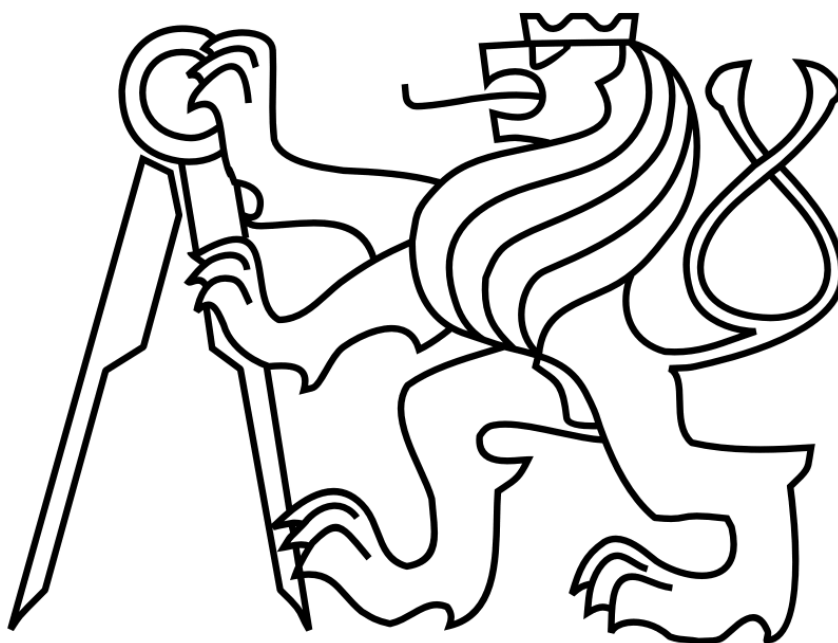


České vysoké učení technické Praha

Fakulta Elektrotechnická



Bakalářská práce

Bezdrátový přenos Zigbee

Praha, 2010

Autor: Jiří Šedivý

České vysoké učení technické v Praze
Fakulta elektrotechnická

Katedra řídicí techniky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Student: Jíří Šedivý

Studijní program: Elektrotechnika a informatika (bakalářský), strukturovaný
Obor: Kybernetika a měření

Název tématu: **Bezdrátový přenos ZigBee**

Pokyny pro vypracování:

1. Navrhněte strukturu systému s několika (3) klienty pro vzájemný bezdrátový přenos a zpracování dat v síti s protokolem ZigBee. Bezdrátový přenos dat realizujte ve variantách:
 - PC ↔ PC
 - PC ↔ mobilní zařízení
2. K dispozici jsou ZigBee moduly PAN802154HAR00 a RC2200DB.
3. Navrhněte a realizujte interface (HW a SW) pro připojení ZigBee modulu ke stacionárnímu PC a ke vhodnému řídicímu mikro počítači mobilního zařízení.
4. Navrhněte a realizujte demonstrační úlohu do cvičení pro bezdrátový přenos s protokolem ZigBee mezi PC a mobilním zařízením.

Seznam odborné literatury:

Dodá vedoucí práce

Vedoucí: Doc. Ing. Jíří Bayer, CSc.

Platnost zadání: do konce zimního semestru 2009/10



prof. Ing. Michael Šebek, DrSc.
vedoucí katedry



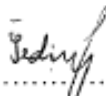
doc. Ing. Boris Šimák, CSc.
děkan

V Praze dne 27. 2. 2009

Prohlášení

Prohlašuji, že jsem svou bakalářskou práci vypracoval samostatně a použil jsem pouze podklady (literaturu, projekty, SW atd.) uvedené v příloženém seznamu.

V Praze, dne 6.1.2010


.....
připis

Anotace

Tématem bakalářské práce je technologie bezdrátového přenosu dat Zigbee, jejíž nasazení se předpokládá hlavně pro úsporné senzorové sítě a automatizaci. Cílem práce je seznámení se se standartem, nastavení bezdrátových modulů a měření jejich přenosových vlastností. Na předchozí text navazuje formulace demonstrační úlohy do cvičení pro bezdrátový přenos dat.

Annotation

The topic of this bachelor's work is technology of wireless data transfer called Zigbee, whose destination is automation and low powered sensor networks. The goals are to getting to now this standart, setting up wireless modules and measuring of transfer characteristics. To this relates formulation of exercise for wireless transfer courses.

Poděkování

Chtěl bych velmi poděkovat všem, kdo mi pomáhali při tvorbě této práce, ať už přímo nebo nepřímo. Zvláště pak děkuji doc. Ing. Jiří Bayerovi, CSc., za trpělivost, a celé mé rodině za podporu při studiu.

1. Úvod	2
2. Seznam zkratk	3
3. O technologii	5
3.1 Historie.....	5
3.2 Standart IEEE 802.15.4.....	5
3.2.1 Fyzická vrstva	5
3.2.2 MAC vrstva	6
3.3 Vrstvy které upravuje Zigbee	10
3.3.1 Síťová vrstva (NWK).....	10
3.3.2 Aplikační vrstva (APL).....	11
3.4 Komunikace v síti.....	12
3.5 Zabezpečení	13
4. Přehled použitých zařízení	15
4.1 PAN802154HAR	15
4.1.1 Specifikace	15
4.1.2 Popis a zapojení	15
4.1.3 Programování.....	16
4.2 RC2200DK-SPPIO	16
4.2.1 Specifikace	16
4.2.2 Balení	17
4.2.3 Popis a zapojení	17
4.2.4 Programování.....	18
5. Návrh sítě se třemi klienty	19
6. Komunikace PC <=> PC a PC <=> Mobilní zařízení	21
7. Analyzátor sítě	25
8. Demonstrační úloha do cvičení pro bezdrátový přenos s protokolem Zigbee	26
9. Závěr	28
10. Použitá literatura	29
Příloha A – Tabulky AT příkazů, adres a hlášení modulů Radiocrafts	31
Příloha B – Tabulka přenosových pásem.....	34

1. Úvod

V této práci demonstřuji technologii Zigbee a ověřuji některé její výhody a nevýhody. Pro realizaci zadání jsem využíval Zigbee moduly od firem Panasonic (PAN802154HAR00) a Radiocrafts (RC2200DK-SPPIO). Stručně také popisuji jak by se dal napsat nový firmware pro Panasonic. Jednu kapitolu také věnuji možnosti odposlechu Zigbee komunikace. V závěru práce uvádím návrh úlohy pro cvičení na bezdrátový přenos dat.

2. Seznam zkratek

- AES – pokročilý systém kryptování
- ALC – seznam důvěryhodných zařízení
- AO – aplikační objekt
- AODV – pokročilý systém routování na vyžádání
- APL – aplikační vrstva
- APS – aplikační podvrstva
- BDM – rozhraní pro programování a ladění
- CBC-MAC – mód zajištění důvěrnosti
- CCM – mód zabezpečení MAC rámců
- CCM* - mód zabezpečení síťové vrstvy
- CSMA-CA – metoda přístupu k fyzickému médiu
- CTR – mód ověření integrity
- EOP – konec packetu
- FFD – plně funkční zařízení
- GTS – garantovaný časový slot
- IEEE – název standartizační organizace
- ISM – pásmo pro užití v průmyslu, výzkumu a lékařství
- ISO/OSI – standartizovaný model topologie síťového zařízení
- JTAG – rozhraní pro programování a ladění
- KVP – pár klíč-hodnota
- MAC – vrstva přístupu k fyzickému médiu
- MIC - kód pro ověření integrity
- NWK – síťová vrstva

PAN – osobní síť

PHY – fyzická vrstva

RFD – zařízení s omezenými funkcemi

SOP – identifikátor začátku paketu

SPI – sériové seriferní rozhraní

SSP – služba zajišťující zabezpečení

ZDO – objekt zařízení Zigbee

3. O technologii

3.1 Historie

ZigBee je velmi mladou komunikační technologií. O technologiích osobních bezdrátových sítí se začalo hodně mluvit kolem roku 1998, kdy se začaly rozšiřovat sítě WiFi a Bluetooth. Ty však nepokrývaly všechny potřeby komunikace. Proto byl v roce 2003 dokončen standart IEEE 802.15.4. Ten specifikoval spodní dvě vrstvy modelu ISO/OSI - fyzická a spojová, které byly vyladěny pro použití v těchto sítích s označením PAN. V té době organizace Zigbee alliance zároveň vyvíjela rozšíření založené na tomto standartu - ZigBee. Dne 14. prosince 2004 byla publikována první specifikace. S tím zároveň začal stoupat zájem firem, které chtěly tuto novou technologii využívat a rozvíjet. V dnešních dnech má Zigbee alliance více než 300 spolupracujících členů. Od ledna 2005 je specifikace veřejná a může z ní tedy čerpat informace každý. V roce 2006 byla zveřejněna úprava Zigbee 2006. Nejnovější schválená specifikace je verze Zigbee 2007/PRO.

3.2 Standart IEEE 802.15.4

Tento standart byl vytvořen pro definici bezdrátových sítí PAN. Jeho hlavními cíli byla jednoduchá nasaditelnost, nízké výrobní náklady, nízká spotřeba pro možnost provozu na baterie a také solidní přenosová rychlost. Definuje požadavky pro fyzickou vrstvu (PHY), linkovou vrstvu (MAC) a topologie sítě.

3.2.1 Fyzická vrstva

Protokol využívá dvě PHY vrstvy, které zahrnují tři volná frekvenční pásma (915 MHz, 868 MHz, 2.4GHz). Důvodem pro použití více pásem je možnost používat zařízení ve více zemích, protože každá země má rozdílnou definici rádiových pásem. Jejich přehled je v tabulce viz příloha B. Jako metodu pro přístup k médiu je užito CSMA/CA.

3.2.2 MAC vrstva

MAC vrstva již definuje komunikaci mezi jednotlivými zařízeními a to buď pomocí rámců nebo bez nich. Rámce jsou definovány 4 (3 pro řízení komunikace a jeden pro přenos dat).

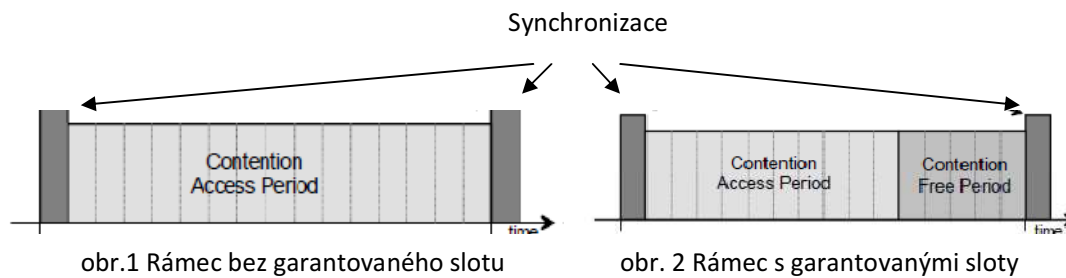
Acknowledgement frame – k přijetí potvrzovací informace

Beacon frame - pro synchronizaci zařízení v síti převádění koncových zařízení do úsporného režimu

Data frame – k datovým přenosům.

MAC command frame – pro centralizované řízení všech zařízení v síti

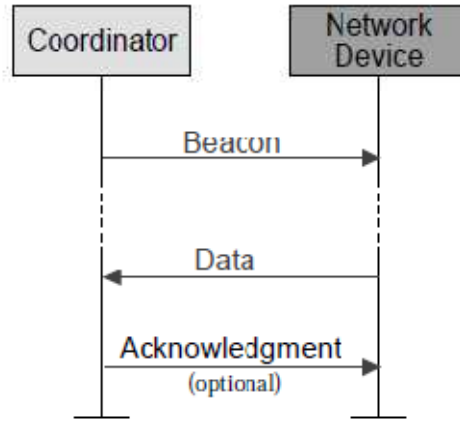
Další možnost jak posílat data umožňuje Super frame (Super rámeček). Je ohraničen synchronizací (beacon) a jeho formát definuje koordinátor. Skládá se z 16ti stejných časových pozic (slot), z nichž může být až 7 nastavených jako garantovaný časový slot (GTS). Struktura se užívá, chceme-li některým zařízením umožnit, aby mohla komunikovat přesně v určený čas, který je daný časovým slotem. Je důležité zmínit, že přenos dat je třeba ukončit před příchodem beaconu nebo před příchodem periody garantovaných časových slotů.



Na základě synchronizace Beacon frame je možné minimalizovat spotřebu klientských zařízení tím, že se zařízení vypne a probudí v přesně nastavenou dobu před přenášením informace. Spotřebu zařízení je tím možné snížit tak, že při vhodné konfiguraci může fungovat až 2 roky na běžné tužkové baterie.

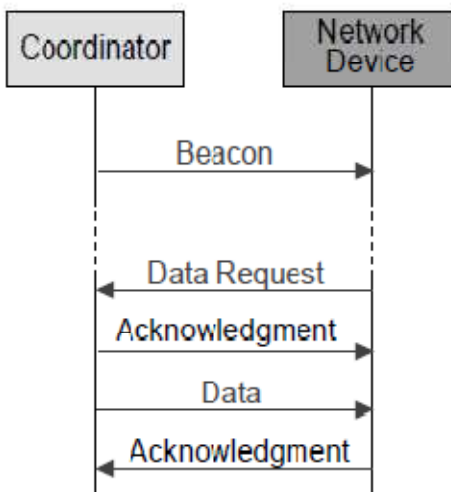
Přenos dat:

Přenos dat ke koordinátoru sítě probíhá tak, že koordinátor vyšle Beacon frame, zařízení ho přijme a odešle data. Ty jsou následně potvrzena koordinátorem.



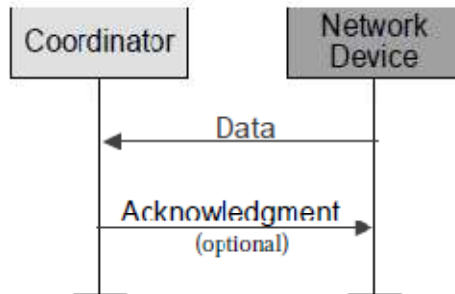
obr. 3 Odeslání dat koordinátoru při synchronizované komunikaci

Přenos od koordinátora do sítě probíhá tak, že odešle Beacon frame a zařízení odpoví požadavkem na data. Koordinátor potvrdí přijetí požadavku a vyšle data. Zařízení nakonec potvrdí přijetí dat.



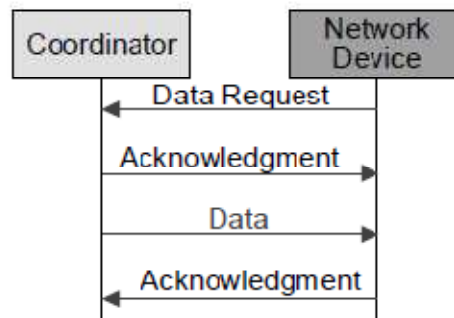
obr. 4 Odeslání dat od koordinátora při synchronizované komunikaci

Pokud funguje komunikace bez rámců, jednotlivá zařízení periodicky dotazují koordinátora. Přenos dat ke koordinátoru vypadá tak, že zařízení odešle data a koordinátor je potvrdí.



obr. 5 Odesílání dat koordinátoru při komunikaci bez synchronizace

Přenos od koordinátora proběhne odesláním požadavku na data zařízením. Koordinátor potvrdí přijetí rámce a poté odešle data. Zařízení nakonec potvrdí příjem dat.

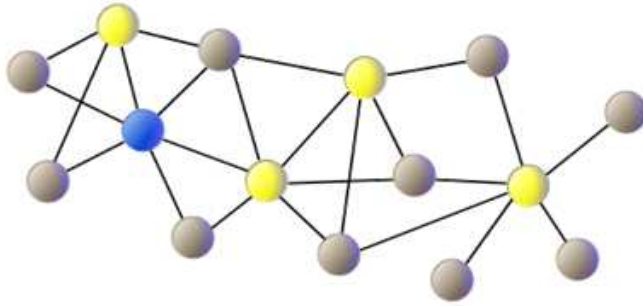


obr. 6 Odesílání dat od koordinátora při komunikaci bez synchronizace

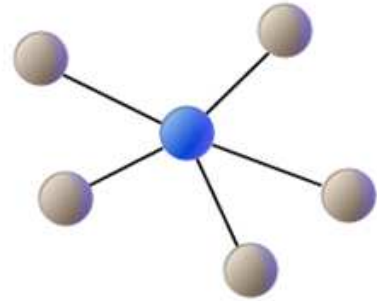
Tato vrstva také upravuje počet adres zařízení. Adresní prostor je velký 64-bitů, což umožňuje prakticky neomezený počet zařízení v síti. Velmi často se však pro zjednodušení používá pouze omezený prostor o velikosti 16-bitů (maximálně 65536 zařízení v síti). Každá síť má navíc ještě svůj 16-ti bitový identifikátor sítě, takže může souběžně fungovat až 65536 sítí.

Další část kterou tento standart upravuje je topologie sítě. V tomto standartu je možno využívat topologii hvězda (star). Skládá se z koordinátora sítě uprostřed a koncových zařízení, která jsou s ním spojena. Další variantou je komunikace mezi dvěma zařízeními (peer-to-peer). Je možné použít i složitější topologie například strom (cluster), který spojuje koordinátora se směrovači, na něž jsou následně navázána koncová zařízení nebo kombinací těchto dvou topologií vytvořit síť (mesh). Ty je však třeba implementovat ve vyšších vrstvách.

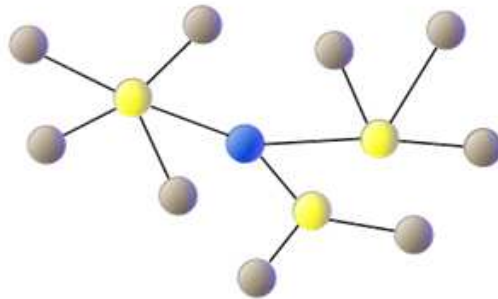
mesh




star




cluster



-  Reduced Function Device (Sensor, Controller, Actuator, etc.)
-  PAN Coordinator
-  Full Function Device (Performs network routing functions)

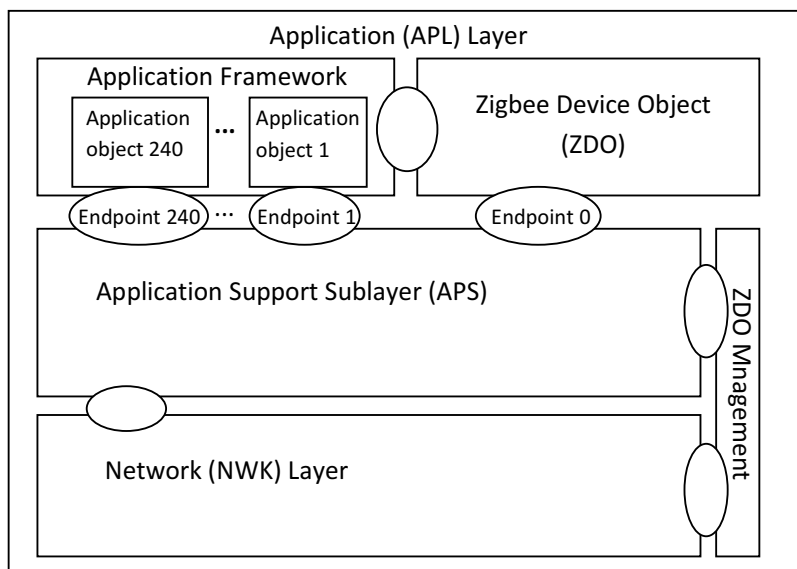
Peer - to - peer



-  ZigBee-compliant Device (Sensor, Controller, Actuator, etc.)

obr. 7 Typy síťových topologií

3.3 Vrstvy které upravuje Zigbee



obr. 8 Schéma Zigbee stacku

3.3.1 Síťová vrstva (NWK)

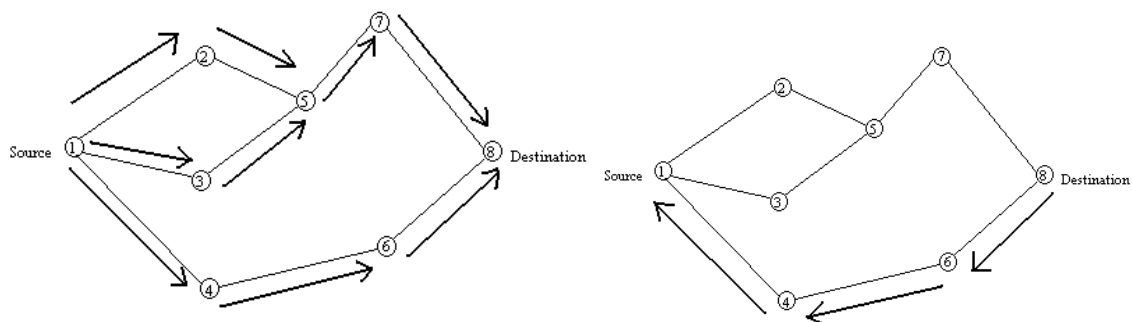
Hlavní funkcí síťové vrstvy je ovládání MAC vrstvy (routováním vytváření složitějších topologií) a vytvoření vhodného propojení na aplikační vrstvu (APL). Její hlavní služby:

- nastavuje vlastnosti zařízení - tedy zda je zařízení koordinátor, směrovač nebo koncové zařízení.
- spouští síť – touto službou může koordinátor vytvořit novou síť.
- připojuje a odpojuje zařízení od sítě – možnost začlenit se a opustit síť, v případě koordinátora a směrovače vyřizování žádostí o odpojení od sítě.
- přiřazování adres zařízením – možnost koordinátora a směrovače přiřazovat adresy novým zařízením v síti.
- prohledávání sousedních zařízení – pro zjišťování informací o přímo připojených zařízeních
- prohledávání routování v síti – tato služba prohledává a zaznamenává cesty v síti pro zvýšení efektivity směrování
- řízení příjmu - zapínání přijmače řízení doby jeho funkce a synchronizace MAC podvrstvy

Routování v síti – využití AODV (Ad hoc On-demand Distance Vector Routing) routovacího protokolu a zaznamenávání do směrovací tabulky. AODV funguje na principu všesměrového vysílání všem sousedním zařízením. Ta vysílají data dál, až dorazí k cíli. Ten

vyšle zpátky odpověď nejkratší cestou ke zdroji. Zdroj vysílání zpráv zaznamená svého souseda, od kterého přišla odpověď a cenu¹ cesty do své směrovací tabulky pro příští použití.

Zabezpečení – jako zabezpečovací mechanismus se používá 128mi bitový algoritmus AES. Další informace ohledně zabezpečení jsou uvedeny níže ve stejnojmenné podkapitole.



obr. 9 Princip fungování AODV

3.3.2 Aplikační vrstva (APL)

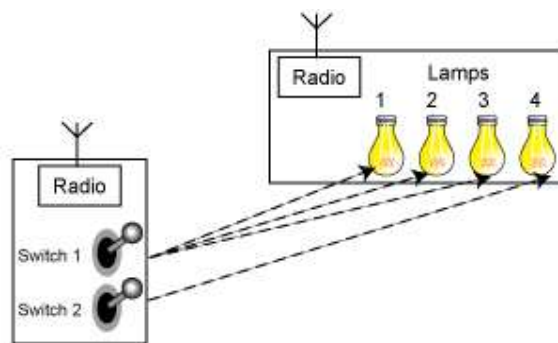
Aplikační vrstva je nejvyšší vrstvou standardu Zigbee. Skládá se ze tří částí – Aplikační podvrstvy (APS), objektu Zigbee zařízení (ZDO) a rámce výrobcem definovaných aplikačních objektů (AO).

Aplikační podvrstva je velmi důležitá pro komunikaci se síťovou vrstvou a dalšími součástmi aplikační vrstvy. Jejím funkcí je prohledávání, která zařízení pracují v dosahu a spojování těch, která si chtějí vyměňovat data. Informace o spojených zařízeních jsou uchovávány ve spojovací tabulce (binding table).

Objekt Zigbee zařízení slouží k nastavení role zařízení v síti, inicializaci spojování a vytváření zabezpečených partnerství mezi zařízeními jednou z definovaných metod. U zařízení v roli koordinátora nebo routru navíc umožňuje vzdáleně iniciovat prohledávání sítě a získávat směrovací nebo spojovací tabulku.

Aplikační objekty – aplikace se může skládat z aplikačních objektů, v nichž jsou umístěny popisovače jednotlivých aplikací. Díky tomu může být jeden radiovysílač využíván pro více aplikací najednou.

¹ Cenou je míněna složitost přenosu.



obr. 10 Komunikace KVP

V rámci jednoho zařízení může být až 240 aplikačních objektů, číslovány 1 – 240. Aplikační objekt 0 je ZDO a 255 je broadcast. Rozsah adres 241 - 254 je zatím nevyužit. Proto je třeba při adresaci uvést také tuto adresu aplikačního objektu (endpointu) v rámci jednotlivých nodů, se kterým chceme komunikovat. Aplikační objekty mohou využívat dvou komunikačních služeb:

- a) Pár klíč-hodnota (KVP) - spojení je omezeno jen na několik XML zpráv get/set. Koordinátor pak může obsahovat jen spojovací tabulku, kde je zaznamenáno, který nod spolupracuje s kterým KVP. To velmi zjednodušuje komunikaci.
- b) Obecné zprávy – tato služba odesílá libovolné zprávy. To může být výhodné u složitějších zpráv, neboť zařízení se k odeslání zprávy nemusí spojovat.

3.4 Komunikace v síti

Základní předpoklad k tomu, aby spolu mohly aplikace komunikovat, je třeba aby splňovaly obecný protokol. Aplikační profily jsou sadou popisovačů pro ovládání určitého typu komunikace. Ty mohou být buď veřejné, standartizované Zigbee aliance, nebo mohou být vytvořeny koncovými dodavateli. Pro příklad veřejných profilů je možno uvést Home Automation (automatizace domácnosti) nebo Smart energy (chytrá energie). Ty jsou již schválené Zigbee Alliance a při jejich implementaci by pak mělo zařízení komunikovat i s ostatními od jiných výrobců, které využívají stejný profil. Při užití profilů vytvořených koncovými dodavateli je však třeba brát v úvahu, že dodavatelé své profily často nezveřejňují (zařízení budou tedy komunikovat pouze se zařízeními od stejného dodavatele).

Při komunikaci je třeba rozlišovat, zda odesíláme data na známou IEEE MAC adresu nebo nikoliv. Pokud adresu koncového zařízení známe (víme kam data poslat), odesíláme je přímo na adresu nejbližšího zařízení v cestě k cíli. Pokud však data posíláme na zatím neznámou adresu, data jsou vyslána všem sousedním zařízením, která je dále rozepisují všem svým sousedům, dokud nedorazí k příjemci.

Pokud se používají spojovací tabulky, je třeba zajistit jejich stálou dostupnost (nebude třeba stále znovu a znovu vytvářet komunikační páry). Proto je vhodné, aby bylo zajištěno stálé napájení koordinátora. Při jeho výpadku totiž dojde ke smazání tabulky. Další z možností je tabulku zálohovat například ve vnější flash paměti.

Pro identifikaci fyzického radiopřijímače je využito IEEE MAC adresy, jak je již zmíněno výše. V tomto zařízení je však třeba ještě stanovit, se kterým aplikačním objektem chceme komunikovat. To je provedeno buď přímou adresací, kdy známe MAC adresu i adresu aplikačního objektu a id aplikačního profilu, nebo adresaci nepřímou, kdy známe jen MAC adresu a další dva parametry jsou uloženy ve spojovací tabulce. Tato metoda je vhodná pro jednodušší zařízení. Vedle toho mohou být ještě dva způsoby adresace :

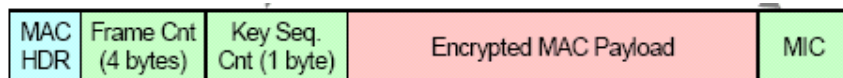
- a) broadcastování - data jsou z radiopřijímače odeslána do všech aplikačních objektů
- b) skupinové adresování - zařízení komunikuje s předem danou skupinou aplikačních objektů.

3.5 Zabezpečení

Základ zabezpečení Zigbee je v ochraně samotného protokolu IEEE 802.15.4. Využívá šifrování AES s klíčem o délce 128 bitů. Samotné zabezpečení rámců MAC vrstvy je tvořeno dvěma stupni:

- a) Ověření integrity (CTR mód) – s MAC rámcem je odeslán vytvořený kod pro ověření integrity (MIC) o různé délce (4, 8 nebo 16 oktětů)
- b) Zajištění důvěrnosti (CBC-MAC mód) – přidává se k rámcu informace o jeho pořadí a klíči. Pokud pořadí rámce odpovídá, přijímací strana odpoví potvrzením.

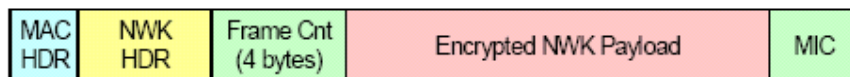
Pokud se tyto dvě zabezpečovací techniky spojí, označují se jako CCM mód.



obr. 11 Rámec zabezpečený MAC vrstvou

Dalším z užívaných bezpečnostních prvků je seznam důvěryhodných zařízení (ACL). S jeho využitím jsou odesílána data jen na adresy na zařízení, která jsou v tomto seznamu podle nastavených bezpečnostních kritérií.

Síťová vrstva je zabezpečena CCM* módem, který je mírnou modifikací CCM módu použitým v MAC vrstvě. Zahrnuje všechny možnosti CCM módu a navíc přidává možnost využít jenom jednu z částí CCM. To zjednodušuje zabezpečení síťové vrstvy, protože se klíč neváže na jednu bezpečnostní sadu a aplikace může použít i jinou sadu na každý NWK rámeček.



obr. 12 Rámeček zabezpečený NWK vrstvou

Funkci zabezpečení obstarává služba SSP. SSP se spojí s protistranou získá její klíč a aplikuje na rámeček bezpečnostní sadu. Po přenosu na druhé straně služba rozkóduje přijatá data. SSP je řízeno z vyšších vrstev, je mu přidělen klíč, kterým šifruje a zároveň vybírá kterou z CCM* sad bude využívat na který rámeček. Celý proces zabezpečení řídí aplikační vrstva. Objektem Zigbee zařízení nebo uživatelskými Aplikačními objekty pokud jsou k dispozici.

Bezpečnostní klíče

Aplikační a síťová vrstva pracují se třemi druhy klíčů:

- Hlavní klíč – předem uložený v každém nodu. Jeho funkcí je bezpečný přenos Spojovacích klíčů mezi nody při začátku komunikace.
- Spojovací klíč – jedinečný pro každý pár nodů. Tento klíč je spravován aplikační vrstvou.
- Síťový klíč – (délka 128b) sdílený mezi všemi zařízeními v síti. Každý node který se chce připojit do sítě jej musí znát. Je generován a obnovován Důvěryhodným nodem (většinou tuto roli plní koordinátor). Při každé obnově dochází zároveň k vynulování počítadla pořadí rámečků, které využívá CBC-MAC mód.

Tyto klíče jsou používány ve dvou bezpečnostních režimech:

- Komerční provoz - používá Hlavní a Spojovací klíč které jsou veřejně přístupné celé síti z Důvěryhodného nodu. Je to však velmi paměťově náročné.
- Domácí provoz – Důvěryhodný node sdílí pouze Síťový klíč. Tento bezpečnostní režim je často užíván v senzorových sítích, kde je nejdůležitější potřebou zachování co nejnižších prostředků (v tomto případě paměťových).

4. Přehled použitých zařízení

4.1 PAN802154HAR



obr. 13 Modul Panasonic

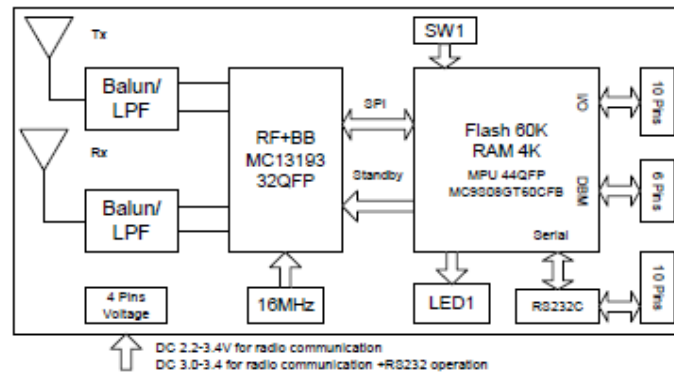
4.1.1 Specifikace

- a) Plná podpora Zigbee, 802.15.4
- b) 2.4GHz ISM pásmo
- c) 16 kanálů, maximální přenosová rychlost 250Kbit/s
- d) RS-232, 2 Analogové 10bitové vstupy, max. 8 digitálních I/O portů
- e) Stíněná vysokofrekvenční část
- f) Napájecí napětí 2.2 - 3.4VDC bez RS-232, 3-3.4VDC s RS-232

4.1.2 Popis a zapojení

Moduly Panasonic obsahují jen velmi málo součástek. Centrem je mikro počítač Freescale-Motorola MC9S08GT60CFB. Jedná se o 8-bitový procesor v 44pinovém pouzdře, obsahující 60K flash paměti, 4K RAM paměti, dva dvoukanalové 16ti bitové časovače, dva sériové porty, rozhraní SPI a rozhraní BDM pro programování. Na něj je přes rozhraní SPI připojen vysílač Freescale MC13193, který splňuje požadavky IEEE 802.15.4 Standard Radio. Vysílá v ISM pásmu na frekvenci 2,4 GHz. Pracuje v jednom ze 16ti kanálů dle specifikace. Jeho napájecí napětí je v rozsahu 2 - 3,4 V DC. Pro užití se Zigbee protokolem je vhodný také díky nízké spotřebě (max. 42mA při komunikaci a 1µA v úsporném režimu). Vysílač je umístěn v pouzdře QFN-32, které je pod kovovým krytem kvůli odstínění. Z odstíněné části vychází na desce plošných spojů vytvořené antény pro příjem a vysílání dat. Dále je k procesoru připojen na první sériový port chip MB3221I od firmy Texas instruments. Jedná se o převodník úrovní sériového portu z důvodu nízkého výstupního napětí procesoru. Dále modul obsahuje jedno tlačítko a červenou LED diodu. Tyto dva prvky jsou připojeny na port procesoru a lze jich po

implementací ve firmwaru využít k ovládní funkce modulu. Dále jsou na modulu osazeny už jen pasivní součástky použité pro správnou funkčnost obvodů.



obr. 14 Schéma zapojení

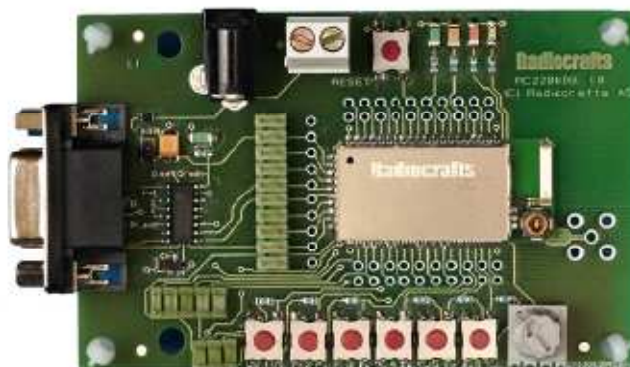
4.1.3 Programování

Pro komunikaci se standartním IBM PC je třeba použít programátor (například Cyclon Pro od firmy Pemicro). Jako vývojové prostředí Panasonic doporučuje Metrowerks Codewarrior Development Studio for HC(S)08 64K C Compiler.

4.2 RC2200DK-SPPIO

4.2.1 Specifikace

- Podpora Zigbee mash sítí
- Až 16 digitálních I/O, až 8 analogových 10bit I/O
- Konfigurace přes AT příkazy
- Nízkopříkonové napájecí módy
- 16ti kanálový vysílač v 2.4GHz ISM pásmu
- Podpora transparentního RS232/RS485/RS422
- Napájecí napětí 4-10V DC



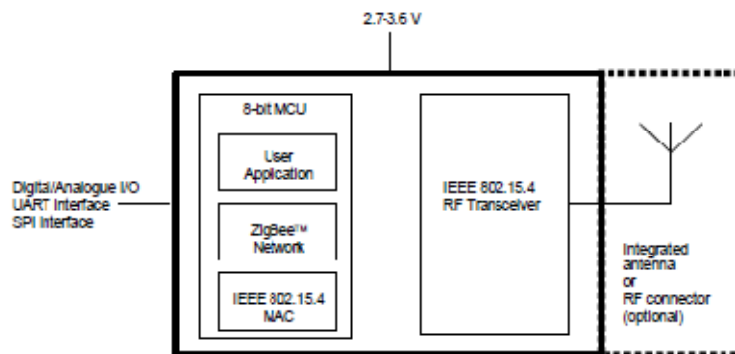
obr. 15 Modul Radiocrafts

4.2.2 Balení

Radiocrafts RC2200DK-SPPIO je celý vývojový kit obsahující vše nutné pro snadný začátek. Tvoří jej moduly RC2200DB, dva napájecí zdroje a dva propojovací sériové kabely.

4.2.3 Popis a zapojení

Moduly RC2200DB jsou vývojové zkušební desky osazené celkem označeným RC2200AT. Jedná se o plošný spoj na němž je osazený procesor AtMega128, radiopřijímač Chipcon/Texas instruments CC2420 a keramická anténa. Procesor má sériový port a je programován přes rozhraní JTAG. Společně s radiopřijímačem jsou ukryty pod kovovým stíněním pro eliminaci rušení. Celek je připojen na vývojovou desku. Ta obsahuje další součástky pro správnou funkci a možnost testování. Integrovaný obvod MAX3232 slouží jako převodník pro RS232. LP2980-3.0V je integrovaný stabilizátor napětí pro napájení procesoru a všech součástí. Dále na ní nalezneme analogové a digitální vstupy (LM60C – teplotní senzor, 4 LED, 6 tlačítek a jeden potenciometr). Velmi užitečnou součástí modulu je i tlačítko RESET, které restartuje procesor a zelená LED dioda signalizující přítomnost napájecího napětí. Ostatní části osazené na desce jsou jen pasivní součástky a konektory.



obr. 16 Vnitřní schéma Zigbee části

4.2.4 Programování

Tento modul obsahuje JTAG programovací rozhraní, kterým se může propojit k počítači přes programátor například Atmel ICE mkII. Pro vývoj softwaru je doporučeno používat volné programy WinAVR / AVR GCC nebo Atmel AVR Studio.

5. Návrh sítě se třemi klienty

K vytvoření sítě jsem využil bezdrátových modulů Panasonic. Tyto moduly jsem obdržel 3, takže jejich volba byla jasná. V jejich procesoru však byl přednahráný pouze velmi jednoduchý firmware, kterým spolu moduly neuměly komunikovat. K přenosu dat bylo proto třeba obstarat jiný, který bude mít také implementován sériový port. Panasonic nabízel na svých stránkách ke stažení mimo jiné i sadu Wireless modem demo. Tato sada obsahuje příručku v pdf a 4 firmwary navržené pro mnou užívané moduly. Každý firmware má svou pevně danou MAC adresu, přenosový kanál a ostatní vlastnosti komunikace. Pro zadaný úkol jsou firmwary dostačující.

Po rozhodnutí o použití této sady jsem je nahrál do modulů. Dle výrobce je možné nahrát firmware do modulů přes sériový port s použitím programu Serial Bootloader. Nahrát firmware do zařízení se mi s ním však nepodařilo. Proto jsem si zajistil programátor Cyclon pro firmy PE micro s vývojovým prostředím Codewarrior určeným pro procesory HCS08. Tím jsem přehrál firmware a dle příručky byly moduly připraveny k použití. Po připojení na napájení se změna firmwaru projevila hned na první pohled. Kontrolní LED dioda začala stále svítit, což jsem pochopil jako funkčnost firmwaru. Po připojení modulů k sériovým portům jsem se řídil dodanými pokyny. Spustil jsem terminálový program Hercules Setup utility, který umí odesílat surová (RAW) hexa data. Nastavil jsem správné vlastnosti přenosu (viz tabulka 1).

Parametr	Hodnota
Rychlost sériového portu	38 400 bps
Stop bity	1
Parita	Ne
Řízení toku	Ne

tab. 1 Nastavení sériového protu

Dále postup byl jasný – odesílat surová data s danou hlavičkou do terminálu a na druhé straně měla data vycházet s pozměněnou hlavičkou – místo adresy přijímajícího zařízení měla být adresa zdroje.

SOP	CMD	Adresa	Délka	Data	EOP
1B	1B	8B (MSB první)	1B	Délka B	1B

tab. 2 Struktura paketu

SOP –	Identifikátor začátku paketu (0x02)
CMD –	Vždy 0x07. V tomto demu nevyužito
Adresa –	Cílová nebo Zdrojová MAC adresa – zadáváme cílovou → na druhé straně se nám zobrazí zdrojová
Délka -	Délka dat
Data -	Přenášená data
EOP –	Identifikátor konce paketu (0xAA)

Při provádění operaci však nastal problém. I když jsem se snažil poslat data přesně dle manuálu, kde posílali 4 bajty, paket s touto délkou mi stále nechtěl projít. Nakonec jsem zjistil, že data nechodí proto, že terminálový program interpretuje délku řetězce 04 jako 0 a 4 bere již jako data. Zkusil jsem 10 bajtů a s takto nastavenou délkou již vše fungovalo bez problémů. Ze specifikace Zigbee vím, že end nody mohou spolupracovat pouze s koordinátorem a nikoliv mezi sebou. Jedná se tedy o topologii hvězda. Proto jsem posílal data od koordinátora směrem k nodům a zpět. Tím jsem ověřil že síť se třemi klienty funguje.

Dle příručky byly firmwary konfigurovány dle tab. 3.

Název firmwaru	Typ zařízení	MAC adresa
koordinátor	FFD	0x1716151413121110
end node 1	RFD	0x2726252423222120
end node 2	RFD	0x2726252423222121
end node 3	RFD	0x2726252423222122

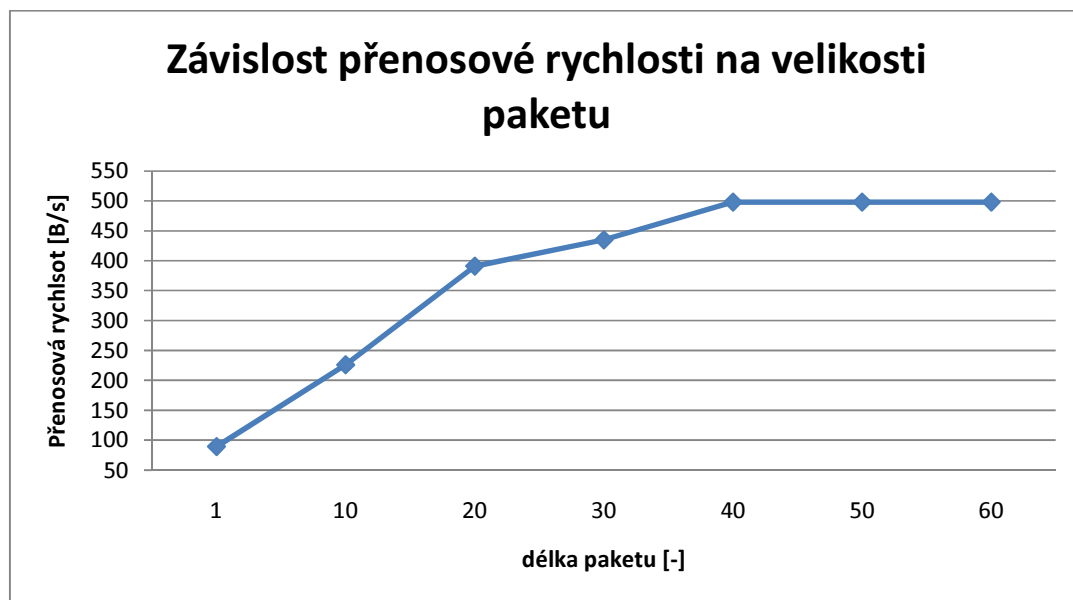
tab. 3 Nastavení firmwarů

Jediná věc kterou jsem pokládal za vhodné ještě udělat, je napsat vlastní firmware a v něm si upravit stack. Kvůli nízké dostupnosti vývojového prostředí Codewarrior jsem však neměl možnost toto udělat. Při návrhu bych však pravděpodobně využil také prostředí BeeKit, které dle zadaných kritérií připraví potřebné zdrojové soubory stacku a hardwaru. Z těch následně vytvoří projekt v programu Codewarrior. Ten si pak může programátor upravit dle svých konkrétních představ a požadavků.

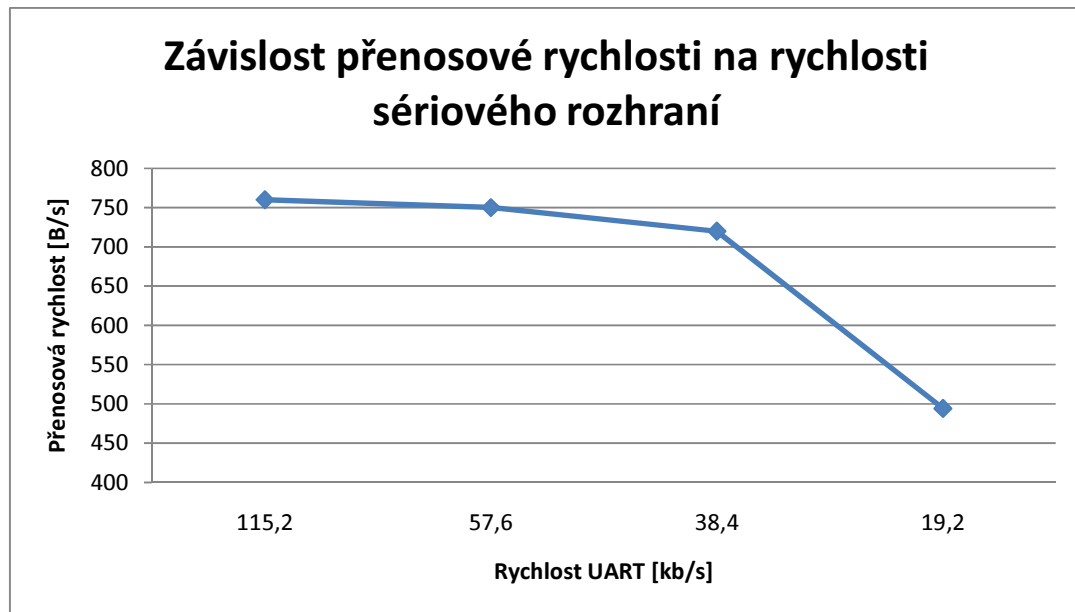
6. Komunikace PC <=> PC a PC <=> Mobilní zařízení

Po seznámení s firmwarem firmy Panasonic jsem dospěl k závěru, že neumožňuje žádné další nastavení (režim spánku, možnost změnit end node na směrovač a jiné), kterým bych mohl vyzkoušet některé z vlastností technologie Zigbee. Svě další pokusy a měření jsem proto dále prováděl na modulech Radiocrafts. Ty obsahují firmware SPPIO™, který je určen pro experimentování se sériovou komunikací a umožňují mnohem více nastavení než firmware Panasonic. Po připojení k sériovému portu počítače a připojení napájení moduly vypisují, v jakém stavu se nacházejí přímo do terminálu. To je velmi praktické, protože díky manuálu můžeme zjistit, jaký stav či jakou chybu nám modul hlásí.

Po prvním seznámení s komunikací jsem se pokoušel zjistit, jakou má vliv na přenosovou rychlost délka paketu a rychlost sériového portu. Výsledky měření ukazují následující grafy.



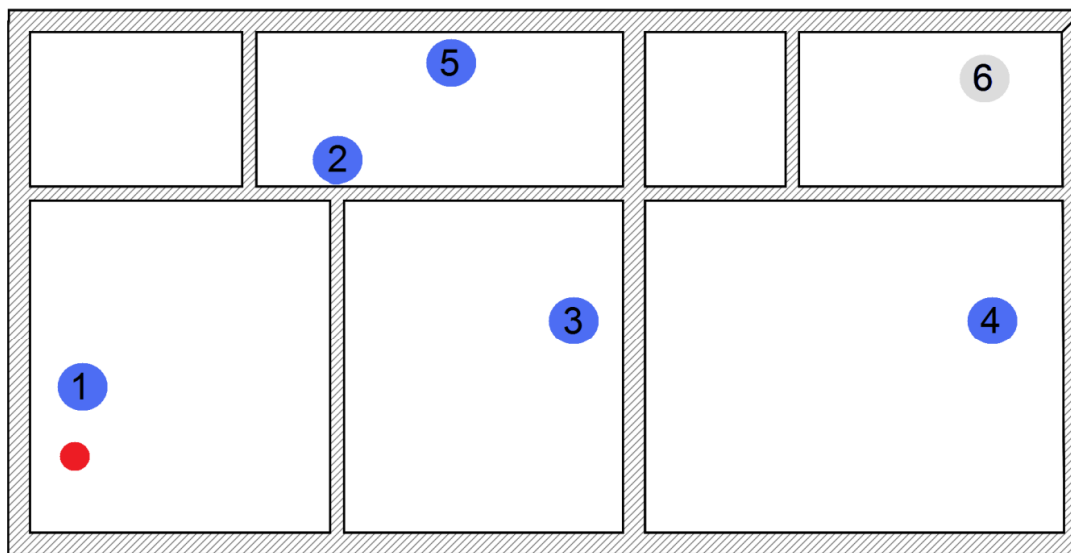
obr. 17 Závislost přenosové rychlosti na velikosti paketu



obr. 18 Závislost přenosové rychlosti na rychlosti sériového rozhraní

Z předchozích měření mi vyplynulo jako nejvhodnější použít delší pakety a přenosovou rychlost nastavit na maximum – 115 kb/s. Pro začátek jsem zkusil určit na jakou vzdálenost jsou moduly schopny spolu komunikovat. Abych mohl operovat venku, vyrobil jsem si pro napájení modulů bateriové adaptéry pro 4 tužkové baterie – to mi přišlo jako nejvhodnější pro simulaci 6V zdroje. Dále jsem nechtěl pro toto měření používat počítače, protože nemám k dispozici dva notebooky a hlavním cílem bylo určit největší dosah. Proto jsem využil potenciometru na jednom a LED diody na druhém modulu. Firmware jsem nakonfiguroval tak, aby četl hodnotu na výstupu potenciometru a cyklicky jí odesílal každých 40ms do druhého zařízení. Poté jsem oba moduly vzal do volného prostředí (louky - pole) a tam jsem zkoušel jaký dosah budou mít. Podle výrobce je maximální dosah závislý také na poloze antén. To si mi také potvrdilo. Podařilo se mi získat spojení na 60m, ovšem při změně polohy modulu komunikace občas selhávala a k její plné obnově došlo až po zkrácení vzdálenosti o 5-10m. Podle výrobce může nastat omezení dosahu způsobené změnou polohy až 20% čemuž tato čísla odpovídají.

Další částí mých měření byla komunikace v uzavřeném prostoru budovy. K měření jsem využil prostor ve kterém přebývám v Praze. Jedná se o byt 3+1 v 7. patře panelového domu. Nejdříve jsem stejnou metodikou jako v otevřeném prostředí vyzkoušel maximální dosah v uzavřeném prostoru. Tím jsem zjistil, že v této zástavbě jsou data šířena na maximální vzdálenost asi 11 m. Měřil jsem v různých místech dle přiloženého plánu. Ve všech bodech, kromě čísla 6 se mi podařilo navázat spojení a přenášet signál z analogového vstupu.



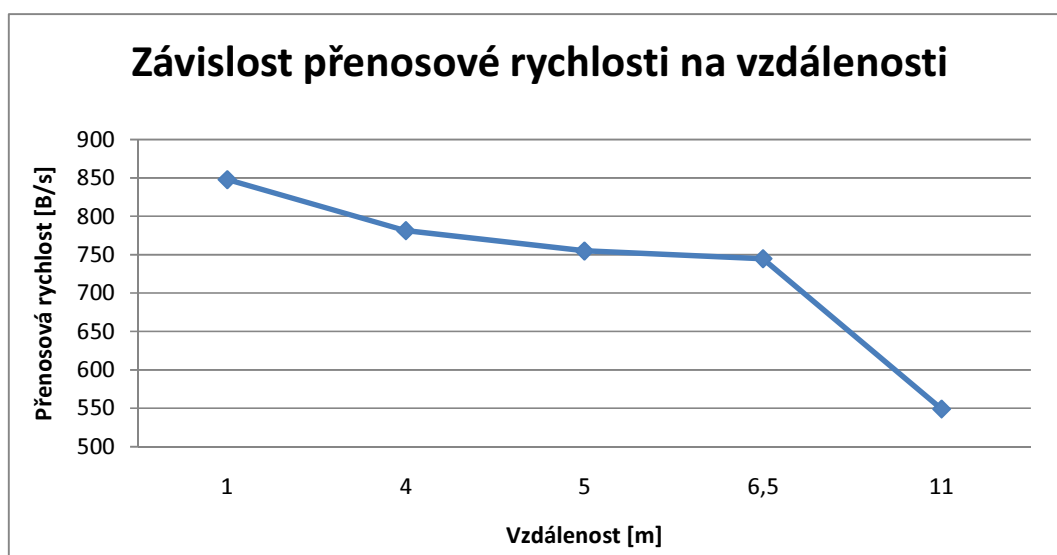
● Koordinátor
 ● Směrovač odpovídal
 ● Směrovač bez odpovědi

obr. 19 Plánek měřicích bodů

Další moje měření bylo určování přenosové rychlosti, opět v místech vyznačených na plánu. Pro měření byla nastavena délka paketu na 60 B a přenosová rychlost sériového portu nastavena na 115,2 kb/s. Pro testování jsem použil soubor o velikosti 107 kB. Komunikace probíhala ve směru od koordinátora ke směrovači. Výsledky měření jsou uvedeny v tabulce níže.

Místo	Vzdálenost [m]	Přenosová rychlost [B/s]
1	1	848
2	4	782
3	6.5	755
4	11	549
5	5	745

tab. 4 Naměřené hodnoty přenosu souboru



obr. 20 Závislost přenosové rychlosti na vzdálenosti

7. Analyzátor sítě

K dispozici jsem měl sadu pro analýzu a odposlech datových paketů v síti Zigbee. Jedná se o USB zigbee modul a software MeshDecoder od firmy Frontline. Zahájil jsem souvislou komunikaci – nejdříve mezi moduly Panasonic, později i mezi Radiocrafts.

Po spuštění programu jsem vybral prohledávání všech kanálů, abych zjistil zda nejsou v dosahu i jiné sítě a také abych ověřil svůj vysílací kanál. Po prohledání všech kanálů jsem viděl že vysílám pouze já. Vypnul jsem tedy moduly, následně zapnul odposlech na mém kanálu a opětovně zapnutím modulů Panasonoc a následným zahájením přenosu inicializoval odposlech. Pozoroval jsem, jak probíhá komunikace a data vyexportoval. Stejně měření jsem provedl mezi moduly Radiocrafts.

Na závěr jsem otevřel obě dvě komunikace a porovnal hodnoty a rozdíly.

U Panasoniců komunikace probíhala bez použití rámců. Nejdříve došlo k asociaci zařízení a poté se end node opětovně dotazoval koordinátora na data. Mezi dotazy docházelo k posílání dat směrem od end nodu ke koordinátoru. Ten na přijatá data odpovídal potvrzovacím rámcem.

Po spuštění koordinátora Radiocraft vysílat žádosti o synchronizaci (beacon) a beacon frame. To ustalo, když jsem zapojil směrovač a ten odeslal žádost o připojení do sítě. Dále probíhala jen komunikace – přenos dat → jejich potvrzení. Bylo možno vyčíst zdrojovou i cílovou adresu packetu, stejně jako PAN id sítě.

Chtěl jsem také zjistit s jakými profily moduly pracují. U Radiocraftu se mi podařil nalézt název profilu v beacon frame - Home Controls. Panasonic však synchronizaci nevysílal, takže jsem u něj našel, pouze číslo cílového endpointu – 0 , což je ZDO.

8. Demonstrační úloha do cvičení pro bezdrátový přenos s protokolem Zigbee

Pro tuto úlohu jsem se rozhodl doporučit moduly Radiocrafts. Jsou velmi jednoduché na ovládání a je možné na nich ukázat některé možnosti bezdrátového přenosu Zigbee. V zadání se zaměřím na úkoly řešené v předchozí kapitole. V první řadě student vyzkouší zda vůbec funguje přenos. Po tomto ověření aktivuje čtení z trimru na jednom modulu a jeho hodnotu bude zobrazovat jasnou LED diodu na modulu druhém. Poté vyzkouší čtení dat z potenciometru v okně pc připojeného ke koordinátoru. S využitím tohoto nastavení proměří dosah bezdrátové sítě. Další možný prvek zadání je změna nastavení směrovače jako end node. Na tom je pak možné předvést režim spánku a jeho vlastnosti. V poslední části úlohy student využije zachytávač sítě a s jeho pomocí získá přímý náhled do komunikace.

Zadání úlohy:

- 1) Připojte moduly k sériovému portu osobního počítače. Spustte na něm terminálovou aplikaci a vyberte port, ke kterému je modul připojený. Jako parametry přenosu nastavte rychlost 19,2 kb/s, 8 data bitů, 1 stop bit a řízení toku – Hardware. Potvrďte nastavené údaje. Následně zapojte do modulů napájení – nejdříve koordinátor a následně směrovač (v případě že jste ho již zapojili dříve – zmáčkněte tlačítko Reset). Koordinátor odpoví „STATUS01“ následuje „STATUS02“ a „STATUS07“. Směrovač vypíše „STATUS01“ a „STATUS02“. Tím zařízení potvrdí, že síť je zformovaná.
- 2) Pokud toto do několika vteřin moduly nevypíše (případně vypíše chybu) je třeba nastavit správné parametry sítě. Vždy při nastavování musíte nejdříve přejít do příkazového režimu příkazem „+++“.

*Další nastavující příkazy zapisujete ve formátu „ATSx=y“ kde x je adresa v zařízení a y je hodnota. Pokud chcete znát hodnotu adresy x, zjistíte jí příkazem „ATSx?“.
Pro přechod z příkazového režimu do datového použijete příkaz „AT0“.*

- 3) Úspěšnost bude potvrzena „STATUS5“. Nyní můžete psát ATS příkazy. „ATS3?“ vypíše jakou roli má zařízení nastavenou („1“ je koordinátor a „2“ je směrovač). Pokud je to třeba změnit, nastavte správnou hodnotu na adresu 3. Dále je dobré si nechat vypsát adresy 4 a 5. Adresa 5 by měla odpovídat adrese 4 na druhém zařízení. Dále nastavíte délku paketu v adrese 7 na hodnotu „1“. Tím zajistíte že každý byte se ihned odesílá.
- 4) Ověřte funkčnost A/D a D/A převodníků. Na koordinátoru do adresy 12 zapíšete hodnotu „CA“ , do adresy 14 hodnotu „0F“ a do adresy 27 hodnotu 1, čímž zajistíte nastavení

výstupu. Následně je třeba na směrovači přepsat adresu 12 hodnotou „35“, 14 hodnotou „0F“ tím se nastaví čtení dat. Pro pohodlnou komunikaci ještě nastavte cyklické čtení a odesílání dat zápisem hodnot „2“ na adresu 10 a „25“ (určuje pauzu mezi odeslanými daty 1-255) na adresu 11. To způsobí, že všechna data se budou odesílat každou 1s. Před testy je však ještě třeba provést RESET dle bodu 1). V tomto nastavení proměřte dosah modulů – se směrovačem se můžete pohybovat a při cyklické změně nastavení trimru můžete chodit po budově a výsledky následně vyčíst z terminálu, na který je připojen koordinátor (popřípadě může změny sledovat kolega).

- 5) Nyní je také vhodná chvíle vyzkoušet zachytávač sítě. Po startu jeho obslužného programu vyberte „Frame display“ a nastavte kanál přenosu Zigbee na kterém vysíláte (nebo použijte automatické vyhledávání). Nyní stačí zapnout zachytávání sítě a po jeho spuštění by se měly začít objevovat pakety vysílané mezi moduly. V tuto chvíli je dobré restartovat oba moduly, čímž dojde k vysílání paketů pro navázání spojení, které by jinak nebyly zachyceny. Po chvíli je dobré odchytávání zastavit a prohlédnout si strukturu dat, které moduly odesílají.
- 6) Pro další část měření je třeba nastavit adresy 27 na koordinátoru nastavit na „0“ a 10 na směrovači také na „0“.
- 7) Abychom mohli demonstrovat sleep mode, je třeba modul který doteď pracoval jako směrovač nastavit jako koncové zařízení. To můžete provést zápisem na adresu 3 hodnoty „3“. Poté je nutné provést RESET obou modulů. Tím začne komunikace koordinátor-koncové zařízení. Samotný sleep mode aktivujete z příkazového režimu zápisem „1“ na adresu 2. Následně přejdete do datového režimu, kdy koncové zařízení vypíše do sériového portu „STATUS11“ čímž oznámí že se uspalo. Při odeslání jakéhokoliv znaku vypíše „STATUS12“ což značí že přešel do aktivního režimu a čeká na data, aby mohl odeslat jeden packet. V našem případě k tomu dojde při odeslání jakéhokoliv znaku, protože máme nastavenou délku paketu 1B. Vyzkoušejte také odesílat znaky z koordinátora, ty však nedorazí, protože zařízení v tomto režimu nepřijímá data. Pokud je k dispozici ampérmetr, proměřte odběr obvodu při spánkovém režimu a při vysílání. Bližší data k měření odběru naleznete v datasheetu k vývojovému kitu RC2200DK. Pro ukončení tohoto režimu zapíšete do koncového zařízení na adresu 3 hodnotu „2“ čímž jej opět změníte na směrovač.

Další ATS příkazy, stavová a chybová hlášení naleznete v příloze A.

9. Závěr

V zadané práci jsem měl za úkol ověřit hodnoty uváděné specifikací Zigbee praktickým měřením. Síť modulů Panasonic jsem zprovoznil, pro omezené možnosti použitého firmwaru při přenosu a experimentování jsem s nimi ale další měření neprováděl. Jednou z možností bylo napsat firmware, ve kterém bych mohl implementovat vlastní stack. Vývojové prostředí a programátor však byly málo dostupné, proto jsem se rozhodl využít pro přenos moduly Radiocrafts. Naměřené přenosové vzdálenosti (60 m v otevřeném prostoru a 11 m v panelovém domě) splnily má očekávání. Výsledné hodnoty jsou sice na spodní hranici výrobce, ale ze zkušenosti vím, že to tak velmi často bývá. Přenosová rychlost pod 1 kB/s byla méně než jsem očekával. Pro sběr dat ze sensorů a automatizaci však plně postačuje. S využitím analyzátoru sítě jsem mohl pozorovat dva různé typy komunikace. Závěrem formuluji návrh úlohy do cvičení předmětu bezdrátových sítí.

10. Použitá literatura

- [1] IEEE, Std. IEEE Std 802.15.4-2003. *IEEEexplore* [online]. 2003 [cit. 2010-01-06].
- [2] ZIGBEE SPECIFICATION. *Zigbee.org* [online]. 2008 [cit. 2010-01-06]. Dostupný z WWW: <<http://www.zigbee.org/ZigBeeSpecificationDownloadRequest/tabid/311/Default.aspx>>.
- [3] FOX, D. Wireless Modem Demo. [online]. 2005 [cit. 2010-01-06].
- [4] FOX, D., et al. LR/WPAN PAN802154HAR Application Notes. [online]. 2005 [cit. 2010-01-06]. Dostupný z WWW: <http://www.panasonic.com/industrial/components/pdf/zigbee_appnote_1105.pdf>.
- [5] RC2200AT-SPPIO Data Sheet (rev. 0.71). [online]. 2006 [cit. 2010-01-06]. Dostupný z WWW: <http://radiocrafts.com/uploads/rc2200at-sppio_data_sheet_0_71.pdf>.
- [6] CRAIG, William C. Zigbee: "Wireless control that simply works". *Zigbee.org* [online]. [cit. 2010-01-06]. Dostupný z WWW: <http://www.zigbee.org/imwp/idms/popup/pop_download.asp?contentID=5438>.
- [7] RC2200DK Demonstration Kit User Manual (rev. 1.0). [online]. 2005 [cit. 2010-01-06]. Dostupný z WWW: <http://radiocrafts.com/uploads/rc2200dk_user_manual_1_0.pdf>.
- [8] RC220x Data Sheet (rev. 1.0). [online]. 2008 [cit. 2010-01-06]. Dostupný z WWW: <http://radiocrafts.com/uploads/rc220x_data_sheet_1_1.pdf>.
- [9] *Types of ZigBee Networks* [online]. Software technologies group, [cit. 2010-01-06]. Dostupný z WWW: <http://www.stg.com/wireless/ZigBee_netw.html>.
- [10] STEVANOVIĆ, Dusan . Zigbee / IEEE 802.15.4 Standard. [online]. 2007 [cit. 2010-01-06]. Dostupný z WWW: <<http://www.cse.yorku.ca/~dusan/Zigbee-Standard-Talk.pdf>>.
- [11] GASCÓN, David . *Security in 802.15.4 and ZigBee networks* [online]. , February 5, 2009 [cit. 2010-01-06]. Dostupný z WWW: <<http://www.sensornetworks.org/index.php?page=0903503549>>.

[12] KINNEY, Patrick . *ZigBee Technology: Wireless Control that Simply Works* . [online]. 2003 [cit. 2010-01-06]. Dostupný z WWW: <http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=5162>.

[13] DIGI, International Inc. An Introduction to ZigBee. [online]. 2008 [cit. 2010-01-06]. Dostupný z WWW: <<http://www.rabbit.com/documentation/docs/manuals/ZigBee/Introduction/>>.

[14] *Wikipedia.org* [online]. [cit. 2010-01-06]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Main_Page>.

Příloha A – Tabulky AT příkazů, adres a hlášení modulů Radiocrafts

Tabulky jsou převzaty z dokumentu RC2200AT-SPPIO Data Sheet (rev. 0.71)

Parameter	Command	Argument	Note
General			
Enter AT mode	+++		Sequence is used to switch from on-line Data Mode to on-line Command Mode while in a data call
Exit AT mode	ATO		Command is used to switch back from on-line Command Mode to on-line Data Mode.
AT test	AT		Used to verify connection to the modem. Successful communication returns 'OK'
List AT commands	ATS		Returns a list of available AT commands
Echo characters	ATEr	r=0: No Echo r=1: Echo on	Turns on/off local echo
Display Result Code	ATOQ	r=0: Do not display replies r=1: Display replies	The RF modem will reply to the command, with "OK" or with a result of the command if applicable. ATOQ can be used to turn off such replies.
Product Identification			
Identification	ATIn	n=0: Product code n=1: Product name n=2: Product revision n=3: Copyright n=4: Firmware revision	Command is used to read the products ID
Special registers / configuration registers (permanent change)			
Returns value of register r	ATSr?	For details, see Configuration Memory (S-register, table below)	Read a special register. Special register = Configuration memory register address.
Changes value of register r to n	ATSr=n		Set special register. All permanent configuration changes are done through special registers.
Returns all special register settings	ATS?		Reads back all registers. Can be used to verify settings.
Reset all special register values to default (factory settings)	ATF		This command does NOT overwrite the IEEE address at MAC_ADDR
Operating modes and test modes			
Set modem in Power Down	ATPD		Sets module in Power Down, while UART is still active
Set Power Up/Idle	ATIDLE		"Normal mode"; used to wake up after Power Down, and clear the test modes ATTX and ATRX

Set TX Mode	ATTX		Test mode only. TX mode with DTM modulation
Set RX Mode	ATRX		Test mode only. RX mode with un-buffered data UIU and DLCK available at external pins
Change operational parameters (non-permanent)			
Set Channel (Frequency)	ATChn	nn = 11 - 26	Used to change radio channel without programming default value in S-register
Set Output Power	ATPwn	n = 1 - 5	Used to change radio output power without programming default value in S-register
Set Destination Address	ATDA=XX	XX = 00-15-20-12-34-56-78	Used to change destination address without programming default value in S-register. Use IEEE MAC address format
Get Destination Address	ATDA?		Used to read the current destination address. Uses IEEE MAC address format
I/O ports			
Get ADC Set DAC	ATAr? ATAr=n	r = 0 - 7 r = 0 - 7 n = 0 - 1023	Read local ADC channel r Set local DAC channel r to n
Get general I/O port	ATDr?	r = 1 - 2	Read digital I/O from port r (1 or 2)
Set general I/O port	ATDr=n	r = 1 - 2 n = 0 - 255	Set digital I/O on port r (1 or 2) to n

Error code	Message	Possible cause for error message
WARNG01	Test mode warning	This warning message will be displayed when the commands ATTX, ATRX and ATPD are issued to indicate that command ATIDLE should be issued to return back to normal mode
WARNG02	No paired device warning	This warning message may be displayed when the command AT0 is issued. This warning indicates that the device is not paired successfully and thereby does not enable Data transfer. Data transfer is supported only when it is paired successfully with another device.
WARNG03	End Device in sleep mode warning	This warning message will be displayed for any AT command (except for AT0 and ATS2=0) issued to an end device that is in sleep mode following an external interrupt through UART. The device should be put back to normal state by issuing AT0 or ATS2=0.
WARNG04	End Device sleep mode not paired warning	This warning message will be displayed when the command ATS2=1 is issued in RFD and the device is not paired successfully and thereby does not enable Sleep mode. Sleep mode is supported only when it is paired successfully with another device.
ERROR01	Bad command	If the first character is a value other than 'A', or if the <Enter> key is pressed before the first character
ERROR02	<Reserved>	<Reserved for future use>
ERROR03	Not allowed	If ATS2=1 is executed on a FFD (Coordinator or Router), or if Packet Interval value is set to 0
ERROR04	Parse failure	Wrong AT command, or some undefined character
ERROR05	Value already set	When a device is to be set to sleep mode (ATS2=1), when already in sleep mode.
ERROR06	Illegal port operation	If the command ATAr=n is issued when the port pin is not configured as analogue pins.
ERROR07	Illegal port operation	If the command ATAr=n or ATDr=n is issued when the port pin is set as input pin.
ERROR08	Invalid Value	Value is out of range
ERROR09	Illegal format or value	When destination MAC address (ATS5) is issued in an invalid format, or the address of the device (local address) is given as the destination MAC address.
ERROR10	Illegal format	When the address of the device (ATS4) is issued in an invalid format.
ERROR11	Illegal configuration	When the device is to be configured as a coordinator (ATS3=1), when it is in Sleep Mode.
ERROR12	Illegal command	When any other command other than ATIDLE is issued after ATTX, ATRX and ATPD commands.

Status code	Message	Note
STATUS01	Entered Init State	After Reset
STATUS02	Exited Init State	After successful booting
STATUS03	Network Formation Complete	When Coordinator has formed a new network
STATUS04	Network Join Complete	When Router or End Device has joined a network
STATUS05	Entered Command Mode	After '+++'
STATUS06	Entered Data Mode	After AT0
STATUS07	Device Paired Successfully	After successful pairing with node with destination address
STATUS08	Device Pairing Failure	If pairing with node with destination address fails
STATUS09	Entered Power Down mode	After ATPD
STATUS10	Exited Power Down mode	After UART port interrupt
STATUS11	Entered Sleep mode	After ATS2=1 and AT0
STATUS12	Exited Sleep mode	After ATS2=0

Příloha B – Tabulka přenosových pásem

PHY	Oblast působnosti	Frekvenční pásmo	Počet kanálů	Modulace	Datové parametry		
					Přenosová rychlost	Symbol rychlost	Modulace
868/915 MHz	Severní amerika, Austrálie	915 MHz	0	BPSK	20 kb/s	20 kbaud	BPSK
	Evropa	868 MHz	10	BPSK	40 Kb/s	40 kbaud	BPSK
2.4 GHz	Globální	2.4 GHz	16	O-QPSK	250 kb/s	62.5 kbaud	16-tková Ortogonální