslání a příjem dat, měří úroveň přijímaného signálu a definuje parametry bezdrátového přenosu. Parametry bezdrátového přenosu jsou použitá frekvence a typ modulace. Standard IEEE 802.15.4 může pracovat na jednom ze tří možných nelicencovaných frekvenčních pásem. 2450 MHz, 915 MHz nebo 868 MHz. Každá z frekvencí se používá pro jinou lokalitu a má tyto přenosové vlastnosti:

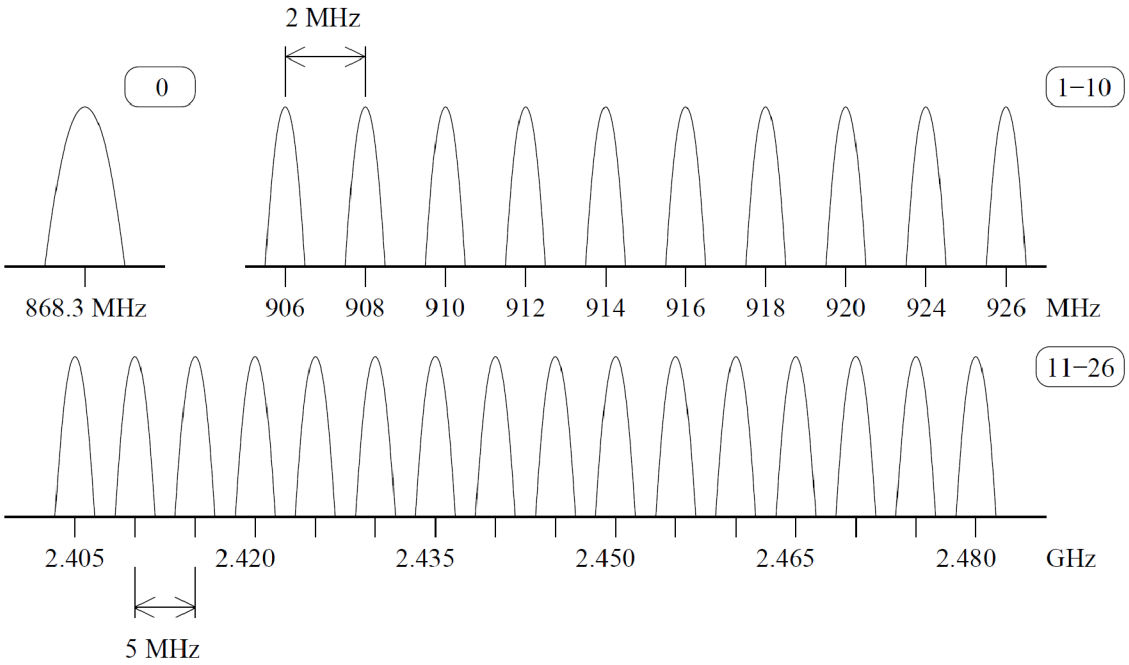
1. pásmo ISM 2,4 GHz – je definováno globálně, má přenosovou rychlost 250 kb/s a využívá 16 přenosových kanálů,

2. pásmo ISM 915 MHz – je definováno pro USA a Austrálii, má přenosovou rychlost 40 kb/s a využívá 10 kanálů,
3. pásmo 868 MHz – je definováno pro Evropu, má přenosovou rychlost 20 kb/s a pracuje na jednom přenosovém kanálu.

Pásmo pracující na frekvenci 2,4 GHz nabízí 16 kanálu ve frekvenčním rozpětí 2400 až 2483,5 MHz. Jako modulace signálu je použita O-QPSK (Offset Quadrature Phase-Shift Keying). Data jsou nejprve rozdělena na 4 bitové symboly a poté mapovány na 32 bitů dlouhé čipy, které jsou modulovány. Vyšší frekvence v tomto případě umožňuje dosáhnout nižší latence a vyšší propustnosti na úkor horších parametrů šíření signálu a potřeby vyšší citlivosti přijímače.

U frekvenčních pásem 915 MHz a 868 MHz se data modulují metodou BPSK (Binary Phase-Shift Keying) a přenáší pomocí DSSS (Direct Sequence Spread Spectrum). První ze zmíněných frekvenčních pásem má rozsah 902 až 928 MHz, druhé 868 až 868,6 MHz. Postup přenosu dat spočívá v diferenciálním zakódování dat, vytvoření čipů dlouhých 15 bitů a následné modulaci. Použité techniky pro přenos signálu zaručují dobrý výkon a minimalizují spotřebu energie. [3], [4], [9], [10], [12].

Přenosové kanály jsou číslovány od 0 do 26. Jednotlivé rozložení kanálů v uvedených frekvenčních pásmech ilustruje obrázek 2.2.




*Obr. 2.2 Rozložení kanálů 0 – 26 ve frekvenčních pásmech 2,4 GHz, 915 MHz a 868 MHz.*

Fyzická vrstva standardu IEEE 802.15.4 má na starosti tyto úkoly:

- aktivace a deaktivace rádiového vysílače,
- detekce energie (ED – Energy Detection) v rámci používaného kanálu,
- indikace kvality linky (LQI – Link Quality Indication)
- výběr volného kanálu (CCA – Clear Channel Assessment).
- výběr frekvence kanálu.

Vysílač nebo taky transceiver může pracovat ve třech režimech. Vysílání, příjem a spánek. Je zapnut nebo vypnut na požadavek vrstvy přístupu k médiu (MAC).

Detekce energie je další funkcí fyzické vrstvy. Detekce energie se používá ke zjištění kvality přijímaného signálu na daném kanále. Přijímaný signál není u detekce energie vyhodnocován, ani dekódován. Délka trvání měření odpovídá intervalu pro přijetí osmi symbolů. Výsledek měření je předán jako osmibitová kladná celočíselná konstanta, typicky síťové vrstvě (NWK). Na síťové vrstvě je tato hodnota použita jako součást algoritmu pro výběr kanálu nebo jako součást CCA mechanizmu pro určení, zda je přenosové médium volné nebo obsazené.

LQI měření zjišťuje poměr síly a kvality přijatých paketů. Měření je možné provádět pomocí přijímače ED, odhadem signálu/šumu nebo kombinací obou technik. Výsledek měření můžou využít vyšší vrstvy ZigBee.

Technika CCA se využívá pro zjištění dostupnosti přenosového média. Je-li volné nebo obsazené. Má 3 operační módy:

1. mód detekce energie – CCA vyhodnotí obsazené médium, pokud je na přenosovém médiu detekována energie nad hranicí prahové hodnoty ED.
2. mód nosné – CCA vyhodnotí obsazené médium, pouze pokud je detekován signál s modulací a rozprostřením charakteristickým pro standard IEEE 802.15.4. Síla signálu může být vyšší nebo nižší než prahová hodnota ED.
3. mód nosné s detekcí energie – jedná se o techniku, které pracuje na obou, výše uvedených principech. Obsazené médium je vyhodnoceno v tom případě, pokud je na něm detekován signál charakteristický pro IEEE 802.15.4 a energie signálu je vyšší než prahová hodnota ED.

### 2.2.3 Vrstva přístupu k médiu (MAC)

Vrstva přístupu k médiu leží na linkové vrstvě. Poskytuje rozhranní mezi fyzickou vrstvou a vyššími vrstvami protokolu. Účelem MAC (Medium Access Control) je vytvářet infrastrukturu sítě a spravedlivě rozdělovat a efektivně sdílet přenosové médium mezi jednotlivými uzly.

Komunikace mezi dvěma sousedními uzly sítě probíhá pomocí takzvaných rámců. Typy rámců jsou čtyři. *Data Frame*, *Acknowledgement Frame*, *MAC Command Frame* a *Beacon Frame*. Využívají se, tak jak jdou postupně za sebou, pro přenos dat, pro potvrzování přijatých rámců, pro konfiguraci koncových uzlů v síti a pro synchronizaci zařízení v síti. Na sestavování rámců se podílí fyzická vrstva i vrstva přístupu k médiu.

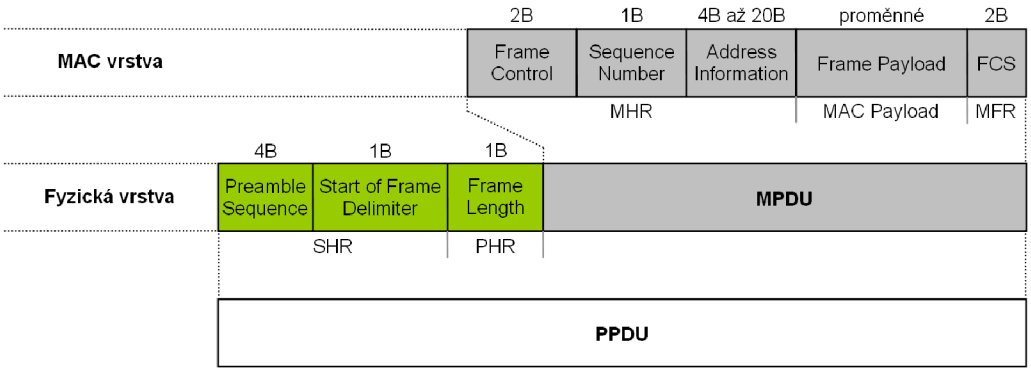
MAC vrstva přidává do rámce část zvanou MPDU (MAC Packet Data Unit). Ta je znázorněna na obrázku 2.3. Sdílenou částí pro všechny typy rámců, až na výjimku, jsou první tři pole MPDU. *Frame Control*, *Sequence Number* a *Address Information*. Označované jako MHD (MAC Header). A poslední pole, FCS (Frame Check Sequence). Označované jako MFR (MAC Footer). Výjimku tvoří pouze potvrzovací rámec.

Pole *Frame Control* je dlouhé 16 bitů. Nese informaci o typu rámce a řídící příznaky. *Sequence Number* následuje bezprostředně za *Frame Control*. Uchovává unikátní číslo pro daný rámec. Pole je velké 8 bitů. Jeho hodnota se používá pro potvrzovanou komunikaci. Třetím polem, které je společné pro všechny typy rámců, vyjma potvrzovacího rámce, je *Address Information*. V tomto poli jsou uloženy čtyři údaje, které definují adresu příjemce a adresu odesílatele. Adresa příjemce je rozdělena na identifikátor cílové PAN (Destination PAN Identifier) a adresu cíle v ní (Destination Address). Identifikátor PAN má velikost 16 bitů a obsahuje jedinečné označení PAN. Adresa cíle může být dlouhá 16 nebo 64 bitů. Záleží na řídícím příznaku *destination addressing* uloženém v poli *Frame Control*. Adresa odesílatele má stejnou strukturu jako adresa příjemce. Mění se pouze význam polí. První ze dvou polí, identifikátor zdrojové PAN (Source PAN Identifier), je jedinečné označení PAN, ze které byl rámec odeslán. Oba dva identifikátory PAN, jak cílové, tak zdrojové, mají význam pouze tehdy, pokud se v jednom prostoru nachází více síti podle standardu IEEE 802.15.4. Druhý údaj uchovává adresu zdrojového uzlu (Source Address), který rámec odeslal. Má velikost 16 nebo 64 bitů. Velikost adresy zdrojového uzlu je závislá na příznaku *destination addressing*. Poslední pole FCS má velikost 16 bitů. Je v něm přenášeno 16 bitové CRC (Cyclic Redundancy Check) [7], [8].

Mezi sdílenými částmi v MPDU je obsah, který je pro každý typ rámce specifický. Označuje se *Frame Payload*. Jeho strukturu a význam v jednotlivých rámcích popisují podkapitoly uvedené níže v této kapitole.

Rámec je jako celek označen PPDU (PHY Packet Data Unit), jak ilustruje obrázek 2.3. První tři pole jsou pole doplněné fyzickou vrstvou. Za nimi pak následuje část doplněná MAC vrstvou popsaná výše. Rámec, doplněný o údaje fyzikou vrstvou, vždy začíná preambulí. Tento prvek slouží pro synchronizaci. Preambule je dlouhá 4 bajty a je složena z 32 logických nul. U každého rámce následuje za preambulí oddělovač začátku rámce (SFD – Start of Frame Delimiter) a má délku 8 bitů. Obsahuje pevnou sekvenci, hodnotu 229 dekadicky. SFD slouží pro oddělení synchronizace od užitečného obsahu rámce. Obě tyto části, preambule a SFD, patří do pole SHR (Synchronization Header). Za tímto polem následuje sedm bitů určujících délku rámce v bajtech. 8 bit je rezervován

pro pozdější účely a tak nevyužit. Toto 8 bitové pole je označováno PHR (PHY Header). Struktura a význam SHR a PHR je pro všechny rámce stejná. [8] [13] [14].




*Obr. 2.3 Struktura rámce.*

Vrstva přístupu k médiu podporuje dva operační módy, které jsou voleny koordinátorem PAN sítě a jsou to:

- Beacon-enabled mód.
- Non Beacon-enabled mód.

**Beacon-enabled mód**

*Beacon* rámce jsou generovány periodicky koordinátorem PAN. Slouží pro synchronizaci připojených zařízení a pro identifikaci PAN. *Beacon* rámec je prvním rámcem takzvaného superrámce (Superframe), který slouží k výměně všech datových rámců mezi jednotlivými uzly v síti a koordinátorem sítě. Přenosy všech zpráv (rámců) jsou uskutečněny během trvání tohoto superrámce.

Pokud koordinátor sítě zvolí *beacon-enabled* mód, začne používat strukturu superrámce pro řízení komunikace mezi jednotlivými zařízeními patřícími do dané PAN. Struktura superrámce je definována koordinátorem a informace o ní je odeslána ostatním zařízením uvnitř *beacon* rámce [8].

**Non Beacon-enabled mód**

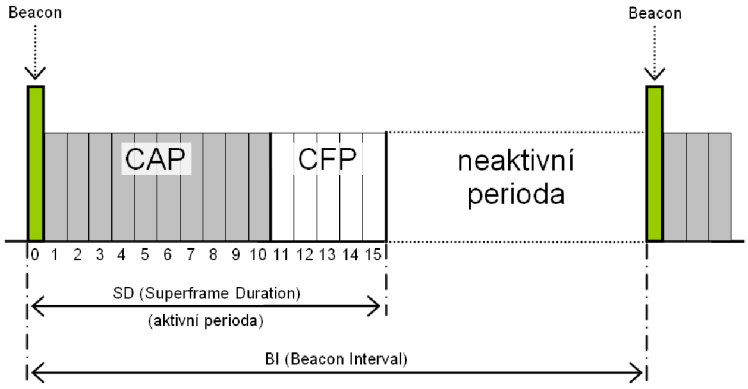
V tomto módu nejsou generovány ani *beacon* rámce a ani superrámce. Komunikace v *non beacon-enabled* módu probíhá prostřednictvím žádosti o zaslání dat. Všechny zprávy, až na výjimky jsou zaslány okamžitě po potvrzení tohoto příkazu. Mezi výjimky patří potvrzovací rámce a některé datové rámce. Každé zařízení v síti může vyslat své data použitím neslotovaného CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) mechanizmu. [3], [4], [8].

**Struktura superrámce**

Superrámec je konstrukce využívaná pro zasílání zpráv v *beacon-enabled* módu (viz předchozí text). Jedná se o časové pásmo rozdělené do menších časových úseků, zvaných sloty. Strukturu superrámce (viz Obr. 2.4) určuje koordinátor sítě. Použitím této techniky vznikají v komunikaci velmi dlouhé mezery, což má za následek velmi nízkou spotřebu. Jednotlivé superrámce jsou mezi sebou odděleny *beacon* rámcem. *Beacon* rámec je úvodní rámec každého superrámce a má za účel synchronizaci. Dále identifikuje PAN, definuje strukturu superrámce a přiděluje GTS (Guaranteed Time Slot) pole. BI (Beacon Interval) z obrázku 2.4 udává dobu trvání celého superrámce. Jeho hodnota je dána konstantou *aBaseSuperframeDuration* a parametrem BO (Beacon Order). Časové sloty se vyskytují v části aktivní periody (SD – Superframe Duration) a je jich 16. Sloty v aktivní periodě jsou rozděleny do dvou bloků. CAP (Contention Access Period) a CFP (Contention Free Period). [7], [11].

CAP následuje bezprostředně za *beacon* rámcem a je přenášena slotovanou CSMA/CA metodou. Jakékoliv zařízení v síti může využít služby CAP. Například nové zařízení, které se chce připojit k síti. Zařízení, které nestihne vyslat své data během tohoto časového úseku, musí vyčkat na další vysílání superrámce.

CFP následuje za CAP. Je složena z několika GTS. GTS slotů může být minimálně 0 a maximálně 7. Jsou alokovány koordinátorem PAN sítě. Každý GTS slot může obsadit několik základních časových slotů z CFP. GTS sloty jsou využívány pomalými (*low-latency*) a prioritními zařízeními.




*Obr. 2.4 Příklad struktury superrámce.*

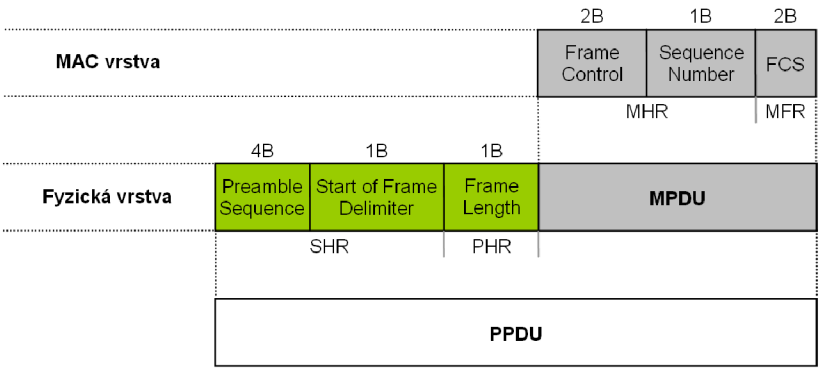
Vysílání superrámce se může opakovat v intervalech 15 ms až 252 s [7]. Pro vlastní komunikaci se využívají již zmíněné čtyři typy rámců. *Data Frame*, *Acknowledgement Frame*, *MAC Command Frame* a *Beacon Frame*.

### Data Frame

*Data Frame*, nebo-li datový rámec je rámec, jehož funkcí je přednos užitečné informace. Strukturu datového rámce vychází z obrázku 2.3. Pole *Frame Payload* je pouze nahrazeno polem *Data Payload*. Maximální velikost přenášených dat je 104 bajtů na jeden rámec. Hodnota *Frame Type*, která definuje typ rámce v poli *Frame Control*, musí být v tomto případě nastavena na 0x1. Data jsou předána MAC vrstvě vyšší vrstvou protokolu ZigBee s žádostí o zaslání.

### Acknowledgement Frame

Nebo taky potvrzovací rámec (viz Obr. 2.5), je rámec pro potvrzovanou komunikaci. Jeho struktura je značně odlišná od ostatních rámců definovaných standardem IEEE 802.15.4. Rámec je složen pouze z polí *Frame Control*, *Sequence Number* a FCS. Pole *Sequence Number* obsahuje pořadové číslo rámce, pro které je potvrzovací rámec zaslán.




*Obr. 2.5 Acknowledgement Frame.*

### MAC Command Frame

Je příkazový rámec MAC vrstvy. Pomocí něj lze konfigurovat koncová zařízení a uzlů nezávisle na jejich typu. Strukturu celého rámce vychází z referenční struktury na obrázku 2.3. Pole *Frame Payload* bylo nahrazeno dvěma separátními poli. První určuje typ příkazu (Command Type) a druhé jeho hodnotu (Command Payload). Velikost těchto dvou polí nesmí dohromady přesáhnout 104 bajtů.

### Beacon Frame

*Beacon* rámec je úvodní rámec každého superrámce. Jeho hlavní úlohou je synchronizace zařízení v síti s vysíláním tohoto rámce. *Beacon* rámec nese informaci o struktuře superrámce, GTS polích a nevyřízených transakcích se zařízeními v síti. Tyto údaje jsou uloženy ve čtyřech rozdílných polích, které nahrazují pole *Frame Payload* z obrázku 2.3. Jsou to pole *Superframe Specification*, *GTS fields*, *Pending Address* a *Beacon Payload*. *Beacon* rámec může být zaslán pouze koordinátorem PAN v *beacon-enabled* módu. V proměnné *Frame Type* je specifikován hodnotou 0x0.

## 2.3 ZigBee

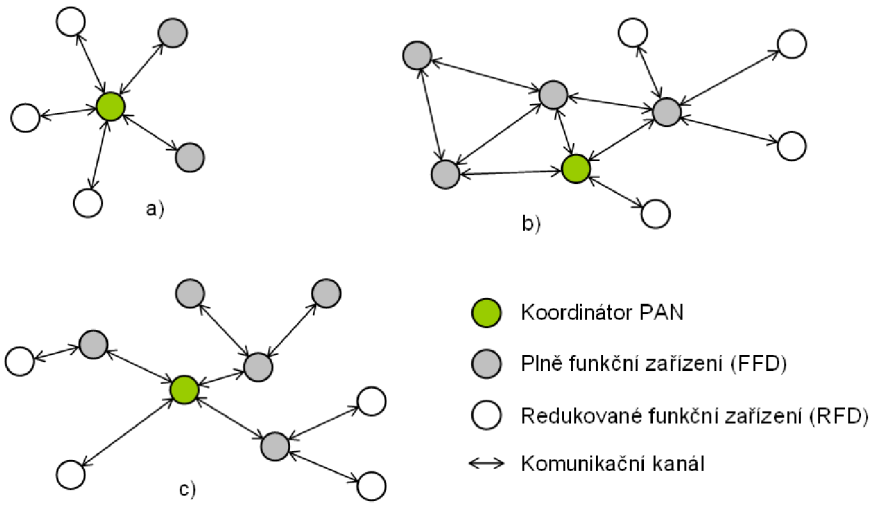
Specifikuje síťovou (NWK) a aplikační (APL) vrstvu. Ty definuje a spravuje organizace ZigBee Alliance. Aplikační vrstva je složena z podpůrné aplikační podvrstvy, ZigBee objektů a z aplikačních objektů definovaných výrobci. Poskytuje rovněž zabezpečení přenášených dat [1].

### 2.3.1 Síťová vrstva (NWK)

Síťová vrstva poskytuje rozhranní mezi aplikační vrstvou standardu ZigBee a MAC vrstvou standardu IEEE 802.15.4. Jejím účelem je připojování nových zařízení k síti nebo naopak, odebírání stávajících zařízení ze sítě. Síťová vrstva se dále stará o aplikaci zabezpečovacích mechanizmů na rámce a směrování rámců k požadovaným uzlům. Jejím účelem je také hledat cesty k jednotlivým zařízením v rámci celé sítě a tyto cesty uchovávat v paměti. [1], [2], [13].

**Topologie sítě**

Standard ZigBee definuje 3 typy topologie sítí. Ty jsou znázorněny na obrázku 2.6. Základní topologií je typ hvězda (Star). Ta se skládá z centrálního zařízení, které přebírá funkci koordinátora sítě. Zbylé zařízení tvoří koncové nody, které komunikují přímo s koordinátorem sítě. Druhá topologie je označována jako stromová topologie (Tree). Vlastností této architektury je, že koncové zařízení, ať už plně funkční zařízení (FFD) nebo zařízení s redukovanou funkcí (RFD), nemusí komunikovat přímo s koordinátorem sítě. Pro takovou komunikaci využívají zařízení FFD ve funkci směrovače. Stromová architektura tak umožňuje prodloužit vzdálenost mezi koncovým zařízením a koordinátorem. Poslední topologií je kombinace obou předchozích (Mesh). Dovoluje tak sestavení libovolné struktury sítě [14].




*Obr. 2.6 Topologie a) hvězda (Star), b) polygon (Mesh), c) strom (Tree).*

### 2.3.2 Aplikační vrstva (APL)

Aplikační vrstva standardu ZigBee se skládá z podpůrné aplikační podvrstvy (APS), objektů ZDO (ZigBee Device Objects), aplikačních objektů a zabezpečení.

Podpůrná aplikační podvrstva je zodpovědná za údržbu tabulek pro spojení a přeposílání zpráv. Rovněž tvoří rozhranní mezi nižší síťovou vrstvou a vyšší aplikační vrstvou. Objekty ZDO ustanovují roli ZigBee uzlů. Dále se starají o inicializaci nebo odpovídání na požadavky týkající se navázání spojení. Určují bezpečnostní vztahy, jako jsou veřejné a symetrické klíče a využívají se pro hledání ostatních zařízení v síti. Aplikační objekty jsou stěžejní pro vývojáře. Určují formát zpráv a zpracování akcí, které umožňují vývojářům vytvářet interoperabilní a distribuované aplikace. Aplikační profily umožňují aplikacím zasílat nebo příjmat data a zpracovávat příkazy. [1], [2], [5].

### 2.3.3 Komunikace v síti ZigBee na úrovni aplikační vrstvy a síťové vrstvy

Kapitola popisuje reálnou komunikaci v síti ZigBee mezi aplikační a síťovou vrstvou. Je uvedena především proto, aby si čtenář udělal představu o tom, jak probíhá dorozumívání mezi jednotlivými vrstvami protokolu. Kapitola se zaměřuje především na vytvoření sítě koordinátorem a připojení uzlu do této sítě. Zbylé komunikační schémata s popisem komunikace na více vrstvách a v ostatních situacích, které uvádí tabulka 2.1, lze nalézt v použité literatuře [1], [3], [8].

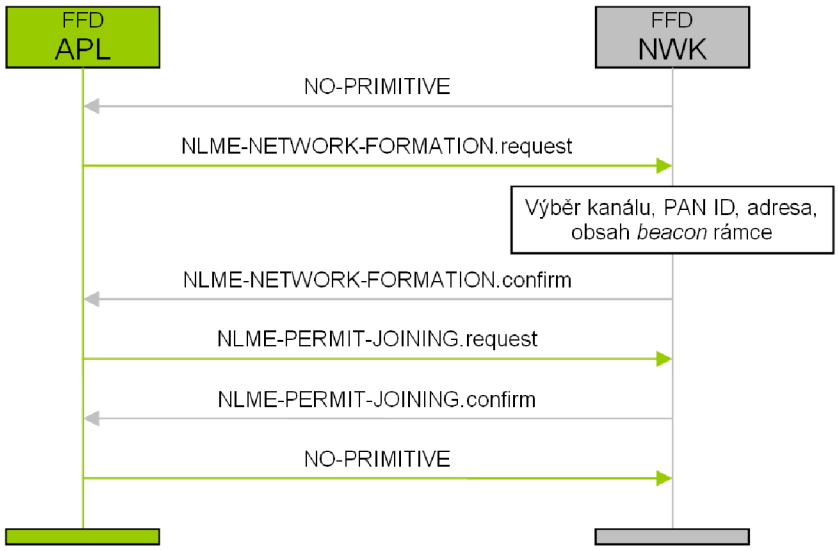
| krok | Koordinátor PAN | RFD/FFD |
|---|---|---|
| **1.** | Vytvoření sítě | Vyhledávání sítě |
| **2.** | Povolení přístupu do sítě | |
| **3.** | Objevení zařízení | Pokus o připojení k síti |
| **4.** | Navázání spojení a určení způsobu komunikace | |
| **5.** | Výměna dat | |
| **6.** | Událost o odpojení zařízení | Odpojení ze sítě |

Tab. 2.1 Postup vytvoření sítě a navázání spojení mezi koordinátorem PAN a koncovým zařízením.

### Vytvoření sítě

PAN může být vytvořena pouze FFD zařízením ve funkci koordinátora. Aby bylo zařízení schopné vytvořit síť, nesmí být připojeno k žádné jiné síti. Procedura k sestavení nové PAN je iniciována skrze parametr *NLME-NETWORK-FORMATION.request* na žádost aplikační vrstvy (viz obr. 2.7). Žádost je potvrzena síťovou vrstvou, která vrací parametr *NLME-NETWORK-FORMATION.confirm*. V případě, že u zařízení nebyly splněny podmínky pro vytvoření nové sítě, je nastaven chybový příznak. V opačném případě se provede skenování dostupných přenosových kanálů, nastavení identifikátoru PAN a nastavení 16 bitové adresy PAN koordinátoru.

Dalším krokem inicializace sítě je žádost o povolení připojovat nové zařízení k síti. Žádost je vytvořena parametrem *NLME-PERMIT-JOINING.request*, který je zaslán síťové vrstvě. Proces je zobrazen na obrázku 2.7. Kromě koordinátora PAN může do sítě připojovat nové uzly i zařízení s funkcí směrovače, u kterého musí proběhnout stejná žádost o povolení. Ta je potvrzena síťovou vrstvou a parametrem *NLME-PERMIT-JOINING.confirm*. [1].

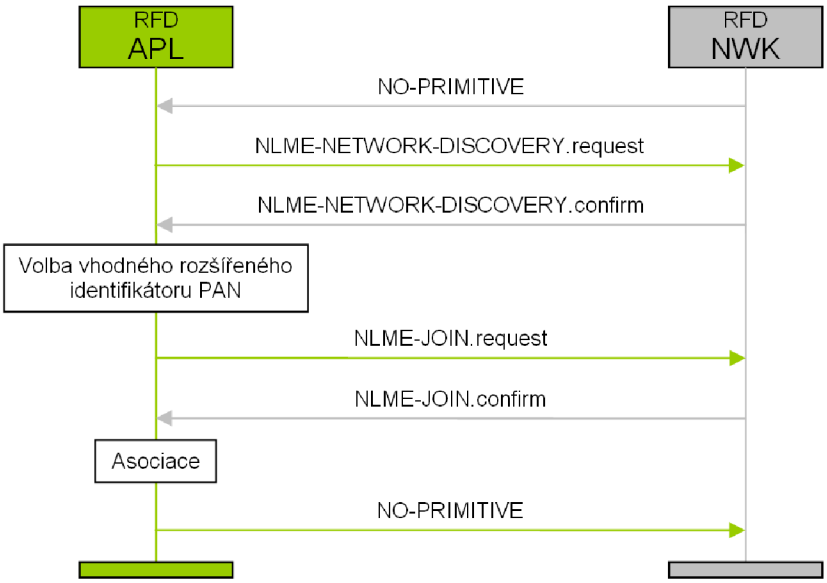



*Obr. 2.7 Schéma komunikace mezi APL a NWK při sestavování sítě.*

### Připojení uzlu do sítě

Pokud se chce zařízení připojit do již existující sítě, musí se asociovat. Proces je započat zasláním požadavku o připojení do sítě síťové vrstvě (viz obr. 2.8). Síťová vrstva posléze předá požadavek nižším vrstvám standardu IEEE 802.15.4. Tyto vrstvy provedou aktivní nebo pasivní sken dostupných kanálů. Nalezené sítě jsou aplikační vrstvě potvrzeny parametrem *NLME-NETWORK-DISCOVERY.confirm*. Zároveň jsou předány informace o nalezených sítích, jako je přenosový kanál, identifikátor PAN a rozšířená a krátká adresa rodičovského zařízení. Aplikační vrstva provede výběr vhodné sítě a předá požadavek na připojení síťové vrstvě prostřednictvím parametru *NLME-*

*JOIN.request*. Síťová vrstva pak nižším vrstvám. Nastává proces asociace. Ten je potvrzen na aplikační vrstvě přijetím parametru *NLME-JOIN.confirm* s příznakem úspěchu. [1].




*Obr. 2.8 Schéma komunikace mezi APL a NWK pro vyhledání a připojení uzlu k dostupné PAN.*

## 2.4 Zabezpečení na jednotlivých vrstvách

Bezpečnost v senzorových sítích je důležitá hned z několika důvodů. Bezpečnost v senzorových sítích by měla zaručovat spolehlivý přenos dat skrze síť tak, aby nedocházelo ke ztrátě dat, nebo chybám v přenášených datech. Nemělo by docházet ke kolizi s jinou PAN. Síť by měla být chráněna proti náhodným signálům. Použití zabezpečení by dále nemělo umožnit neoprávněné vniknutí do sítě nebo zcizení dat útočníkem [16].

Standard ZigBee a IEEE 802.15.4 řeší možné problémy s útoky na síť a přenosem dat hned několika způsoby. Každá vrstva těchto dvou standardů obsahuje určité zabezpečovací mechanizmy k dosažení požadovaných bezpečnostních a ochranných vlastností. Bezpečnost je základní výhodou tohoto standardu na poli senzorových sítí.

Podkapitoly se stručně zabývají zabezpečením na jednotlivých vrstvách protokolu IEEE 802.15.4/ZigBee.

### 2.4.1 Zabezpečení na fyzické vrstvě

Pro zvýšení spolehlivosti přenosu dat se na fyzické vrstvě používá technika přímého rozprostřeného spektra (DSSS – Direct Sequence Spread Spectrum). Je jednou z metod pro šíření spektra v bezdrátové komunikaci. Zavádí u přenášených dat redundanci. DSSS je založeno na principu nahrazení jednotlivých bitů početnější sekvencí bitů. Takzvaných chipů, které se pak přenášejí vzduchem. Chipy mají nejčastěji pseudonáhodný charakter. Signál je tak rozprostřen do větší části rádiového spektra a při přenosu se jeví jako šum. Metoda DSSS zajišťuje u přenášeného signálu menší náchylnost na rušení, čím zvyšuje spolehlivost přenosu [17].

### 2.4.2 Zabezpečení na vrstvě přístupu k médiu

Specifikace IEEE 802.15:4 dovoluje na této vrstvě použít tři bezpečnostní režimy. Nezabezpečený režim, režim s přístupovými seznamy a zabezpečený režim.

MAC vrstva zavádí hned několik řešení pro spolehlivost a zabezpečení sítě a přenášených dat. Pro spolehlivost přenosu dat přidává MAC vrstva do přenášených rámců takzvaný MIC (Message Integrity Code). Tento ochranný mechanizmus zajišťuje integritu rámce. Podle potřeby síly zabezpečení může nabývat délky 32, 64 nebo 128 bitů. Používá se už v základním režimu zabezpečení. Tedy v nezabezpečeném režimu.

Dalším bezpečnostním prvkem je čítač rámců (Frame Count) a sekvenční čítač (Key Sequence Count). Oba dva jsou u místěny v rámcích vytvářených MAC vrstvou. Konkrétně v části *Frame Payload*. Čítač rámců je inkrementován o hodnotu 1 pokaždé, když je přenášen takto zabezpečený rámec. Tímto mechanizmem je zajištěna spolehlivost doručení rámců ve správném pořadí a odmítání rámců, které se opakují. Sekvenční čítač rámců je stanoven vyššími vrstvami protokolu IEEE 802.15.4/ZigBee. Lze jej například použít, pokud je počítadlo rámců vyčerpáno. Je-li vytvořen nový šifrovací klíč, sekvenční čítač rámců se nuluje. [3], [16].

V režimu s přístupovými seznamy se používá u každého zařízení tabulka ACL (Access Control List). Každý záznam v tabulce obsahuje adresu cíle a informaci o stupni zabezpečení. Tabulka může mít až 255 záznamů. Doporučuje se, aby všechna zařízení v PAN měla stejný stupeň zabezpečení. ACL například obsahuje hodnotu posledního přijatého čítače rámců nebo sekvenčního čítače. Zařízení si v režimu s přístupovými seznamy povolují přístup pouze na základě svých adres. Pokud cílové zařízení má uloženou adresu zdrojového zařízení v ACL, příjme jeho data a aktualizuje si pole čítače rámců a sekvenčního čítače. V opačném případě je zpráva zamítnuta. ACL je zavedena i v zabezpečeném režimu s kryptografickou ochranou. Při volbě tohoto typu zabezpečení jsou v ACL uloženy i symetrické klíče.

Nejvyšším stupněm zabezpečení ve specifikaci IEEE 802.15.4 je zabezpečený režim podporující šifrování odchozích i příchozích rámců. IEEE 802.15.4 uvádí několik pracovních módů

šifry. Každý mód má jiné vlastnosti a rozdílné zabezpečení. Jednotlivé módy jsou uvedeny v tabulce 2.2.

| Identifikátor | Název zabezpečení | Služby zabezpečení | | | |
|---|---|---|---|---|---|
| | | Kontrola přístupu | Šifrování | Integrita zpráv | Sequential Freshness |
| 0x00 | Žádné | | | | |
| 0x01 | AES-CTR | X | X | | X |
| 0x02 | AES-CCM-128 | X | X | X | X |
| 0x03 | AES-CCM-64 | X | X | X | X |
| 0x04 | AES-CCM-32 | X | X | X | X |
| 0x05 | AES-CBC-MAC-128 | X | | X | |
| 0x06 | AES-CBC-MAC-64 | X | | X | |
| 0x07 | AES-CBC-MAC-32 | X | | X | |

*Tab. 2.2 Bezpečnostní mechanizmy definované standardem IEEE 802.15.4 [3].*

Kontrola přístupu využívá autentizaci. Používá se tehdy, pokud si chce zařízení ověřit identitu jiného zařízení, se kterým chce komunikovat. Aby tento princip mohl fungovat, musí každé zařízení mít seznam ACL. Šifrování je metoda ochrany dat pomocí symetrické šifry. Data mohou být zašifrována sdíleným klíčem mezi skupinou zařízení nebo klíčem sdíleným pouze mezi dvěma uzly, typicky uloženým v ACL. Šifrování je možné použít pouze na datové rámce, *beacon* rámce a příkazové rámce MAC vrstvy. Ne však na potvrzovací rámce. Podpora integrity zpráv byla již popsána v předešlých odstavcích. Pro připomenutí se jedná o využití kryptografického kontrolního součtu (MIC) pro ochranu zpráv bez použití šifrování. Použitelnost na typy rámců je stejná, jako u šifrování. Pouze potvrzovací rámce nepoužívají integritní kódy. Integritní kód bývá uložen přímo v zařízení nebo v ACL. *Sequential Freshness* je bezpečnostní služba, která chrání zařízení před útoky založenými na odpovědi. U přijatého rámce se porovná *freshness* hodnota s poslední známou přijatou *freshness* hodnotou. Pokud je *freshness* hodnota novější, než poslední známá, rámec je přijat a *freshness* hodnota aktualizována. Jinak je rámec zamítnut.

Režim AES-CTR se používá pouze v zabezpečeném režimu a zajišťuje aktuálnost a důvěrnost přenášených dat. Odesílaná zpráva je rozdělena na bloky o velikosti 16 bajtů. Šifrování v tomto módu je zajištěno operací XOR, která se provede na jednotlivé bloky nezašifrované zprávy a výstup algoritmu AES. Čítač rámce je složen z adresy odesílatele, statické výplně, čítače rámce, sekvenčního čítače klíče a čítače bloku. Zároveň plní roli inicializačního rámce. Všechny dílčí čítače jsou průběžně aktualizovány. Dešifrování probíhá analogicky. Přijímací strana kontroluje stavy všech čítačů a tím detekuje případné útoky [16].

AES-CCM pokrývá všechny možnosti zabezpečení, které uvádí standard IEEE 802.15.4. Používá kombinaci módu AES-CTR, popsaného výše a AES-CBC-MAC, popsaného níže.

Mód AES-CBC-MAC podporuje integritu zpráv a kontrolu přístupu. Odesílaná zpráva je rozdělena do bloků. Při šifrování každého bloku se používá blok předcházející. Pro první blok se používá iniciační vektor. Výsledkem tohoto mechanizmu je kryptografický kontrolní součet MIC. MIC je přenášen v otevřené podobě. Kontrola se provede tak, že příjemce si vypočte svůj MIC a porovná ho s přijatým. Na základě výsledku je zpráva přijata nebo zamítnuta [16].

### 2.4.3 Zabezpečení na síťové vrstvě

Síťová vrstva nepoužívá žádné šifrování, ani kontrolní součty. Má na starosti spolehlivost sítě. Tedy její řízení. V její kompetenci je správné zasílání a příjmení rámců. Dále zajišťuje správné připojování zařízení do sítě. Nebo odpojování zařízení od sítě. Mezi nejnebezpečnější útoky na senzorové sítě patří právě napadení směrovacích protokolů [1].

### 2.4.4 Zabezpečení na aplikační vrstvě

Aplikační vrstva standardu ZigBee zajišťuje správu kryptografických klíčů a je zodpovědná za správný přenos zašifrovaných dat. Bezpečnost na aplikační vrstvě je řízena pomocí centrálního zařízení, takzvaného *Trust Center*. V PAN se může nacházet pouze jedno *Trust Center*. Většinou je to koordinátor PAN. *Trust Center* se používá k distribuci síťových klíčů všem uzlům a pro údržbu síťového klíče. Také řídí přístup zařízení do sítě. Může pracovat ve dvou režimech:

- Rezidenční režim (Residential Mode).
- Komerční režim (Commercial Mode).

V rezidenčním režimu je používán pro šifrování a dešifrování zpráv pouze jeden klíč. A to síťový (Network Key). Rezidenční režim se používá pro sítě, u kterých není potřeba vysoké míry zabezpečení. Výhodou jsou nízké nároky na paměť, *Trust Center* a samotnou komunikaci mezi uzly. Nevýhodou je naopak nižší úroveň zabezpečení. Údržba klíčů a jejich aktualizace není v tomto režimu podporovaná.

Komerční režim oproti rezidenčnímu podporuje vysokou míru zabezpečení. Pro komunikaci mezi zařízeními jsou používány všechny klíče, které standard ZigBee specifikuje. Těmi jsou master klíč (Master Key), linkový klíč (Link Key) a síťový klíč (Network Key). Výhodou je centralizovaná distribuce kryptografických klíčů a jejich aktualizace. Nevýhodou pak vyšší paměťová náročnost a vyšší nároky na *Trust Center* a komunikaci.

Všechny tři uvedené typy klíčů můžou být přednastaveny už z výroby. Pokud tomu tak není, jsou mezi uzly distribuovány technikou *Key Transport* nebo *Key-establishment*. [1], [16]

# 3 Návrh bezdrátového hlasovacího systému

Kapitola představuje stěžejní bod řešení projektu. Špatný návrh může vést k pozdějším komplikacím při implementaci. Dobrý návrh naopak k usnadnění řešení projektu. Proto se celá kapitola snaží přinést co nejspecifičtější pohled na daný problém. Dále navrhuje možné řešení a postupy pro pozdější realizaci projektu. Snaží se v případě možnosti použití více vhodných postupů a metod vybrat ten nebo tu nejvhodnější.

## 3.1 Stručný úvod do hlasování

Nejznámějším a nejčastěji používaným hlasováním je hlasování na internetu. Často jsou tímto způsobem realizovány různé ankety, hlasování o nejoblíbenější skupinu, písničku, film, článek, produkt a spoustu dalšího. Tento způsob lze využít ovšem i k důležitějším událostem významným pro celý stát. Předpokládá se například využití hlasování po internetu k volbě prezidenta, pro volby do poslanecké sněmovny nebo evropského parlamentu.

Daleko specifičtější elektronické hlasovací systémy jsou hlasovací systémy v radách měst a obcí, firmách, školách, na valných shromážděních nebo třeba v poslanecké sněmovně. Tyto systémy by měli vykazovat uživatelskou přívětivost, spolehlivost a jistou míru zabezpečení, podle důležitosti.

Elektronické hlasovací systémy, podle použití přenosového média, je možné rozdělil do dvou skupin. První jsou ty, které využívají pro přenos informace fyzické médium. Buď metalické, nebo optické. Dnes je dostupná spousta standardů, které způsob přenosu dat po tomto typu média umožňují. Například Ethernet, RS232, Profibus a spousta dalších. Druhou skupinou jsou ty, které využívají pro přenos informace bezdrátové prostředí. Tento typ přenosu pokrývají standardy jako Wi-Fi, Bluetooth, IrDA nebo ZigBee. Výhodou bezdrátového přenosu je mobilita a jednoduchost instalace. Nevýhodou je pak rušení vysílaného signálu nebo možnosti napájení.

Princip hlasování, sběru hlasů a jejich vyhodnocení je často v celé své architektuře rozdělen na komponenty, kdy každá z nich plní svojí specifickou úlohu. Architektura hlasovací sítě je většinou složena ze samotných hlasovacích zařízení. Tím může být již zmíněný osobní počítač nebo speciální zařízení navržené jenom k tomuto účelu. Tyto generované data jsou v sítí hlasovacích zařízení shromažďovány takzvanou centrální jednotkou, která hlasy zpracovává. Může jím být například server, PLC (Programming Logic Controller) nebo jiné zařízení, které na sebe dokáže tuto funkci převzít. Zobrazení výsledků je pak exportováno na výstupní periferii, jako je monitor, tiskárna, grafický panel nebo na web.

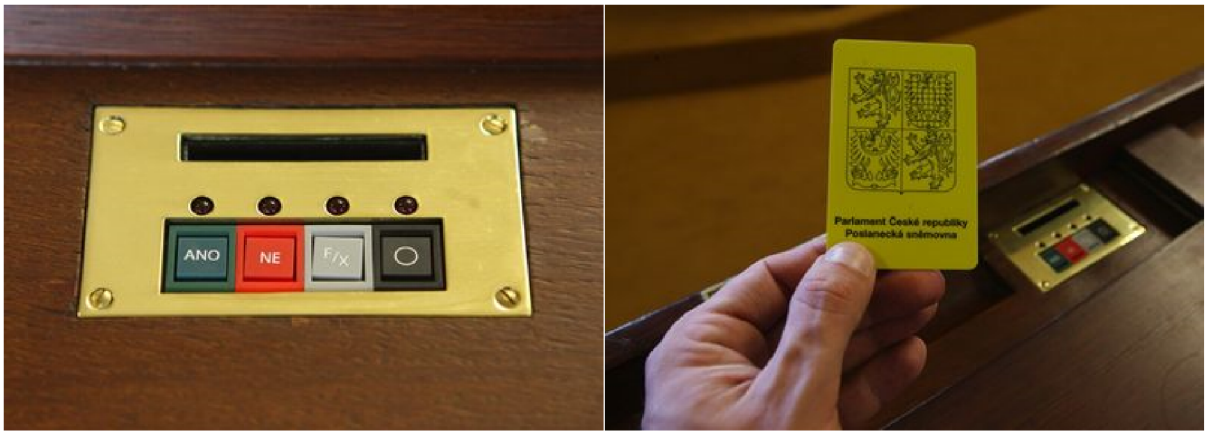
### 3.1.1 Hlasovací zařízení PS PČR

Výrobou hlasovacích zařízení se zabývá řada firem po celém světě. Kapitola a její obsah se zaobírá uplatněním hlasovacích zařízení v praxi. Pro příklad byl vybrán elektronický hlasovací systém používaný v PS PČR (Poslanecké Sněmovně Parlamentu České Republiky).

Elektronický hlasovací systém byl poprvé v poslanecké sněmovně parlamentu České republiky nainstalován v září roku 2003. Dodavatelem byla americká firma Daktronics. Do té doby probíhalo hlasování zvednutím ruky, kdy příslušné hlasy sčítaly pověřené skrutátorky. Zařízení pracovalo na operačním systému Microsoft MS-DOS. Jakékoliv rozšiřování systému nebo jeho údržba byla komplikovaná.

V září 2008 byl zprovozněn nový hlasovací systém. Dodavatelem byla společnost ELVAC IPC s.r.o. Jednalo se o rekonstrukci stávajícího systému. Předmětem rekonstrukce byla výměna centrální jednotky hlasovacího systému a doplnění hlasovacího systému o informační LED zobrazovače. Požadavkem na realizaci bylo zachování sítě hlasovacích konzol (viz obr. 3.1) a zachování veškeré funkčnosti stávajícího systému.

Řídící jednotkou nového zařízení jsou dva servery běžící na operačním systému Linux. Jeden server je vždy aktivní. Druhý slouží jako záloha v případě poruchy prvního serveru. Server řídí sběr dat z hlasovacích uzlů a obsluhuje tiskárny, klientské stanice a LED displeje v obou hlasovacích místnostech poslanecké sněmovny. Zároveň zajišťuje komunikaci s intranetem. Systém je postaven na architektuře klient-server, kdy na serveru běží terminálová konzole. Ta se využívá pouze pro údržbu systému. Na klientských stanicích je pak spuštěná grafická nadstavba. Komunikace, kromě hlasovacích zařízení, probíhá po klasickém ethernetu. Servery jsou před výpadkem elektrické energie chráněny pomocí záložního zdroje UPS (Uninterruptible Power Supply). Obslužný software je navržen a implementován v programovacím jazyku Java. Důvodem je stabilita, přenositelnost jazyku mezi operačními systémy a možná pozdější rozšiřitelnost. [18].




*Obr. 3.1 Hlasovací zařízení poslanecké sněmovny parlamentu ČR a karta pro hlasování.*

Princip hlasování je založen na výběru z možností:

- Ano
- Ne
- Zdržel se hlasování.

Pro každou volbu je jedno tlačítko. Zabezpečení a zároveň spuštění hlasovacího zařízení je zajištěno pomocí speciální karty, která je zobrazena na obrázku 3.1. Po vložení karty je hlasovací zařízení aktivováno a zároveň je povolena možnost hlasovat. Výsledky jsou zobrazovány na informačních LED displejích. Forma zobrazení je navržena tak, aby byla co nejvíce přehledná. Na displeji se zobrazují kromě celkových výsledků hlasování také projednávané body, jejich přesnější popis, pořadí přihlášených poslanců a podrobnější rozdělení hlasů podle politických stran.

## 3.2 Vývojový kit

Pro realizaci a testování projektu je k dispozici vývojový kit Freescale 1321xNSK-BDM [19]. Vývojový kit obsahuje dvě rozdílné zařízení a to:

- 1321x-Sensor Reference Board (SRB)
- 1321x-Network Coordinator Board (NCB).

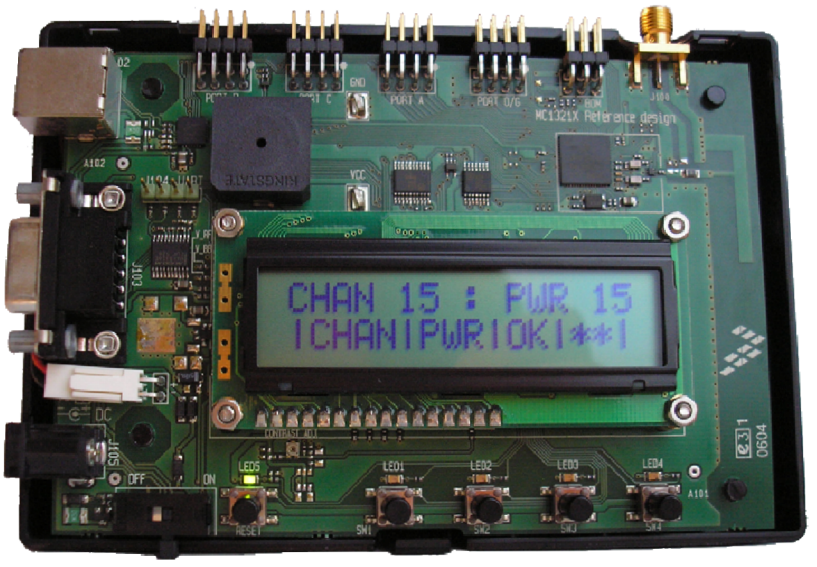
### 3.2.1 Network Coordinator Board

1321x-NBC (viz obr. 3.2) je vývojová deska kompatibilní s protokolem IEEE 802.15.4/ZigBee. Je postavena na čipu MC13213 s vysílačem pracujícím v ISM pásmu 2,4 GHz. Pro propojení s PC má modul integrované dvě rozhranní. USB a RS232. Blokové schéma je zobrazené na obrázku 3.3.

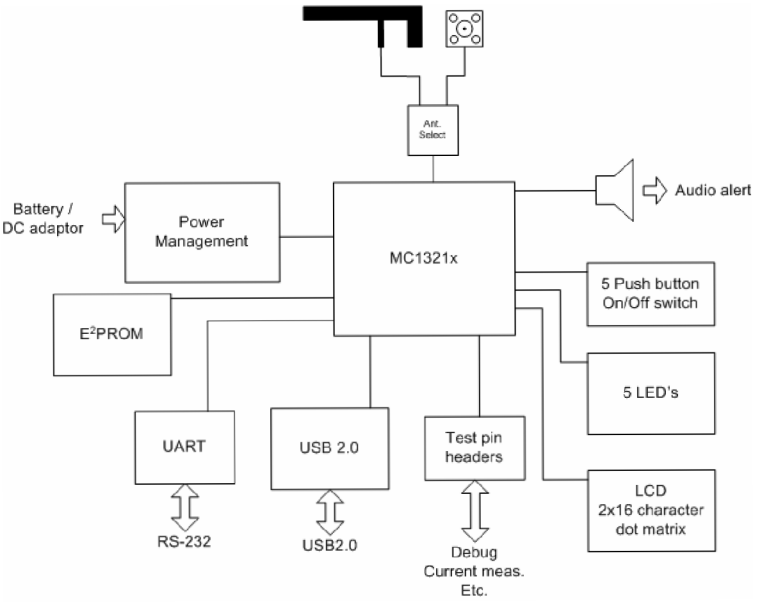
Součástí modulu 1321x-NBC je:

- USB 2.0 konektor
- RS 232 konektor
- Vypínač (pro přepínání stavů ON/OFF)
- Resetovací tlačítko
- 4 tlačítka (SW1, SW2, SW3, SW4)
- 5 LED (LED 1, LED 2, LED 3, LED 4, LED 5)
- Dvouřádkový maticový LCD displej s 32 znaky
- Napájecí konektor pro 5 – 9 V DC
- Držák pro dvě napájecí AA baterie

- Vestavěná anténa
- Konektor SMA RF pro připojení externí antény
- 4 osmi pinové porty pro připojení externích periferií k mikrokontroléru
- 2x 3 pinový BDM (Background Debug Module) konektor pro programování flash paměti a debug prostřednictvím USB Multilink modulu.



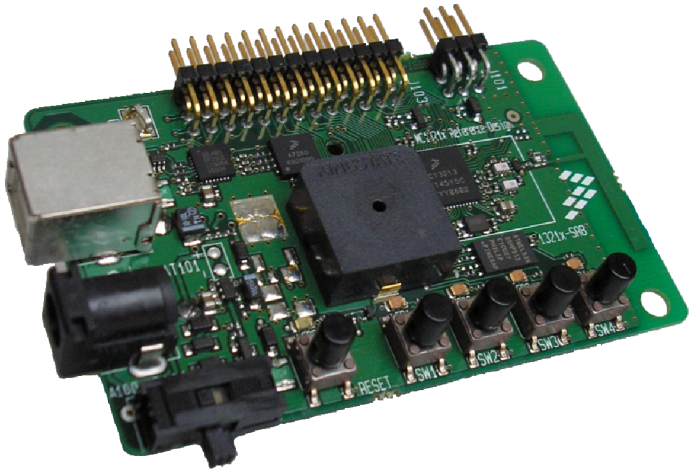

*Obr. 3.2 Vývojová deska 1321x-NBC.*



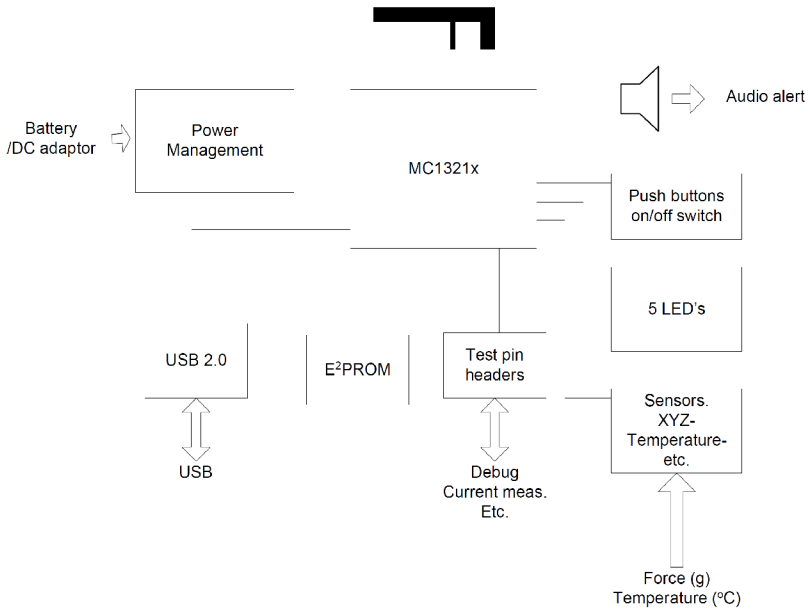

*Obr. 3.3 Blokové schéma vývojové desky 1321x-NBC [19].*

### 3.2.2 Sensor Reference Board

1321x-SRB (viz obr. 3.4) je malý kompaktní modul kompatibilní s protokolem IEEE 802.15.4 a ZigBee. Základem je čip MC13213, který pracuje ve frekvenčním ISM pásmu 2,4 GHz a. Oproti desce 1321x-NBC postrádá rozhranní RS 232, maticový LCD displej a některé další vstupní prvky. Blokové schéma je zobrazeno na obrázku 3.5.



*Obr. 3.4 Vývojová deska 1321x-SRB.*




*Obr. 3.5 Blokové schéma vývojové desky 1321x-SRB [19].*

Součástí modulu 1321x-SRB je:

- USB 2.0 konektor
- Vypínač (pro přepínání stavů ON/OFF)
- Resetovací tlačítko
- 4 tlačítka (SW1, SW2, SW3, SW4)
- 5 LED (LED 1, LED 2, LED 3, LED 4, LED 5)
- Napájecí konektor pro 5 – 9 V DC
- Držák pro dvě napájecí AA baterie
- Vestavěná anténa
- 26 pinový konektor pro připojení externích periférií k mikrokontroléru
- 2x 3 pinový BDM (Background Debug Module) konektor pro programování flash paměti a debug prostřednictvím USB Multilink modulu.

### 3.2.3 Čip Freescale MC13213 SiP

MC13213 SiP (System in Package) zahrnuje 8 bitový mikrokontrolér MC9S08GT s vysílačem MC1320x na jediném čipu. Čip má rozměry 9mm x 9mm x 1mm a celkem 71 pinů. Teplotní pracovní rozsah je od -40°C až do +85°C.

Mikrokontrolér spadá do rodiny HCS08. K dispozici je 60 KB flash paměti a 4KB paměti RAM. Má dedikované SPI (Serial Peripheral Interface) vnitřně připojené k modemu. Dále dvě nezávislé sériové komunikační rozhranní s maximální přenosovou rychlostí 115200 Baudů. Vysílač MC1320x je plně kompatibilní se standardem IEEE 802.15.4. Pracuje ve frekvenční ISM pásmu 2,4 GHz na 16 kanálech po 5 MHz. Síla výstupního signálu je škálovatelná. Nabízí přenosovou rychlost 250 kb/s. Má integrovaný přepínač mezi vysíláním a příjmem a podporuje 3 operační módy pro zvýšení životnosti baterie.

Další podporované rozhranní a vlastnosti čipu MC13213 jsou uvedeny v použité literatuře [20].

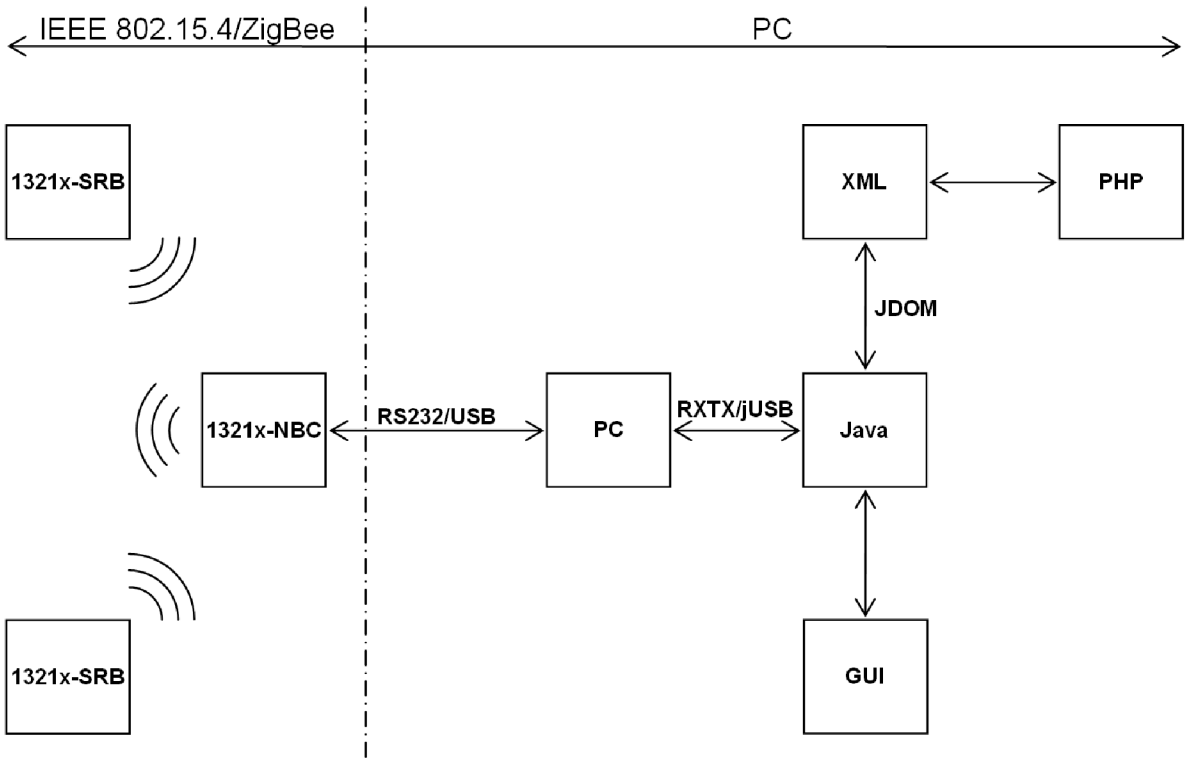
## 3.3 Návrh architektury

Předchozí kapitoly se zabývali problematikou hlasování a dostupnými hardwarovými vývojovými prostředky pro realizaci projektu. Následující text se zabývá návrhem architektury bezdrátového hlasovacího systému jako celku a v rámci zadání projektu. Pro řešení daného problému využívá poznatků uvedených v předchozích kapitolách a navrhuje další, nové prostředky, pro úspěšné zvládnutí projektu.

Návrh bezdrátového hlasovacího systému vychází z architektury ilustrované na obrázku 3.6. Uvedená architektura specifikuje vhodné rozhranní a implementační prostředky pro realizaci

projektu. Při výběru použitých technologií, ať už implementačních nebo komunikačních, byl kladen důraz na vlastnosti, jako je složitost použití a použitelnost na daný problém, spolehlivost, schopnost komunikace s jinou technologií, podpora, cenová dostupnost a zkušenost.

Architektura na obrázku 3.6 téměř vychází z teoretického modelu popsaného v posledním odstavci kapitoly 3.1. Skládá se ze dvou částí. První z nich je realizována bezdrátovou technologií založenou na protokolu IEEE 802.15.4/ZigBee (viz kapitoly 2, 3.2 a 3.3.1). Druhá část běží na PC (viz kapitoly 3.3.2, 3.3.3, 3.3.4).




*Obr. 3.6 Architektura bezdrátového hlasovacího zařízení.*

### 3.3.1 Přihlašování do sítě, hlasování a sběr hlasů

Bezdrátová síť IEEE 802.15.4/ZigBee je použita pro samotnou komunikaci hlasovacích zařízení s centrální jednotkou. Jako hlasovací zařízení, je použita vývojová deska 1321x-SBR. K dispozici pro interakci s uživatelem jsou 4 programovatelná tlačítka a 4 programovatelné LED. Účelem návrhu je vhodně tyto komponenty využít. Tlačítka lze využít při hlasování pro volbu z možnosti:

- Ano
- Ne
- Zdržel se hlasování
- Chybná volba.

Nebo pro volbu jedné nebo více možností z *N*, jako je například:

- Možnost A
- Možnost B
- Možnost C
- Možnost D.

Hlasování při druhém uvedeném příkladu je limitováno počtem tlačítek desky 1321x-SBR. Pro volbu z více než 4 možností by bylo třeba zařízení rozšířit o přídavnou periferii s větším počtem tlačítek. Ovšem pro tuto práci je počet tlačítek dostačující. Možnost D by v tomto případě mohla být nahrazena možností *chybná volba* nebo *zdržel se hlasování*. Hlasování bude probíhat na principu vyzívání, kdy nejprve je vznesena otázka a až posléze účastníci vybírají jednu z nabízených možností. Doba pro výběr odpovědi a její potvrzení by měla být časově omezena.

Aby hlasovací zařízení bylo schopno se účastnit hlasování, musí být do sítě přihlášeno pod daným uživatelem. Předpokládá se, že každý uživatel musí být v systému registrovaný. Bez registrace mu je možnost hlasovat odepřena. O přidávání nových uživatelů do systému by se měla starat aplikace na straně PC.

Koncept přihlašování by měl být takový, že uživatel zadá na hlasovacím zařízení pouze přidělenou kombinaci kláves, kterou potvrdí. Hlasovací zařízení zašle vložená data a na straně serveru se kombinace porovná s databází. Pokud bude uživatel identifikován, je hlasování povoleno, v opačném případě je účastník zamítnut. Pro přihlašování do systému by byla v tomto případě přídavná periferie více než vhodná. Přihlašování by mohlo probíhat prostřednictvím čtečky čipových karet, elektronických klíčů, v krajním případě pomocí biometrického senzoru nebo klasické numerické klávesnice. Nicméně tento problém bych prozatím nechal otevřený.

Celou síť je třeba jistým způsobem řídit. Tím je myšlena distribuce a sběr dat. Pro tento účel bylo vybráno zařízení 1321x-NBC. Zařízení v architektuře slouží jako centrální jednotka fyzické hlasovací sítě a zároveň jako prostředník mezi touto sítí a osobním počítačem. Pro propojení 1321x-NBC s PC jsou k dispozici rozhranní RS232 a USB. Každé rozhranní je vhodné pro jinou oblast nasazení. Pro realizaci projektu ovšem předpokládám použití RS232.

### 3.3.2 Export dat na server a funkce serveru

V předchozí kapitole 3.3.1 bylo uvedeno použití rozhranní RS232 pro komunikaci mezi centrální jednotkou hlasovací sítě a serverem. Server je v tomto případě reprezentován implementovanou aplikací v programovacím jazyce Java běžící na klasickém osobním počítači. Vzhledem k tomu, že použité PC disponuje sériovou linkou RS232, použití tohoto rozhranní se přímo vybízí.

Hlavním úkolem serveru je komunikace s centrální jednotkou hlasovací sítě, archivace přijatých hlasů od jednotlivých účastníků, správa účtů účastníků a popřípadě i export výsledků hlasování na zobrazovací jednotku PC. Jelikož Java přímo komunikaci se sériovým portem nepodporuje, je potřeba využít pro tento účel příslušné API (Application Programming Interface). Na internetu je ke stažení několik variant. Po prostudování jednotlivých variant bylo vybráno API RXTX ve verzi 2.1-7 [21]. Následující podkapitoly se zabývají stručným úvodem k použitým technologiím.

**RXTX 2.1-7**

RXTX je nativní knihovna, která poskytuje Javě přístup k sériovému a paralelnímu komunikačnímu rozhranní. RXTX je volně stažitelné z internetu [21]. Podporovanými operačními systémy jsou Windows, Linux, Mac OS a Solaris. Náhradou za RXTX může být například Java Communications ve verzi 2.0 nebo 3.0 podporované přímo společností Sun Microsystems. Nevýhodou tohoto API v nižší verzi 2.0 je nestabilita. Ve vyšší verzi 3.0 pak nižší podpora operačních systémů.

Instalace API RXTX spočívá v uložení přiložených knihoven na příslušná místa v počítači. Použití je jednoduché a přívětivé. API je rovněž stále vylepšováno a aktualizováno. Příklad implementace je uveden v algoritmu 3.1. Algoritmus 3.1 popisuje připojení aplikace v jazyce Java k sériovému portu RS232 a vytvoření nového vlákna pro čtení dat na tomto rozhranní.

```
CommPort com_port = portID.open(this.getClass().getName(), 2000);

if (com_port instanceof SerialPort) {
    SerialPort sp = (SerialPort) com_port;
    /**
     * Nastaveni parametru serioveho portu
     * > speed      - rychlost komunikace
     * > data_bits  - pocet datovych bitu
     * > stop_bits  - pocet stop bitu
     * > parity     - parita prenaseneho znaku
     */
    sp.setSerialPortParams(speed, data_bits, stop_bits, parity);

    InputStream in_stream = null;
    in_stream = serial_port.getInputStream();

    //Vlakno pro cteni dat ze serioveho portu
    (new Thread(new COMPortDataReader_Thread(in_stream))).start();
}
```

*Algoritmus 3.1 Ukázka použití API RXTX pro přístup k sériovému portu RS232.*

**Java**

Java je jedním z nejrozšířenějších a nejpoužívanějších programovacích jazyků na světě. Je objektově orientovaná a svojí syntaxí se inspiruje od jazyků C a C++. Oproti nim však odpadla spousta konstrukcí, které nebyly vhodné. Ty byly z jazyka buď odstraněny úplně, nebo nahrazeny jinými, jednoduššími principy. Velkou výhodou, která dělá k Javy tak mocný nástroj, je její přenositelnost mezi různými platformami operačních systémů. Je tedy jedno, na jakém počítači je vytvářená aplikace spouštěna. Soubory s kódem mají příponu `.java`. Přeložený program, *bajtkód*, se ukládá do souborů typu `.class`. Další výhodami Javy je široká komunita vývojářů, technické zázemí, pravidelné aktualizace a volně dostupné vývojové prostředky, jako například vývojové prostředí NetBeans [22].

### 3.3.3 Archivace záznamů hlasování a správa účtů

Archivace výsledků hlasování a správa účtů účastníků hlasování probíhá na straně serveru. K implementaci serveru je použit programovací jazyk Java, popsaný v kapitole 3.3.2. Správa účtů, tedy jejich vytváření, modifikace nebo mazání, je vedena prostřednictvím GUI (Graphical User Interface) implementovaným v Javě.

Pro účel ukládání dat, ať už o uživatelích nebo hlasování, byly zvažovány tři technologie. MySQL, XML a klasické textové dokumenty.

Pro další postup byl vybrán jazyk XML. Java už v základu obsahuje nástroje pro práci s tímto typem dokumentu. I přes to byl pro zpracování XML dokumentů vybrán nástroj JDOM. JDOM poskytuje oproti nástrojům integrovaným v Javě jednodušší použití.

**XML**

XML (Extensible Markup Language) je standardem konsorcia W3 a v současné době se jedná o jeden z nejdůležitějších formátů výměny dat strukturovaným způsobem. XML během posledních deseti let doznal v této oblasti značného rozšíření díky svým dobrým vlastnostem. Jedná se o otevřený formát, jehož specifikace volně přístupná na stránkách konsorcia W3.

Následující příklad 3.1 demonstruje použití XML dokumentu pro uložení výsledků hlasování. Příklad obsahuje ID hlasování, téma, datum a počet účastníků, kteří hlasovali pro, proti anebo se hlasování zdrželi.

Z příkladu 3.1 lze postřehnout, že struktura zobrazovaného XML dokumentu je značně podobná jazyku HTML. Jedná se o hierarchickou nebo také stromovou strukturu. Oproti HTML přibila možnost definovat si své vlastní značky. To přispívá k vlastnosti uchovávat libovolná data. XML deklarace neboli hlavička dokumentu popisuje verzi XML a kódování. Zbylou část tvoří textový obsah dokumentu. Ten je tvořen textovými značkami (elementy) a atributy, které uchovávají

samotné data. Dále pak komentáři. Každý element, pokud není koncový nebo prázdný, může mít další potomky. Každý z těchto potomků může být dále tvořen dalšími potomky [22].

```
<?xml version="1.0" encoding="UTF-8"?>
<hlasovani id="201001060001">
  <tema>Výstavba nového parku</tema>
  <datum>2010-01-06</datum>
  <ano>11</ano>
  <ne>4</ne>
  <zdrzel_se>3</zdrzel_se>
</hlasovani>
```

Příklad 3.1 Ukázka krátkého XML dokumentu s údaji o hlasování.

**JDOM**

JDOM (Java Document Object Model) byl vyvíjen za účelem zjednodušení obecně složitého rozhraní DOM. Plní převážně tutéž úlohu, akorát s menším úsilím vynaloženým ze strany vývojáře. Neobsahuje svůj vlastní parser. K tomuto účelu využívá libovolný existující parser. Implementačním jazykem se mu stala Java.

Pokud chce vývojář pracovat s XML dokumentem pomocí JDOMu, musí nejprve dokument načíst do paměti klasickým DOMem. Teprve poté předat ukazatel na tuto strukturu. JDOM, oproti DOMu, umožňuje snazší manipulaci s celým XML dokumentem. Jde především o průchod stromem, přidávání, editaci a mazání elementů a atributů a v neposledním případě i práci s ostatními informacemi, jako jsou komentáře, jmenné prostory, a tak dále.

I když se jedná o dobrý a používaný nástroj, není součástí ani Java Core API v JDK 1.6, ani JWSDP 2.0 (Java Web Services Developer Pack 2.0) [22].

### 3.3.4 Export záznamů hlasování na web

Vzhledem k použitému formátu pro uložení záznamů o hlasování je možné k těmto souborům velmi jednoduše přistupovat přes webové rozhranní z klasického prohlížeče. Pro postup zpracování XML souborů a jejich vizualizace v HTML (HyperText Markup Language) se předpokládá použití jazyka PHP. Formát zobrazovaných dat by měl být prostřednictvím grafů a tabulek s dodatkovými informacemi.

**PHP**

PHP je skriptovací programovací jazyk určený především pro programování dynamických internetových stránek. Nejčastěji bývá začleňován přímo do struktury jazyky HTML, XHTML (Extensible HyperText Markup Language) či WLM (Wireless Markup Language).

PHP kódy jsou překládány na straně serveru pomocí PHP interpretu. Ke koncovému uživateli se přenáší pouze výsledek zpracování. Syntaxe jazyka vychází z programovacích jazyků Java, C nebo Perl. Důležitou vlastností PHP je přenositelnost mezi různými operačními systémy a podpora mnoha knihoven. Například pro práci s databázemi MySQL, ODBC, Oracle nebo komunikačními protokoly, jako je FTP, http, SMTP, IMAP, POP3, a tak dále [23].

# 4 Závěr

Práce splnila všechny cíle uvedené v úvodu v kapitole 1.2. Popsala podrobně protokol IEEE 802.15.4/ZigBee se zaměřením na funkčnost a vlastnosti jednotlivých vrstev. Dále naznačila schéma komunikace mezi jednotlivými vrstvami protokolu a teoreticky uvedla možnosti zabezpečení v senzorových sítích založených na tomto standardu.

Dalším bodem, který byl v rámci semestrálního projektu zpracován, byl návrh architektury bezdrátového hlasovacího systému. Realizovaný návrh vycházel částečně z všeobecně používaných metod v elektronických hlasovacích systémech plus byl doplněn o nové návrhy a podměty. Stěžejní technologií použitou k docílení výsledného systému je vývojový kit 1321xNSK-BDM. Tato bezdrátová technologie představuje v architektuře síť hlasovacích zařízení. Další navrhované nástroje pro definovanou a správnou funkčnost celého systému jsou Java, PHP, JDOM a RXTX.

Semestrální projekt se stal jakýmsi teoretickým úvodem pro řešení diplomové práce. Ta se následně zabývá implementací navrhovaného bezdrátového hlasovacího systému, jeho praktickým odzkoušením a shrnutím dosažených výsledků.

# Literatura


[1] ZigBee Alliance: *ZigBee Specification*. [online], Verze 053474r17 (2008), © 2007, poslední aktualizace 17.01.2008, [cit. 2010-01-03]. URL <http://www.zigbee.org>

[2] ZigBee Alliance: *ZigBee RF4CE Specification*. [online], Verze 1.00 (2009), © 2009, poslední aktualizace 17.03.2009, [cit. 2010-01-03]. URL <http://www.zigbee.org>

[3] The Institute of Electrical and Electronic Engineers: *Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*. [online], Verze 802.15.4-2003, © 2003, [cit. 2010-01-03], ISBN 0-7381-3677-5 SS95127, 679s.
URL <http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf>

[4] The Institute of Electrical and Electronic Engineers: *Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*. [online], Verze 802.15.4-2006, © 2006, [cit. 2010-01-03], ISBN 0-7381-4997-7 SS95552, 323s.
URL <http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf>

[5] Wikipedia: *ZigBee*. [online], poslední aktualizace 11.12.2009, [cit. 2010-01-03].
URL <http://en.wikipedia.org/wiki/ZigBee>

[6] BRADÁČ, Z.; FIEDLER, P.; HYNČICA, O.; BRADÁČ, F.: Bezdrátový komunikační standard ZigBee. *Automatizace*, ročník 48, č. 4, Duben 2005, str. 261.

[7] KOTON, J.; ČÍKA, P.; KŘIVÁNEK, V.: *Standard nízkorychlostní bezdrátové komunikace ZigBee*. [online], poslední aktualizace 18.04.2006, [cit. 2010-01-03].
URL <http://access.feld.cvut.cz/view.php?cisloclanku=2006032001>

[8] KOUBÂA, A.; ALVES, M.; TOVAR, E.: IEEE 802.15.4 for Wireless Sensor Networks: A Technical Overview. Technická zpráva, verze 1.0, IPP Hurray!, Polytechnic Institute of Porto, 2005.

[9] Wikipedia: *IEEE 802.15.4-2006*. [online], poslední aktualizace: 26.12.2009, [cit. 2010-01-03].
URL <http://en.wikipedia.org/wiki/802.15.4>

[10] LABIOT, H.; AFIFI, H.; DE SANTIS, C.: *Wi-Fi, Bluetooth, ZigBee and WiMAX*. Dordrecht: Sprinter, první vydání, 2007, ISBN 978-1-4020-5396-2, 316 s.

[11] EADY, F.: *Hands-on ZigBee: Implementing 802.15.4 with Microcontrollers*. Boston: Newnes, 2007, ISBN 978-0-12-370887-8, 336s.

[12] FUCHS, M.: Řízení bezdrátové komunikace pomocí ZigBee. Diplomová práce, Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2008, vedoucí diplomové práce Ing. Tomáš Frýza Ph.D.

[13] BARTEK, L.: *Protokol ZigBee pro bezdrátové senzorové sítě*. Bakalářská práce, Vysoké učení technické v Brně, Fakulta informačních technologií, 2008, vedoucí bakalářské práce Ing. František Zbořil, Ph.D.

[14] CUNHA, A.; KOUBÂA, A.; SEVERINO, R.; ALVES, M.: Open-ZB: an open source implementation of the IEEE 802.15.4/ZigBee protocol stack on TinyOS. Technická zpráva, verze 1.0, IPP Hurray!, Polytechnic Institute of Porto, 2007.

[15] KOUBÂA, A.; ALVES, M.; NEFZI, B.; SONG, Y.: Improving the IEEE 802.15.4 Slotted CSMA/CA MAC for Time-Critical Events in Wireless Sensor Networks. Technická zpráva, verze 1.0, IPP Hurray!, Polytechnic Institute of Porto, 2006.

[16] TRCHALÍK, R.: *Senzorové sítě – ZigBee*. [online], Brno, FIT VUT v Brně, [cit. 2010-01-03].

[17] Wikipedia: *Direct Sequence Spread Spectrum*. [online], poslední aktualizace 12.11.2009, [cit. 2010-01-03].
URL <http://cs.wikipedia.org/wiki/Direct_Sequence_Spread_Spectrum>

[18] ELVAC IPC s.r.o.: *Industrial PC & Solutions: Profil, Portfolio, Reference*. [online], [cit. 2010-01-03].
URL <http://www.elvac.eu/ipc/download/reference/KATALOG-IPC-reference-CZ-2009.pdf>

[19] Freescale Semiconductor: *13213 Evaluation Kits User's Guide*. [online], verze 1.1 (2007), © 2005 – 2007, poslední aktualizace červen 2007, [cit. 2010-01-03].
URL <http://www.freescale.com/files/rf_if/doc/user_guide/13213EVKUG.pdf>

[20] Freescale Semiconductor: *MC13211/212/213*. [online], verze 1.8 (2009), © 2005 – 2009 poslední aktualizace srpen 2009, [cit. 2010-01-03].
URL <http://www.freescale.com/files/rf_if/doc/data_sheet/MC1321x.pdf>

[21] RXTX: *Download*. [online], poslední aktualizace 05.10.2009, [cit. 2010-01-03].
URL <http://rxtx.qbang.org/wiki/index.php/Download>

[22] ALBRECHT, P.: Interaktivní vizualizace XML. Bakalářská práce, Vysoké učení technické v Brně, Fakulta informačních technologií, 2008, vedoucí bakalářské práce Ing. Petr Chmelař.

[23] Wikipedia: PHP. [online], poslední aktualizace 12.12.2009, [cit. 2010-01-03].
URL <http://cs.wikipedia.org/wiki/PHP>