Metody a způsoby bezdrátového přenosu dat ze snímačů na centrální jednotky

Methods and processes of wireless communication between sensors and central units

Petr Dlabač

Bakalářská práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Petr DLABAČ**
Osobní číslo:	**A10111**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Metody a způsoby bezdrátového přenosu dat ze snímačů na centrální jednotky**

Zásady pro vypracování:

1. Zpracujte analýzu zadání.
2. Vypracujte literární rešerši o metodách a způsobech přenosu.
3. Uveďte seznam teorie související s přenosem dat.
4. Porovnejte praktické aplikace přenosů WLAN a WPAN.
5. Uveďte možnosti měření kvality přenosu dat.

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. DYER, S., A. Survey of istrumentation and measurement. John Wiley and Sons, 2001, s. 1096. ISBN 0-471-39484-X.
2. Altmann W. Practical Process Control for Engineers and Technicians. ELSEVIER, 2006, s. 290, ISBN 978-0-7506-6400-4
3. Tumanski, S. Principles of electrical measurement. Taylor &Francis, Boca Raton, s. 472, ISBN 0-7503-1038-3
4. WEBSTER, J., G. The measurement, instrumentation, and sensor handbook. New York: CRC Press LLC; Springer-Verlag, 1999, s. 1932. ISBN 3-540-64830-5
5. HRUŠKA,F. Technické prostředky informatiky a automatizace. Učební texty. 1.vyd. Zlín: UTB ve Zlíně, duben 2007, s.193. ISBN 978-80-7318-535-0
6. HRUŠKA,F. Senzory pro systémy informatiky a automatizace. Učební texty. 1.vyd. Zlín: UTB ve Zlíně, prosinec 2007, s.177. ISBN 978-80-7318-630-2

Vedoucí bakalářské práce: **doc. Ing. František Hruška, Ph.D.**
Ústav elektroniky a měření

Datum zadání bakalářské práce: 25. února **2013**

Termín odevzdání bakalářské práce: **30. května 2013**

Ve Zlíně dne 25. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Bakalářská práce se ve velké míře zabývá bezdrátovým přenosem dat ze snímačů na centrální jednotky. V teoretické části se popisují jednotlivé metody a způsoby, jak lze bezdrátového přenosu docílit a rozdělí se na jednotlivé propojovací úrovně. Shrneme si také teorii, která se k bezdrátovému přenosu váže. Praktická část této práce se vztahuje k praktickým aplikacím WPAN a WLAN s důrazem na jejich porovnání. V závěru se popisuje metoda, jak lze měřit kvalitu bezdrátového přenosu. Součástí je praktická ukázka měření s moduly ZSTAR2 a ZSTAR3.

Klíčová slova: Bezdrátový přenos, snímač, centrální jednotka, WPAN, WLAN, měření, ZSTAR3

ABSTRACT

This thesis largely deals with wireless data transmission from sensors to a central unit. The theoretical part describes various methods and ways wireless transmission is achieved and how it is devided to each interface level. We summarize theory which relates to wireless transmission. The practical part of this work relates to practical applications of WPAN and WLAN with an emphasis on their comparition. In the end, we describe method how to measure quality of wireless transmission. Practical demonstration of measurement on modules ZSTAR2 and ZSTAR3 is included.

Keywords: Wireless transmission, sensor, central unit, WPAN, WLAN, measurement, ZSTAR3

Tímto bych rád poděkoval vedoucímu své práce doc. Ing. Františku Hruškovi, PhD. za vedení mé bakalářské práce, návrhy, konzultace a poskytnutí materiálů a pomůcek. Rád bych také poděkoval přátelům a rodině, kteří stáli při mně při psaní této práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD

Historie prvních přenosů pomocí drátů spadá hluboko do dějin lidstva. Lidé měli odjakživa tendenci komunikovat mezi sebou a není proto divu, že se komunikace na větší vzdálenost stala předmětem výzkumu nejednoho vědce. V době vzniku telegrafů si ještě asi málokdo dokázal představit komunikaci bezdrátově. Věda ovšem šla nezadržitelně kupředu a ještě ke konci 19. století se povedl první přenos bez kabelů na vzdálenost asi dva kilometry.

Mílovými kroky pak vědci hlavně v druhé polovině 20. století přicházeli se stále lepšími a novějšími metodami bezdrátového přenosu. Přičemž 90. léta a rozmach osobních počítačů v domácnostech měly za následek další vývoj a snahu o zvyšování přenosových rychlostí a také zpřístupnění pro běžného uživatele.

Dnes není bezdrátový přenos ničím neobvyklým. Existuje několik organizací, které se zabývají přímo vývojem protokolů a standardů, které s ním souvisí. To má za následek větší variabilitu a škálovatelnost pro koncového uživatele. Z hlediska využití se tak pracuje na bezdrátových přenosech, které se využijí v domácnostech, na cestách, v průmyslové automatizaci nebo ve zdravotnictví. To je pouze výčet základních míst, kde se přenos signálů ze senzorů na centrální jednotku využije.

Žijeme v době, kdy spousta lidí nestíhá a potřebuje být stále mobilní a přitom v kontaktu se světem. Není proto vhodnější uplatnění mobilních datových přenosů, kdy si uživatel zjistí jakékoliv informace prakticky odkudkoliv za pochodu. Komunikace na stovky kilometrů se stále zdokonalují s příchodem nových standardů, které pomocí novějších modulací a přenosových technik umožňují čistší a stabilnější signál. Ruku v ruce s rozvojem zařízení, které nám bezdrátový přenos umožňují, tak dosahujeme opravdu vysokých přenosových rychlostí, ať jsme kdekoliv. Online video konference, nebo pouze konference v rámci jedné bezdrátové sítě již také dávno nejsou vizí budoucnosti.

I. TEORETICKÁ ČÁST

1 ANALÝZA METOD A ZPŮSOBŮ BEZDRÁTOVÉHO PŘENOSU DAT ZE SNÍMAČŮ NA CENTRÁLNÍ JEDNOTKY

Nejnovějším trendem ve světě komunikací je pro informační systémy bezdrátové připojení a LAN pracující s protokolem I-Ethernet. Bezdrátový přenos se pro své vlastnosti se stává nepostradatelnou součástí domácností či firem. Vezmeme-li v potaz historii a rozvoj automatizace či informatiky, není divu, že blízká budoucnost bude patřit systému integrované automatizace. Jedná se tak o propojování systémů informačních s těmi automatizovanými. Zmínit můžeme propojení SIA a GSM telefonů pomocí internetu. Blíže se o jednotlivých vlastnostech dozvíme v následujících kapitolách.[1]

Důležitou roli při propojování a přenosu dat hraje bezpečnost. S tím souvisí rozvoj bezpečnostních protokolů a standardů. V dnešní době, kdy útoky hrozí ze všech stran, se výrobci musí snažit eliminovat potencionální hrozby právě bezpečným datovým tokem. Platí, že systém funguje jako jeho nejslabší článek. V tomto případě, máme-li bezdrátový přenos pro nějaký bezpečnostní systém, nelze opomenout zabezpečit právě datovou komunikaci. Uživatelé jsou si toho také vědomi a mají možnost si většinou vybrat ze zabezpečení, které právě jim padne na míru. V honbě za klientem se tak výrobci snaží přijít se stále lepšími variantami, které jsou daleko bezpečnější a uživatelsky přístupnější. Opomenout jako jednu z variant přenosu dat nelze ani roli Internetu, který je dnes už dostupný prakticky všude. Ať už jej využíváme jako Wi-Fi přístupový bod nebo máme mobilní internet. Internet nám tedy umožňuje se z lokální úrovně objektu propojit s celým světem v reálném čase. Toho využívá v dnešní době spousta zařízení.[2]

1.1 Komunikace v SIA

Metody a způsoby bezdrátového přenosu dat spadají pod SIA. Systémy integrované automatizace jsou využívány ve všech oborech a oblastech. Ať už se jedná o průmysl, zemědělství, či státní správu, nebo dokonce v domácnostech v rámci inteligentních domů, které jsou ruku v ruce s rozvojem techniky k vidění stále častěji.[2]

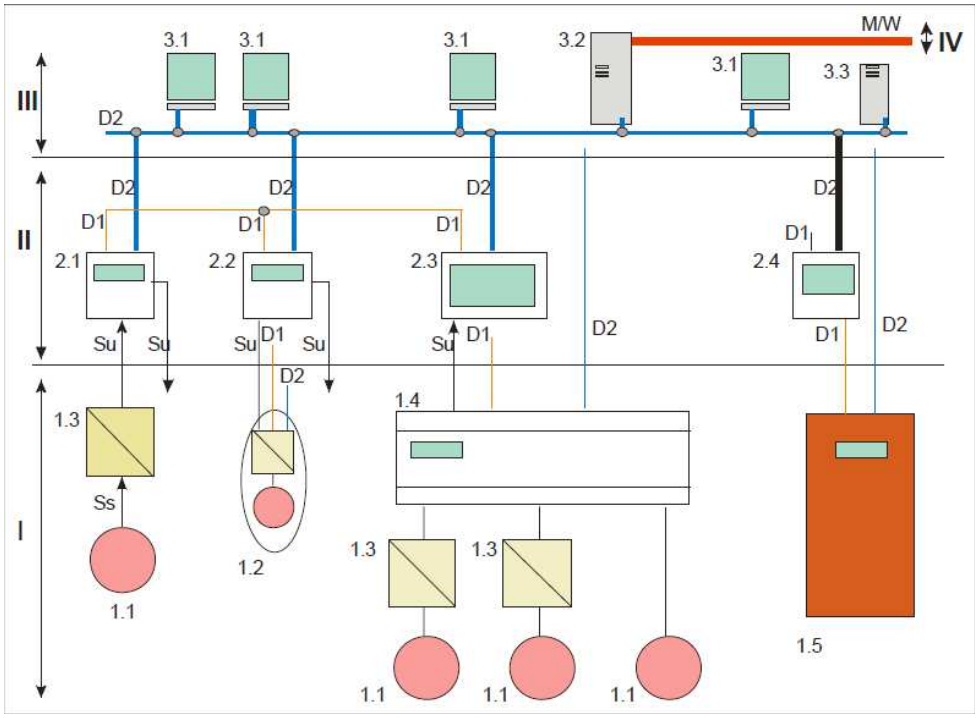
Využití různých technických a programových prostředků nám umožňuje v systému SIA komunikaci a přenos dat mezi sebou. Musí být zajištěno kvalitní fyzické i logické propojení veškerých struktur, abychom docílili spolehlivé a bezpečné funkce SIA.[2]

Na SIA pohlížíme jako na čtyři základní úrovně přenosu dat (Tab. 1). Spojíme-li všechny čtyři úrovně logicky dohromady, vznikne nám systém, který máme zobrazen na obrázku (Obr. 1).

Tab. 1 Základní úrovně komunikace v SIA

I. Úroveň - signálová periférní	**Su, Sn -** komunikace
Přenos pomocí signálů mezi snímači, akčními členy a podsystémem. Signály máme unifikované (Su) a neunifikované (Sn).	Napájecí zdroje Napájecí kabely Propojovací signální kabely
II. Úroveň - datová podsystémů (SAN)	**D1**
Přenos celých bloků údajů mezi podystémy.	RS232, USB, RS485 ZigBee, Blueetooth, EnOcean IrDa, GSM
III. Úroveň - datová lokální (LAN)	**D2**
Přenos informací mezi podsystémy v rámci jednoho systému.	TCP/IP, I-Ethernet, Wi-Fi
IV. Úroveň - datová vnější (WAN,MAN)	**D3**
Přenos informací do vnějšího prostředí.	Přenos mezi městy a ve světě
GSM – Datový mobilní přenos	Audio a datové přenosy

Na obrázku (Obr. 1) je zobrazena komunikace a propojení jednotlivých úrovní SIA. Úroveň I. se skládá ze snímačů a vyhodnocovacích jednotek. K přenosu na této úrovni dochází pomocí signálu neunifikovaného či unifikovaného (Sn, Su). V úrovni II. se již věnujeme přenosu pomocí datových podsystémů PAN, zde značeno jako D1 a ve III. úrovni lokální datový přenos LAN značen jako D2. Zobrazen je i IV. úroveň pomocí M/W, což nám značí již přenos informace do vnějšího prostředí jako je město či stát.[2]



Obr. 1 Obecné schéma propojení v SIA[1]

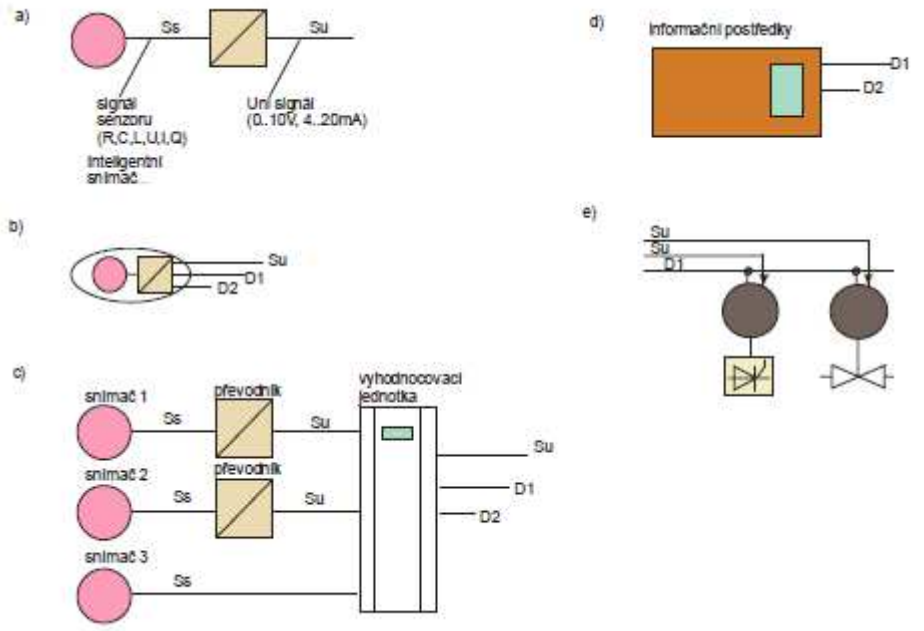
2 LITERÁRNÍ REŠERŠE O METODÁCH A ZPŮSOBECH PŘENOSU

2.1 Propojovací systémy signální úrovně

Jedná se o nejnižší úroveň propojovacích systémů. Spadá do oblasti, kde se sbírají data z různých měření nebo nasnímaná data. Tyto se pak potřebují přenést na další úroveň. Z hlediska výstupu v jakém vzešli, můžeme tyto varianty rozdělit na tři. Buďto že tyto data mají výstupní signál unifikovaný, s datovým výstupem D1 nebo již s datovým výstupem D2.[2]

Propojení a přenos dat na této úrovni se koná za pomoci signálů elektrických, elektromagnetických a jiných. Signálem je myšlena hodnota informace, kterou bychom mohli nejčastěji vyjádřit pomocí elektrického napětí, které se pohybuje v rámci (0 až 10V), elektrického proudu v rozsahu (4 až 20mA DC), či dalších parametrů jako je elektrický odpor, náboj nebo indukčnost. Prostředkem pro propojení je u bezdrátového přenosu například infračervené záření nebo laserový paprsek.[2]

Máme několik možností propojení na signální úrovni (Obr. 2). První variantou (a) je, že snímač má jako výstup signál neunifikovaný, který se při napojení na převodník mění na signál unifikovaný. Další variantou (b) je pokud snímač má nejenom senzor, ale i obvod s mikrokontrolérem na vyhodnocování, čímž dostaneme výstup, jako unifikovaný signál Su, propojení D1 či D2. Pak tedy mluvíme o inteligentním snímači. Třetí varianta (c) se využívá u komplikovanějších obvodů a jedná se o zapojení více snímačů na jednotku, která provádí další vyhodnocení. A jak je možno vidět na obrázku (Obr. 2) výstupem je opět Su, D1 nebo D2. Varianta čtyři (d) využívá informační prostředky k zjišťování a sběru dat. Poslední variantou (e) je možnost propojení pomocí ovládacího zařízení.[2]



Obr. 2 Schéma signálních propojení[1]

Využití této nejnižší úrovně má v praxi své přednosti. Vysoká přenosová rychlost, která se blíží k rychlosti světla. Výborně si vede i co se doby odezvy týče. Výhodou je i jednoduché propojení, spolehlivost a pořizovací cena se také pohybuje nízko. Jelikož se ale jedná o opravdu základní propojení, má ve srovnání s vyššími úrovněmi i svá úskalí. Jednou z nich je omezenost při nastavení rozlišení, nelze tak vyloučit vznik možných odchylek. Další nevýhodou je, že transformace námi měřené veličiny má omezený rozsah. Je tak těžké pracovat s některými daty, chceme-li je transformovat na signál 0-10V, ve kterém se pohybují.[2]

2.2 Propojovací systémy datové úrovně D1/SAN

Úroveň D1 nám umožňuje přenos dat, nejedná se ale o jednoduché signály či impulsy. Jde již o větší množství dat, často v rámci bloků nebo jako zpráva, díky které mezi sebou mohou komunikovat jednotky podsystémů dané úrovně. Jde o sériové propojení, jak už z názvu SAN může vyplynout. Často se můžeme setkat také s pojmem PAN, který je dále probírán v dalších kapitolách, ale setkáme se s ním již za nedlouho. V jednotlivých bodech propojovacích systémů datové úrovně D1 totiž vyzdvihneme přednosti a poukážeme na případné nedostatky daných variant.[2]

V domácnostech se můžeme ještě setkat s propojením RS232, který je již většinou nahrazen komfortnější variantou USB. Ten je rozšířen a je nedílnou součástí každého prodávaného počítače nebo notebooku. Vývojáři jsou si toho vědomi a neustále přichází s dalšími vylepšeními. Ke stávajícímu datu je nejrychlejší varianta USB 3.0 a brzy na sebe nenechá čekat ani varianta 4.0. Málo rozšířená, ale velký potenciál má také wireless USB.[2]

Možnosti přenosů u bezdrátových i klasických drátových variant jsou zobrazeny v tabulce (Tab. 2). Modrá část tabulky nám značí klasické varianty PAN a žlutě jsou zobrazeny bezdrátové varianty PAN. Bezdrátové možnosti budou podrobněji rozebrány v následujících kapitolách.

Tab. 2 Možnosti přenosů v rámci PAN

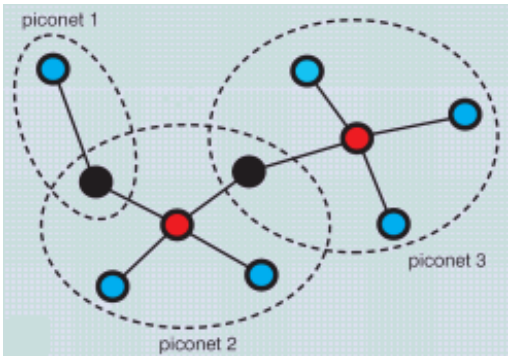
RS232	Bluetooth
RS485	ZigBee
USB	IrDa
Hart	WirelessHart
LonWorks	ISA 100.11a
SPI	WiMedia, UWB
ASI	EnOcean
I2C	Proprietární varianty

2.2.1 Bluetooth

Bluetooth je technologie využívající bezdrátovou komunikaci, na základě které nám dovolí propojit dvě či více zařízení. Tato technologie je již delší dobu standardem u mobilních telefonů novějšího typu. Objevuje se také stále častěji u přenosných počítačů jakožto varianta rychlé komunikace s ostatními zařízeními. Jde také o nedílnou součást náhlavních souprav, či PDA. U sad typu handsfree (Obr. 3), kde se výrobci neustále snaží minimalizovat rozměry, je Bluetooth standardem.[2]

Obr. 3 Handsfree s technologií Bluetooth[1]

Bluetooth nám umožňuje skrze jeden přijímač v počítači připojit až 7 dalších zařízení s technologií Bluetooth. Takovým propojením vzniká piconet, skládající se až z 8 zařízení. Z tohoto uspořádání tedy vyplývá, že se jedná o model Master-Slave. Lze však vytvořit také klasickou dvoubodovou komunikaci. Co se týče piconetu, základní specifikace nám dovoluje využít zároveň až 10 pikosítí v prostoru s průměrem 10 metrů. Sdružení takových sítí se nazývá tzv. „scatternets“ a je vyobrazeno na obrázku (Obr. 4), kde červeně jsou vyznačeny řídící jednotky, modře řízené jednotky a nakonec černě jsou vyznačeny jednotky, které jsou společné pro dvě buňky piconet.[3]



Obr. 4 Scatternet, neboli sdružená síť[3]

Je definován standardem IEEE 802.15.1., a tak patří mezi osobní sítě typu PAN. Pracuje v ISM pásmu 2,4 GHz podobně jako Wi-Fi. Máme několik druhů verzí, uvedeny jsou v tabulce (Tab. 3).

Tab. 3 Vlastnosti jednotlivých verzí Bluetooth[2][4][11]

Verze	Přenosová rychlost	Maximální propustnost	Vlastnosti
1.1	1 Mbit/s	0,7 Mbit/s	Nešifrované kanály
1.2	1 Mbit/s	0,7 Mbit/s	Přeskakování frekvencí (AFH)
2.0 + EDR	3 Mbit/s	2,1 Mbit/s	pi/4- DQPSK a 8 DPSK modulace
2.1 + EDR	3 Mbit/s	2,1 Mbit/s	SSP, rozšířené informace EIR
3.0 + HS	54 Mbit/s	24 Mbit/s	Vysokorychlostní přenos přes Wi-Fi
4.0 BLE	1 Mbit/s	0,7 Mbit/s	Dual – mode nízká spotřeba energie

Jelikož se jedná o bezdrátovou technologii, obrovskou roli hraje místo, kde ji využíváme. V oblasti bez překážek tak dosáhneme lepší kvality signálu na větší vzdálenosti oproti místům, kde se nachází třeba zdi. Při takové situaci, kde komunikaci brání překážka, se sníží kvalita signálu a narůstá množství paketů, které nedorazí správně.[2]

Stejně jako u Ethernetu slouží MAC adresa, i Bluetooth má svou adresu. Jedná se o BT_ADDR pomocí kterého lze všechna zařízení jednoznačně v síti identifikovat.[2]

Je zde použita metoda FHSS, která uskuteční 1600 přeladění mezi 79 frekvencemi s rozestupem 1 MHz v průběhu jedné vteřiny. Toto napomáhá v konečném důsledku navýšit odolnost spojení proti interferenci na téže frekvenci. Existují tři úrovně dle výkonnosti (Tab. 4).[2]

Tab. 4 Výkonnost verzí Bluetooth[17]

Úroveň	Dosah	Výkon
1	100m	100mW
2	10m	2,5mW
3	1m	1mW

2.2.2 IrDA

Organizace Infrared Data Association uvedla IrDA jako technologii využívající infračervené paprsky ke komunikaci dvou zařízení na malou vzdálenost. Standard IrDa byl vytvořen, abychom mohli propojit zařízení tak, aby spolu bezdrátově komunikovaly. K hlavnímu využití patří spojení personálních komunikátorů, notebooků, setkat se s nimi můžeme ale i u videokamer. Nejčastěji se s ní setkáváme u mobilních telefonů. Obrovskou

nevýhodou je nutnost přímé viditelnosti obou zařízení. Nízká je navíc také přenosová rychlost, která oproti např. Bluetooth dosahuje pouze rychlosti 2,4kbit/s až 16Mbit/s. Častěji je nasazován standard Bluetooth, který IrDA předčí prakticky ve všech vlastnostech. Zařízení pomocí IrDA vysílají a přijímají modulované infračervené záření, jež má vlnovou délku 875 nm. Jako přijímač se používá PIN fotodioda a jako vysílač infračervené LED diody.[2]

Zařízení, které rozhraní IrDA využívají, pracují podle norem IrDA 1.0 s maximální přenosovou rychlostí až 115,2 Kbps do vzdálenosti cca 1m a IrDA 1.1 s maximální přenosovou rychlostí až 4Mbps. Stejně jako Bluetooth patří tato technologie do kategorie osobních počítačových sítí PAN.[17]

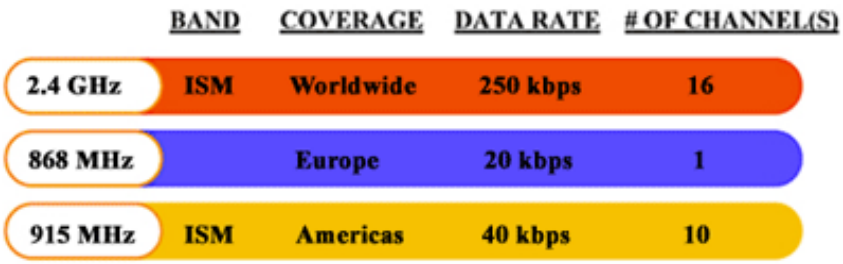
Je několik součástek, které IrDA využívají. Vyrábí se jak IrDA vysílače a přijímače, tak i transceivery, což je integrace přijímače s vysílačem do jednoho celku. Na obrázku (Obr. 5) máme zobrazen zdroj a senzor infračerveného záření, který je nedílnou součástí, chceme-li IrDA využívat.[2]

Obr. 5 Zdroj a senzor IR[1]

2.2.3 ZigBee

ZigBee je bezdrátová technologie, která řeší problémy s kabeláží. V průmyslových oblastech činí zavedení kabelů až 80% nákladů na instalaci senzorů. Mnohdy z důsledku komplikovaného přístupu není drátové provedení možné. Problém nastává u většiny bezdrátových senzorů s nutností velkého množství energie, které spotřebují pro svůj chod. Mají buďto příliš velké baterie, nebo se musí baterie vyměňovat příliš často. Mnozí navíc oponují názorem, že data šířená vzduchem nejsou dostatečně spolehlivě přenášena.[5]

Nízkoenergetická technologie ZigBee zcela zásadně měnila pohled na bezdrátové senzory. Bezpečná síťová technologie fungující na standardu IEEE 802.15.4 a patřící od roku 2004 díky ZigBee alianci podobně jako Bluetooth do sítí PAN pro malé vzdálenosti. Oproti IrDA nevyžaduje přímou viditelnost zařízení a proto je vhodná pro průmyslovou automatizaci. V závislosti na lokalitě se také liší jednotlivé frekvenční pásma pro ZigBee. S tím souvisí také různé přenosové rychlosti a počty kanálů. Rozdělení dle šířky pásma je na obrázku (Obr. 6).[5]



Obr. 6 Frekvence a přenosová rychlost ZigBee[5]

Vzhledem k nízkým přenosovým rychlostem (Obr. 6) nelze počítat s přenosem větších dat jako je tomu u Bluetooth či Wi-Fi. ZigBee hledá využití při přenosu signálů ze snímačů, které jsou často v řádech bytů. Tyto signály dokáže přenášet do vzdálenosti až 100m. Výhodou je i možnost podpory velkého množství zařízení. Díky fungování v nízkých šířkách pásma ZigBee uzly mohou přečkávat ve spánku, čímž šetří baterii, a probudit se až když je potřeba odeslat data. Nízké je i zpoždění pro dobu vstávání, pohybuje se kolem 15msec, což je oproti Bluetooth velká výhoda, u něj totiž toto zpoždění činí v průměru 3 vteřiny.[5]

ZigBee má na výběr ze tří módů. První se snaží udržet své přenosy od překrývání vysílání ostatními uzly, čímž spotřebuje mnoho energie a z tohoto důvodu to není příliš efektivní volba. Druhou variantou je majákový mód, kdy řídící uzel pravidelně probouzí kontrolované uzly a předává jim synchronizační informace. Časté probouzení a příjem dat zvyšuje potřebnou dodávku energie. Existuje ještě poslední varianta pro Zigbee, In-Your-Face-Communication, s nejnižšími nároky na spotřebu. Funguje na principu přeposílání údajů pouze pokud je připraven data poslat a následně vyčká na potvrzení.[5]

Síť ZigBee má tři typy zařízení, které dohromady utváří síťovou topologii, jako je tomu uvedeno na obrázku (Obr. 7).

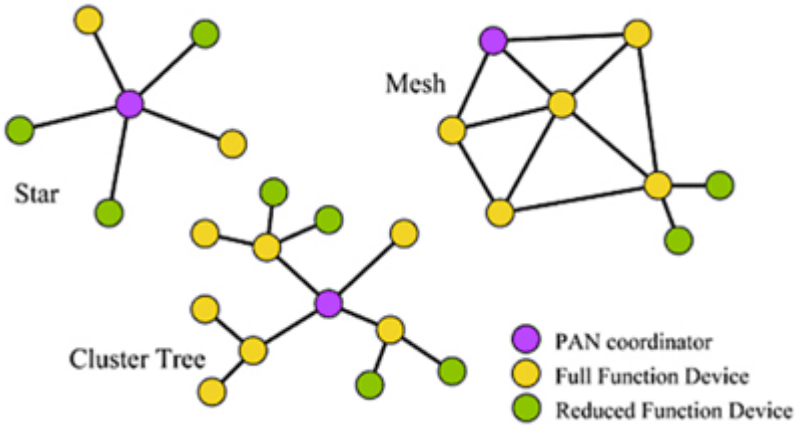
- PAN coordinator – Jak je vidět z obrázku (Obr. 7), PAN koordinátor se nachází v topologii vždy pouze jednou. Jeho hlavní funkcí je koordinace a ukládání dat o síti. FFD i RFD jsou odkázány ke komunikaci právě s koordinátorem sítě.
- FFD – Každá síť ZigBee potřebuje ve své topologii alespoň jedno plně funkční zařízení, které poskytuje vše, co může ZigBee nabídnout. Může se jednat o router, či repeater.
- RFD – Mohou komunikovat pouze s FFD, snižují spotřebu kvůli nižším nárokům na paměť. Jedná se o ořezanou variantu FFD pouze s knihovnami, které jsou potřebné pro chod (koncová zařízení).[5]

FFD zásobník spotřebuje kolem 32kB a RFD zásobník pouze asi 4kB, což jen potvrzuje výborné nízkospotřebové vlastnosti oproti konkurenčnímu Bluetooth, který potřebuje asi 250kB.

ZigBee může fungovat ve třech síťových topologiích (Obr. 7). První topologií je topologie hvězda, dále strom a nakonec topologie mesh.

Topologie mesh je nejdůležitější funkcí pro bezdrátový přenos. Jelikož je takový přenos ovlivněn počasím, teplotou, vlhkostí a překážkami, je tato topologie potřebná pro vypořádání se s tímto rušením, zejména pak v průmyslovém prostředí. Důležité jsou zejména následující vlastnosti:

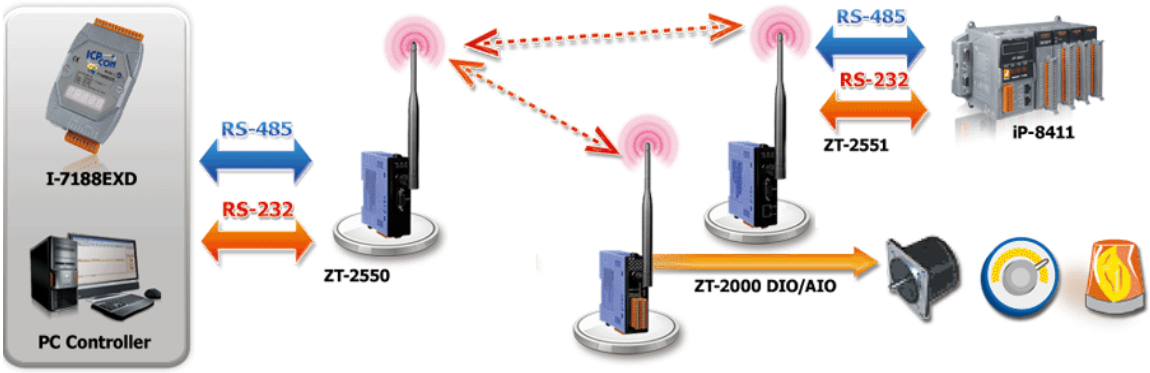
- Najde-li mesh síť nový uzel, automaticky ho přidá do aktuální sítě.
- Pokud uzel nefunguje, najde mesh síť jinou cestu, kudy předá data do dalšího uzlu.
- Přidáním dalších opakovacích uzlů do sítě nám tak umožní mít pro každý uzel víc než dvě možné cesty pro přenos.[5]



Obr. 7 Možnosti topologie sítě[5]

Nemalou zásluhu na nízké spotřebě u ZigBee má také fakt, že využívá k přenosu datového signálu DSSS (direct-sequence spread spektrum) technologii. Jak jsem se již zmínil u Bluetooth, ten využíval FHSS, což je alternativa, která kvůli synchronizaci četnosti skoků vyžaduje mnohem víc energie než DSSS. Metoda CSMA/CA nám umožňuje kontakt s fyzickým médiem. Bezpečnost ZigBee je řešena pomocí šifrování AES s užitím 128 - bitového klíče.[5]

Na obrázku (Obr. 8) uvádíme příklad výrobku ZigBee od firmy ICP DAS. Jedná se o konvertory ZT-2550 a ZT-2551. Umožňuje nám konvertovat RS-232 a RS-485 rozhraní na ZigBee PAN síť. Tato řada konvertorů ovšem může sloužit jako ZigBee router a tím umožňuje rozšířit signál v rámci až 700m. Dokážou vytvořit síť s jedním hostem (ZT-2550) a další ZigBee zařízení pak fungují jako slaves (ZT-2551). Fungování takové sítě je znázorněné na obrázku (Obr. 8).[6]



Obr. 8 Aplikace ZigBee zařízení do stávající situace[6]

2.2.4 EnOcean

EnOcean je bezdrátový standard optimalizovaný pro ultra nízkou spotřebu energie. Vydala ho organizace IEC jako standard ISO/IEC 14543-3-10. Zařízení, které tento standard využívají, nepotřebují baterii a není tak potřeba žádné údržby a výměn zdrojů. Senzory dokážou čerpat energii ze svého okolí, například ze světla, pohybu či teplotních rozdílů. Jednotlivé formy získávání energie jsou zobrazeny na obrázku (Obr. 9). EnOcean se využívá pro průmyslovou automatizaci nebo automatizaci budov. Dokáže spolupracovat s většinou drátových systémů jako je KNX nebo LON.[7]

Tento standard pokrývá první až třetí vrstvu OSI. Jeho dosah se na volném prostranství pohybuje okolo 300m a v budově až 30m. To vše za využití enormně malého množství energie. Klíčem je provedení celého přenosu ve zlomku vteřiny. Využívá se frekvenčního pásma 868MHz nebo 315MHz. Přenosová rychlost se pohybuje okolo 125kbit/s s využitím ASK modulace, nelze tedy počítat s přenosem větších dat. Kompletní výčet vlastností tohoto standardu lze získat ze stránek www.iso.org.[7]

Obr. 9 Konvertor tepla, solární panel a konvertor pohybu pro EnOcean[7]

2.2.5 WirelessHART

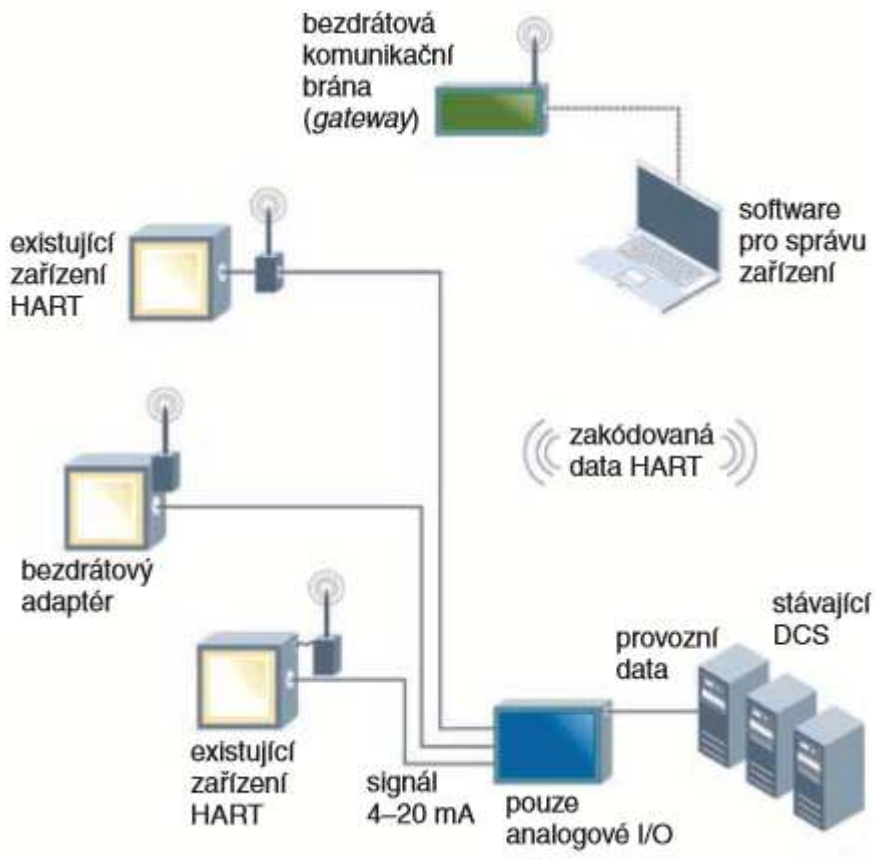
Organizace Hart Communication Foundation vytvořila protokol WirelessHART, aby zkvalitnila propojitelnost prvků u měření. Zásadním bodem je, že se jedná o propojení bezdrátové s využitím zejména v automatizaci. Jedná se o nadstandard protokolu HART konkrétně situovaný v signální propojovací úrovni. Specifickou vlastností je nemožnost komunikace s jinými zařízeními, než těmi od společnosti HART. Tento bezdrátový standard je natolik všestranný, že je možné jej využívat i k detekci netěsností. WirelessHart protokol je také, co se týče bezdrátového přenosu dat, prvním protokolem v oblasti řízení spojitých technologických procesů, jež byl standardizován v Evropě.[10]

Užívá rádiový standard IEEE 802.15.4 ve frekvenčním pásmu 2,4GHz, podobně jako většina bezdrátových řešení. Na základě paketů nám umožňuje přepínání kanálů. Veškeré data a přenosy jsou bezpečně přenášeny a zašifrovány pomocí AES-128 bit. Přístup k médiím je umožněn pomocí technologie TDMA. Nejčastěji využívá topologii mesh, je možné využít i hvězdicovou variantu. Za zmínku stojí obrovský dosah mezi dvěma zařízeními, který činí až 250m.[9]

Prvky, které dohromady tvoří WirelessHART síť jsou:

- Signální snímač, který má zabudovaný protokol WirelessHART.
- Bezdrátová komunikační brána zajišťující styk s centrální jednotkou.
- Bezdrátové adaptéry, bez kterých nelze do sítě připojit zařízení.[16]

WirelessHart je možné přidat již do stávajícího řešení HART. Taková situace je zobrazena na obrázku (Obr. 10). V tomto řešení existuje už několik zařízení HART, které komunikují pomocí analogového signálu 4-20 mA s DCS. Přidání bezdrátového řešení do takové situace lze vyřešit připojením potřebných zařízení WirelessHART. Jedná se o síť mesh, není tedy důležité, aby byly všechny zařízení v dosahu brány, ale hlavně aby byly v dosahu dalšího zařízení v síti. Je potřeba mít také software pro správu všech zařízení. Ten nám umožňuje sledovat komunikaci mezi zařízeními, cestu zpráv a správné fungování sítě.[8]



Obr. 10 Integrace WirelessHart do stávajícího řešení[8]

Jedni z výrobců, kteří nám dodávají přístroje fungující na rozhraní WirelessHart, jsou Siemens, Pepperl+Fuchs, Emerson a další. Společnost Pepperl+Fuchs se od počátků uvedení tohoto protokolu snaží spolupracovat a jako první přišla se zařízeními, jež tento protokol využívaly. Na stránkách výrobců lze zjistit, o jaké konkrétní zařízení se jedná a jaká je jejich technická specifikace.[8]

2.2.6 ISA 100.11a

Jedná se o multifunkční protokol pro bezdrátovou komunikaci vytvořený organizací ISA. Využívá se v průmyslu pro sítě tvořené senzory a akčními členy. Jeho navržení bylo ovlivněné potřebou bezdrátového přenosu údajů do zaběhlých kabelových sítí, nebo do nových řídících sítí, které neměli jednotný protokol. Využijeme-li standard ISA 100.11a, můžeme očekávat protokol, který svými vlastnostmi splňuje náročné podmínky, které se vyskytují v průmyslové automatizaci. Za zmínku stojí robustnost, odolnost vůči rušení celková bezpečnost informací v síti. Další specifické vlastnosti nalezneme v tabulce (Tab. 5).[10]

Tab. 5 Vlastnosti protokolu ISA 100.11a[9]

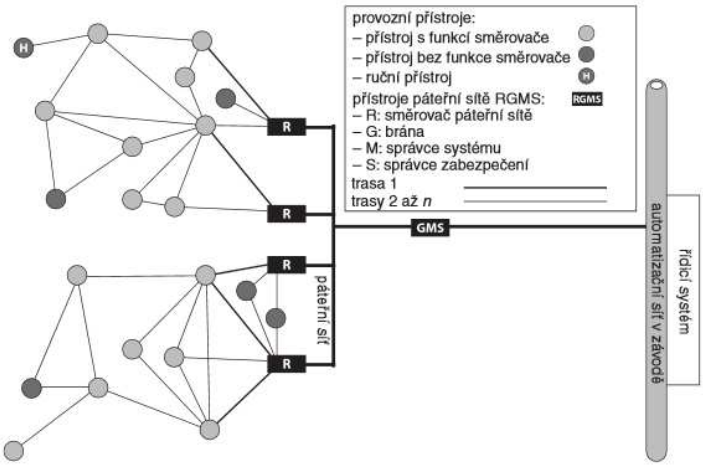
Rádiový standard	IEEE 802.15.4. - 2006
Pásmo	2,4 GHz
Přístup k médiu	CSMA, TDMA
Velikost časového slotu	10-14 ms
Latence	10ms
Topologie	Hvězda-mesh
Zabezpečení	AES
Podpora průmyslových protokolů	Profi bus, FF, Modbus, HART

Systém ISA 100.11a má několik výhod oproti jednostranně zaměřenému protokolu pro HART, kterým je WirelessHART. Z toho vyplývá, že se do budoucnosti s WirelessHART standardem nedá moc počítat.[10]

ISA 100.11a využívá základní komunikační kanál jako prostředek k rádiovému přenosu veškerých zpráv, jež byly dříve určené k přenosu pomocí kabelů. Funguje tak, že se daná zpráva vloží do obálky, jež se za pomocí protokolu ISA 100.11a a rádiového pojítka doručí k potřebnému zařízení, kterému nemusí být ani zřejmé, o jaký typ přenosu se jedná.[10]

V praxi se také hodí mechanismus, pomocí kterého dokáže tento standard převádět u libovolného protokolu aplikační vrstvu na aplikační vrstvu standardu ISA 100.11a, která je optimalizována pro bezdrátový přenos.[10]

Jednou z největších výhod oproti protokolu WirelessHART je existence páteřní sítě. Tímto způsobem se docílí snížení využití kanálu při přenosu zprávy, a tudíž se neodčerpává zbytečná energie navíc. Pomocí páteřní sítě (Obr. 11) můžeme rozšířit pásmo pro přenos zpráv při jejich postupu k bráně. U průmyslových sítí snímačů a akčních členů je totiž časté, že se konverguje stále větší počet tras, jak se přibližujeme směrem k bráně.[10]



Obr. 11 Vysokorychlostní páteřní síť[10]

2.2.7 Proprietární varianty

Proprietární řešení bezdrátového přenosu dat se vztahuje na konkrétní výrobce, kteří často vycházejí z již odzkoušených řešení a pouze implementují své požadavky tak, aby to vyhovovalo právě jim v jejich situaci. Příkladem může být například společnost Apple Inc se svým protokolem Airplay. Jde o proprietální protokol nad sítí Wi-Fi určený pro přenos hudby, videa a fotografií.

MiWi je proprietární protokol firmy Microchip Technology. Spadá pod WPAN a jde o nízko objemový přenos dat s nízkou spotřebou a rychlostí.

2.3 Propojovací systémy datové úrovně D2/LAN

Propojovací systémy této úrovně nám umožňují přenos dat v rámci subsystémů. Oproti datové úrovni SAN mají daleko větší přenosové rychlosti a tak dokážeme přeposílat i větší objem dat. U větších systémů se na této úrovni využívá topologie hvězdice, naproti tomu u malých systémů lze využít i sériové propojení. Využívá se protokol Ethernet TCP/IP a tím můžeme přenášet různé elektronické dokumenty. Hardware, který se na této úrovni využívá, můžeme rozdělit na pasivní a aktivní zařízení.

Pasivní – Kabely, konektory.

Aktivní – Switch, bridge, router, gateway, hub, transceiver.[2]

Organizace IEEE se zabývá standardizací LAN. V této práci se zabýváme bezdrátovým přenosem dat, a proto bude zmíněn v rámci LAN pouze standard 802.11, který se zabývá

certifikací WLAN a nazývá se také Wi-Fi. Evropská varianta pro bezdrátovou verzi LAN je pod taktovkou organizace ETSI. Máme zde dvě varianty HiperLAN1 a HiperLAN2.[11]

2.3.1 IEEE 802.11

Organizace IEEE se zabývá vývojem a uvedením bezdrátových protokolů. V tomto bloku práce se seznámíme s protokoly 802.11 a/b/g/n/ac. Historií spadá původní standard 802.11 do roku 1997 a v následujících letech až dodnes dochází k postupnému vylepšování jeho vlastností s ohledem na čím dál větší nároky např. v průmyslu. Vlastnosti jednotlivých protokolů 802.11 jsou zobrazeny v tabulce (Tab. 6).[11]

Tab. 6 Vlastnosti protokolů spadajících pod 802.11

Protokol	802.11a	802.11b	802.11g	802.11n	802.11ac
Datum schválení	1999	1999	2003	2009	2013/2014
Frekvence [GHz]	5	2,4	2,4	2,4 i 5	5
Radiofrekvenční technologie	OFDM	DSSS	DSSS a OFDM	MIMO a OFDM	MIMO a OFDM
Modulace	BPSK, QPSK	DBPSK a DQPSK	DBPSK a DQPSK	BPSK, QPSK	256-QAM
Přenosová rychlost [Mbit/s]	54	11	54	150	450

Protokol 802.11b: S rostoucí rychlostí kabelových sítí bylo potřeba zrychlit i standard 802.11, který již byl nedostačující. 802.11b je nástupce původního standardu 802.11 a nabral pouze na rychlosti. Rozdílný je však způsob kódování, který se změnil z původního Barker 11 na metodu CCK.[11]

Protokol 802.11g: Svou rychlostí se dostal na totožnou úroveň jako 802.11a, který ovšem pracuje v jiném frekvenčním pásmu. Platí zde zpětná kompatibilita s 802.11b. Změnou je i použití modulace OFDM k dosažení takovéto rychlosti.[11]

Protokol 802.11a: Oproti předchozím standardům pracuje v pásmu 5GHz, a tudíž není zpětně kompatibilní s ostatními. Výhodou je nulové rušení se zařízeními pracujícími právě s frekvencí 2,4GHz. Standard 802.11a dělí pásmo 5GHz dále ještě na více částí, tzv. pásma UNI.[11]

Protokol 802.11n: Tento protokol je zpětně kompatibilní se standardy 802.11b/g/a, jelikož může fungovat i na frekvenci 2,4GHz i 5GHz. Velmi vysoké rychlosti vděčí užitím nejedné

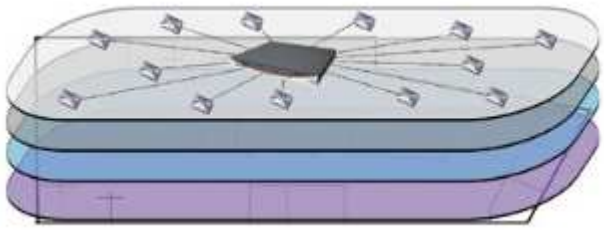
antény a také technologii zvané MIMO. Ta mu dovolí příjem i odeslání z více antén zaráz.[11]

Protokol 802.11ac: Dosahuje až trojnásobného výkonu standardu 802.11n. Oproti předchozím standardům si udržuje výkon po celé délce svého dosahu a je značně spolehlivější. Stejně jako 802.11n může používat variantu s jednou až třemi anténami, které zvyšují možný výkon. Ta se třemi anténami dosahuje až 1,35Gb/s.[12]

2.3.2 Průmyslová Wi-Fi

Nedostatky, které brzdily rozvoj Wi-Fi, byly eliminovány nástupcem Wi-Fi čtvrté generace neboli průmyslovou Wi-Fi. Průmyslová Wi-Fi se již svými vlastnostmi vyrovná klasickému kabelovému připojení a mnohdy ho i překoná. Oproti obyčejné Wi-Fi síti se zlepšila dostupnost, stabilita a také zabezpečení.[13]

Průmyslová Wi-Fi funguje na nové architektuře blanket. Její schéma máme zobrazeno na obrázku (Obr. 12). Tato topologie umožňuje síti zabránit přístupovým bodům, aby se mezi sebou rušily. A platí pravidlo, že síť pracuje lépe, jestliže je použito více přístupových bodů. Snadnost rozšíření sítě o další přístupový bod je dána funkcí plug-and-play. Jednotlivé vrstvy topologie blanket potřebují jeden kanál a my tak můžeme spravovat různé služby odděleně, aniž by se negativně ovlivňovaly.[13]



Obr. 12 Síť s topologií blanket[13]

Pokud se připojuje klient k síti s topologií blanket, tak přesto, že je síť tvořena i desítkami přístupových bodů, tak ji považuje za jeden přístupový bod, definovaný jednou MAC adresou. Provozujeme-li topologii blanket pomocí standardu IEEE 802.11n, lze dosáhnout rychlosti až 300Mb/s.[13]

Firma Siemens má na trhu produkty řady Scalance W. Ty se liší od obyčejných výrobků svou konstrukcí a dalšími inovacemi, které jsou nezbytně nutné pro fungování v průmyslu.

Jde hlavně o funkční bezpečnost, redundance spojení či možnost použití v prostředí s nebezpečí výbuchu. Samozřejmostí je odolnost vůči vnějším vlivům, jako jsou extrémní teploty, vlhkost, prašnost a vibrace.[13]

2.4 Mobilní datový přenos

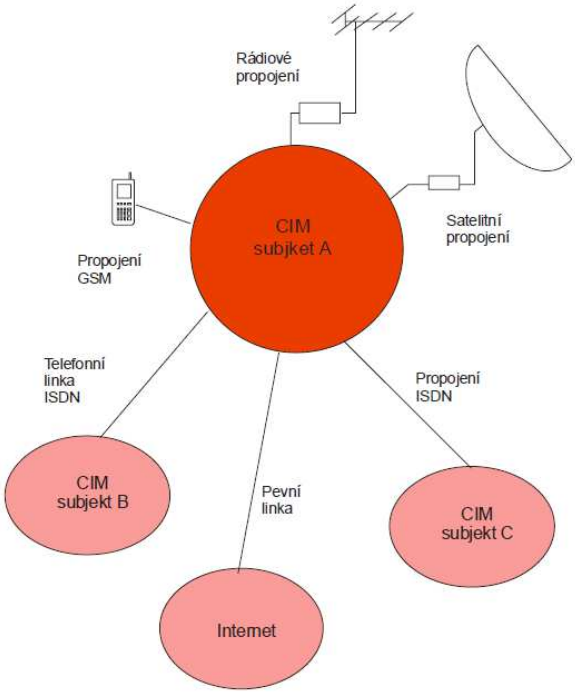
Chceme-li propojit síť s vnějším prostředím, využijeme k tomu přenos pro globální komunikaci. Možnosti, jak toho docílit, jsou zobrazeny na obrázku (Obr. 13). Je zde vidět, že můžeme využít telefonní linku, satelitní propojení nebo mobilní datový přenos GSM.

Mobilní datový přenos lze rozdělit podle generací, vývojem jakým prošly a také podle užití multiple access technologie. Mezi multiple access technologie patří FDMA, TDMA a CDMA.[18]

Rozdělení podle generací v rámci Evropy:

- 1G – Analogové sítě využívající FDMA.
- 2G – GSM využívající TDMA a CDMA.
- 2.5G – Rozšíření o GPRS/EDGE.
- 3G – Až 6 technologií v závislosti na oblasti – Evropa (UTSM), přístup pomocí CDMA.[18]

Využitím mobilního datového přenosu se přenášíme do již licencovaných pásem. V naší republice k současnému datu existují čtyři poskytovatelé služeb sítí mobilních telefonů. Konkurenční boje nutí jednotlivé poskytovatele těchto služeb snižovat ceny, i přesto je obrovskou nevýhodou oproti nelicencovaným pásmům vyšší cena provozu. Vezmou-li se v potaz hustota pokrytí a spolehlivost, dostáváme zajímavou možnost komunikace s vnějším prostředím.



Obr. 13 Schéma vnější globální komunikace[1]

2.5 Klady a zápory způsobů přenosu dat

V této kapitole se podíváme na kladné, ale i na záporné vlastnosti daných řešení, které jsme si v předcházejících kapitolách popsali. Většina vlastností byla již uvedena, zde jsou ovšem zdůrazněny důvody, díky kterým se konkrétní typy přenosů staly populární, nebo naopak, proč nejsou tak často používány.

Propojovací prostředky na signální úrovni

- Výhody: Přenosová rychlost, odezva, jednoduchost propojení, cena.
- Nevýhody: vznik odchylek, nastavení rozlišení, obtížnější transformace dat.

WirelessHart

- Výhody: Jednoduchost, cena, dosah, odolnost proti rušení.
- Nevýhody: Komunikace pouze se zařízeními HART.

Propojovací prostředky datové úrovně D1

BlueTooth

- Výhody: Rozšířenost, v závislosti na verzi rychlost, spotřeba.
- Nevýhody: Spojově orientovaná metoda komunikace.

IrDa

- Výhody: Žádné rušení, nízká cena, bezpečnost.

- Nevýhody: Slabý dosah, nutnost přímé viditelnosti.

ZigBee

- Výhody: Spotřeba, cena, dosah, spolehlivost, flexibilita, jednoduchost.
- Nevýhody: Nízká přenosová rychlost.

EnOcean

- Výhody: Spolehlivost, spotřeba, interoperabilita, frekvenční pásmo.
- Nevýhody: Nízká přenosová rychlost.

ISA 100.11a

- Výhody: Multifunkčnost, robustnost, spotřeba.
- Nevýhody: Dražší komponenty, komplikovanější struktura.

Proprietární řešení

- Výhody: Individuální využití v dané situaci.
- Nevýhody: Omezená kompatibilita.

Propojovací prostředky datové úrovně D2

Wi-Fi

- Výhody: Rychlost, mobilnost.
- Nevýhody: Bezpečnost, dostupnost, stabilita.

Průmyslová Wi-Fi

- Výhody: Stabilita, dostupnost, bezpečnost.

Mobilní datový přenos GSM

- Výhody: Vysoká kvalita, pokrytí mobilními operátory.
- Nevýhody: Cena tarifů mobilních operátorů.

Každá z daných úrovní propojení má několik variant, jak bezdrátový přenos provést. Liší se ve svých zaměřeních a cílových skupinách. Jednotlivé firmy si budují svou klientelu a uzpůsobují tomu vývoj. Nelze tudíž srovnávat například Bluetooth 3.0 a ZigBee, když oba dva standardy mají plnit jiné úlohy.

Ve výsledku máme velké množství variant, jak vyřešit bezdrátový přenos dat právě pro naše účely. Ať už se jedná o průmyslové zautomatizování ve výrobě, nebo jen hledáme řešení pro snadnější ovládání své domácnosti.

3 SEZNAM TEORIE SOUVISEJÍCÍ S PŘENOSEM DAT

První tři kapitoly seznamu teorie vycházejí z převážné většiny z knihy Bezdrátové sítě CISCO[11]. Jde o kapitoly rádiové vlny, vlivy na bezdrátový přenos dat a modulační techniky.

3.1 Radiové vlny

Oproti sítím LAN, kde se data pohybují jako elektrické signály, se u bezdrátových sítí využívá právě rádiové frekvence. To nám umožňuje propojit dvě zařízení bez pomoci drátů. S postupem času a vývoje se zaměřujeme na myšlenku „posílat co možná nejvíce informací co nejvyšší přenosovou rychlostí na co možná největší vzdálenost“.

Elektromagnetické spektrum je v rozsahu 3Hz až 300GHZ. Nás ovšem zajímají pouze frekvence, které nám umožní přenos dat. Za zmínku tedy stojí frekvence 900MHz, 2,4GHz a 5GHz.

Jak už bylo v předchozích kapitolách vysvětleno, s bezdrátovým přenosem souvisí různá úskalí. Jedny z nejčastějších jsou probírány v kapitole 3.2. Chceme-li data převést do RF signálu, je k tomu zapotřebí využít modulační techniku. O jednotlivých technikách je diskutováno v kapitole 3.3.[11]

3.2 Vlivy na bezdrátový přenos dat

3.2.1 Free Path Loss

Máme-li přístupový bod, který vysílá k několika zařízením, pak ne všechny tyto zařízení přijmou stejný signál. Sílu přijatého signálu ovlivňuje dosah zařízení k přístupovému bodu. Umístíme-li zařízení příliš daleko od přístupového bodu, nemůžeme čekat, že nám bude síť fungovat. Free Path Loss nám připomíná, že vlnu nic nezastavuje, ale jednoduše zmizí.

3.2.2 Absorpce

Absorpce je jev ovlivňující negativně bezdrátový přenos a to pomocí snížení amplitudy vlny. Pohlcením vlny vzniká teplo, podobně je to mu i mikrovln. Mezi pohlcovače patří např. lidé, zdi, koberce. Je to podobný případ jako u zvukových vln. Hůře slyšíme někoho, kdo na nás mluví přes zeď.

3.2.3 Odrazy

Podobně jako absorpce i odrazy mají negativní vliv při provozu bezdrátové sítě. Odrazem je myšleno, pokud signál narazí na překážku a odrazí se a následně putuje dál jiným směrem. Odrazy můžeme přirovnat k odrazu světla od předmětů. Frekvence je faktor, na kterém je odraz závislý. Různé frekvence jsou jinak odrazem ovlivněny. Některé předměty odrážejí jednu frekvenci a další odrazit nedokážou.

S odrazy souvisí také pojem rozptyl. Rozptyl nám zhoršuje kvalitu signálu. Jde o odraz signálu do více směrů. Příkladem může být snížení signálu, pokud prudce prší.[11]

3.3 Modulační techniky

V předchozích kapitolách bylo vysvětleno, že modulační techniky jsou nezbytně nutné k fungování bezdrátového přenosu. Modulací se přidávají data k přenosovému signálu a to nám umožňuje posílat zakódovaná data bezdrátově s využitím rádiového signálu. Modulovaná vlna je tvořena ze tří prvků: amplituda, fáze, frekvence. U bezdrátového přenosu se setkáváme většinou se třemi technikami, kterými jsou DSSS, OFDM a MIMO. Ve zkratce se s jednotlivými modulačními technikami seznámíme. Detailní popis by vydal za samostatnou práci.

3.3.1 DSSS

Standardy, které využívají tuto modulační techniku, jsou zobrazeny v tabulce (Tab 6). DSSS funguje na principu rozložení signálu napříč využívaným spektrem. V závislosti na kanálu, který využíváme pro přenos dat, se signál tedy rozloží napříč 22MHz v tomto daném kanálu.

DSSS využívá pro zakódování dat čipovou sekvenci. Je to nezbytně nutná vlastnost, protože může dojít ke ztrátám při přenosu dat z důsledku interference.

Pro nižší přenosové rychlosti jako je 1Mb/s nebo 2Mb/s se využívá při DSSS Barkerův kód. U vyšších rychlostí 5,5Mb/s a 11Mb/s je již potřeba použít kódování CCK.

3.3.2 OFDM

Oproti DSSS nefunguje na principu rozložení spektra. Využívá se stejně jako předchozí technologie u bezdrátových sítí. Tato modulace nám umožňuje vyšší přenosové rychlosti

s minimálním vlivem interference na poškození dat. Existuje několik kanálů s určitými frekvenčními rozsahy o šířce 20MHz. K dispozici jsou pomocné nosné vlny, ty ale dovolují pouze nízkou přenosovou rychlost. Využívá se tak odesílání všech vln najednou paralelně, čímž dosáhneme vyšší rychlosti. OFDM využívají standardy 802.11a/g.

3.3.3 MIMO

Tato technologie se využívá až u nejnovějšího standardu 802.11 a tím je 802.11n. Pro používání této technologie je nezbytné, aby zařízení, které ji bude používat, mělo 2-3 antény pro příjem signálu a také ne jednu anténu pro vysílání daného signálu. S touto technologií je možné dosahovat rychlosti až 450 Mb/s. Je to umožněno díky simultánnímu multiplexingu dat na jednom kanálu. Využívá-li přístupový bod technologii MIMO neznamená to, že by nemohl komunikovat se zařízeními, které MIMO nepodporují. Právě naopak, u těchto zařízení se standardem 802.11a/b/g dokáže zvýšit výkon až o 30%.[11]

3.4 Možnosti zabezpečení bezdrátového přenosu dat

Veškerá řídící data a také celý provoz v síti je přenášen vzduchem. To nevede k ničemu jinému, než k snadnějšímu útoku ze „třetí strany“. Existuje velké množství lidí, kteří rádi testují své znalosti z pronikání do osobních a hlavně střežených údajů ostatních. Záleží už pak na nás, jak se zachováme a jak svá data budeme chtít chránit. Je mnoho způsobů jak bezdrátový přenos zabezpečit. Výčtem se jedná o filtrování MAC adres, skrytí SSID, firewall a jiné omezení přístupu. My, se však budeme zajímat v této práci pouze o autentizaci a šifrování, které se k těm předešlým variantám využívají v různých kombinacích a zabraňují případným nevyžádaným útokům. Chceme-li dosáhnout opravdu vysokého standardu zabezpečení naší sítě, nelze spoléhat pouze na jednu variantu, je potřeba využít kombinaci těchto prvků na veškerých stanicích v síti.[11][15]

Důvody, kvůli kterým se vůbec zaobíráme bezpečností bezdrátových sítí, je několik. Jde hlavně o:

- Ad hoc sítě – Riziko v možnosti obejít bezpečnostní zásady.
- Neoprávněné přístupové body – Nejsou součástí podnikové infrastruktury.
- Chybně přidružení klienti – Řešením je skrytí SSID nebo využití funkce MFP.

- Bezdrátové útoky – Falšování rámce pro správu, průzkumné útoky, přístupové útoky, útoky typu odepření služby a jiné.[11]

3.4.1 Autentizace

Kontrola přístupu je dobrý mechanismus, pomocí kterého se můžeme přihlásit do sítě a zvýšit tak šanci, že se případný pachatel nedostane k našim citlivým datům. V prvé řadě musí klient (žadatel) poslat požadavek k autentizaci do přístupového bodu. Ten následně na takový požadavek reaguje odpovědí a vyšle data nazpátek. Jestliže je přístup klientovi odepřen, jeho žádosti k autentizaci není vyhověno. Tento způsob kontroly vstupu do sítě ovšem není příliš bezpečný, nevyužívá šifrování. Platí ovšem, že šifrovací metody používají ke svému chodu autentizaci.[11][14]

Vylepšenou kontrolou vstupu je mechanismus Shared Key Authentification. Je to bezpečnější varianta, kde je přístup do sítě odepřen těm stanicím, které se nedokážou prokázat správným klíčem. Klíčem může být WEP nebo WPA TKIP. Důležitým faktorem zůstává, že přístupového heslo si jednotlivé stanice uchovávají pouze pro sebe.

Jednoduchá autentizace:

- Otevřená autentizace
- Autentizace za pomoci předem sdíleného klíče
- Filtrace MAC adres

Centralizovaná autentizace:

- 802.1X
- EAP
- Autentizační server
- EAP-TLS
- EAP-FAST
- PEAP
- LEAP[11]

3.4.2 Šifrování WEP

Nejstarší a dříve nejpoužívanější šifrovací algoritmus. Můžeme jej aktivovat, pokud chceme více chránit ve své síti bezdrátový přenos dat. Tento algoritmus spadá pod standard IEEE 802.11 a k dnešnímu datu je již lehce prolomitelný. Zmiňujeme se o něm pouze z historických důvodů, a protože další algoritmy z něj vychází. To, že je prolomitelný, nemění nic na faktu, že se stále používá. I přesto, že mají lidé k dispozici novější algoritmy, stále se uchylují k této variantě a dávají tak větší možnost útočníkům, aby je okradli o jejich data. Cílem takového šifrovacího algoritmu mělo být zabezpečení na úrovni, že si uživatel připadá jako by se nejednalo o bezdrátový přenos, ale jako o klasickou kabelovou síť.[14]

Síla šifrovacího algoritmu je mění podle délky šifrovacího kódu. Ke každému datovému paketu máme přiřazen inicializační vektor, který je i přes různé délky WEP klíče stejný (Tab. 7).[11]

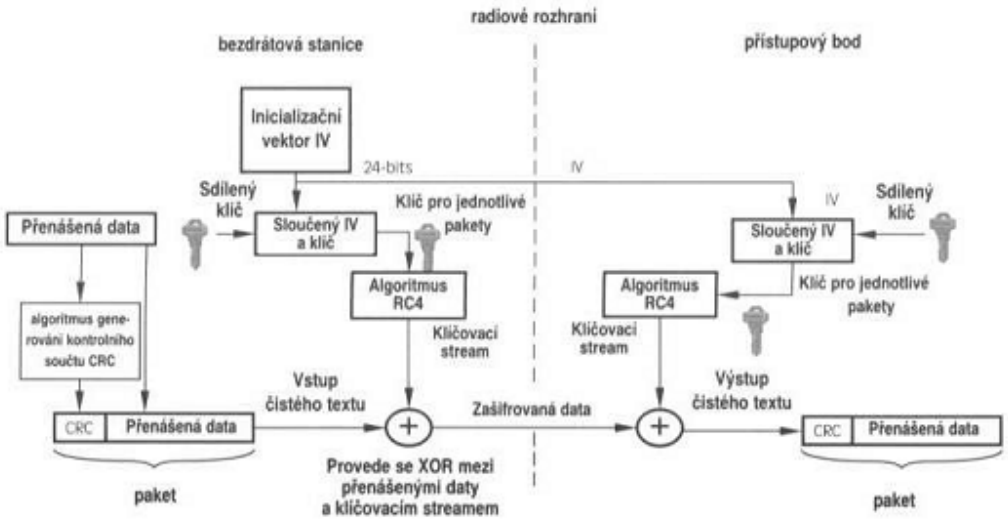
Tab. 7 Vlastnosti WEP klíče[11]

Síla šifrování	Délka WEP klíče	Inicializační vektor
64 bitů	40 bitů	24 bitů
128 bitů	104 bitů	24 bitů
152 bitů	128 bitů	24 bitů
256 bitů	232 bitů	24 bitů

Šifrování dat je nejúčinnější varianta, jak zabránit odposlechu při přenosu dat. U varianty s algoritmem WEP jsou data kódována pomocí šifrování RC4 s kombinací operací s matricemi. Data jsou převáděna na matrice díky vektorovému součinu šifrovacího klíče WEP a náhodně vygenerovaného 24bitového inicializačního vektoru. Klientovi je tak zaslán pouze inicializační vektor spolu s přenášenými daty, nikoliv šifrovací klíč WEP. Klient tak může zpětně odšifrovat dat, jelikož již zná šifrovací klíč a také inicializační vektor. Přehled jednotlivých kroků šifrovacího algoritmu WEP je podrobně popsán na obrázku (Obr. 14).[11]

Praktičnost vyplývá z faktu, že pro jednu síť máme pouze jeden klíč WEP. Vzniká tak ale bezpečnostní riziko, kterého jsou schopni zkušení útočníci využít. Stačí jim získat šifrovací klíč a jsou okamžitě schopni odposlouchávat komunikaci v síti a mají možnost se přihlásit k AP. Využíváme-li algoritmus WEP, měli bychom ručně dělat něco, co sám bohužel

nesvede, a to měnit šifrovací klíč, abychom ztížili práci hackerům. Dynamicky měněn klíč má až algoritmus WPA, o kterém bude nadcházející kapitola.[14]



Obr. 14 Schematický průběh šifrování WEP[14]

3.4.3 Šifrování WPA

Jde o vylepšení stávajícího standardu WEP. Je k nalezení ve všech zařízení podporující Wi-Fi. Umožňuje nám tak mnohem lepší zabezpečení WLAN proti útokům z venku. Využívá ovšem stejný šifrovací algoritmus jako WEP – šifru RC4. WPA přichází s funkcemi, které drželi WEP zpátky. Jedná se hlavně o slabé šifrování pomocí statického klíče a nulovou autentizaci.[11][14]

WPA je variabilní a může se jeho využití měnit s ohledem na umístění. V domácích sítích se využívá jednoduchý režim s přednastaveným klíčem PSK, jenž se dále sdílí pouze s AP a již nedochází žádnému dalšímu ověřování identity stanice. Oproti tomu v podnikových sítích lze využít centrálního autentizačního serveru, pomocí kterého dochází k distribuci klíčů v rámci sítě.[17]

Bezpečnost se oproti WEP zvýšila a velkou zásluhu na tom má rozšířené vybavení WPA:

- Rozšířený inicializační vektor – Ochrana proti slabým klíčům.
- Technika Re-Keying – Dynamická změna klíče WEP.
- Kontrola integrity – Nedochází ke změně dat na cestě.
- Per Packet Mixing – Změna pozice inicializačního vektoru v paketu.

- Protokol TKIP.
- AES.[11]

TKIP je protokol, který ručí za bezpečnost šifrovacího klíče a který je sám i vytváří. Je to velká výhoda oproti zmiňovanému WEP algoritmu, kde byly pouze statické klíče. Uživatel zadává pouze dočasný klíč ke spojení s AP, ten pak generuje klíč nový a poskytne ho síti. Díky tomu ví o klíči jen AP a je tak nezjistitelný.[14]

AES je bloková šifra, nahrazující nedostačující šifru DES, u které může být délka šifrovacího klíče i délka bloku větší nežli 128 popřípadě 256bitů. Nemá-li příjemce daný šifrovací klíč, není dešifrování možné.[11]

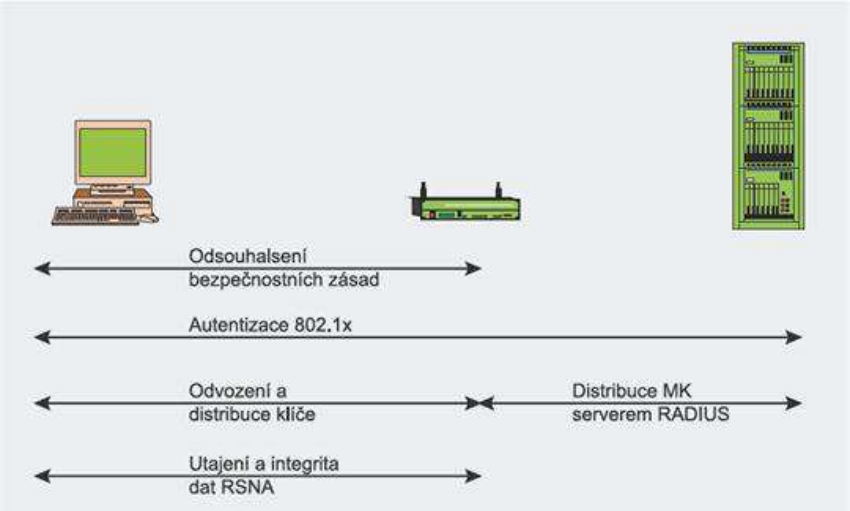
3.4.4 Šifrování WPA2

Jedná se o další verzi standardu WPA. Oproti předchozí verzi, může vyžadovat lepší hardware, protože využívá náročnější šifrování AES. WPA2 je kompatibilní se standardem 802.11i. Nejenže využívá šifrování AES, ale může také využívat kombinaci AES/CCMP, u které se inicializační vektor neustále prodlužuje po každém bloku této šifry.[14]

Srovnáme-li standardy WPA a WPA2 dojdeme k následujícímu vyhodnocení:

- WPA má možnost šifrování AES a jeho nedílnou součástí je protokol TKIP.
- WPA2 nedovoluje užít protokol TKIP, avšak jeho součástí je šifrování AES.
- WP2 má zrychlenější připojení, protože může ukládat klíče do mezipaměti.[11]

Největší zranitelností tohoto standardu je útok na PSK. Což pro PSK znamená pouze sílu daného hesla, které si volí uživatel sám. Zabezpečíme-li bezdrátovou síť pomocí standardu WPA2, musíme provést 4 fáze. Výčet těchto fází a grafické znázornění nám představuje obrázek (Obr. 13). Na obrázku máme možnost vidět počítač, který komunikuje s AP a komunikace dál pokračuje až k RADIUS serveru.[11]

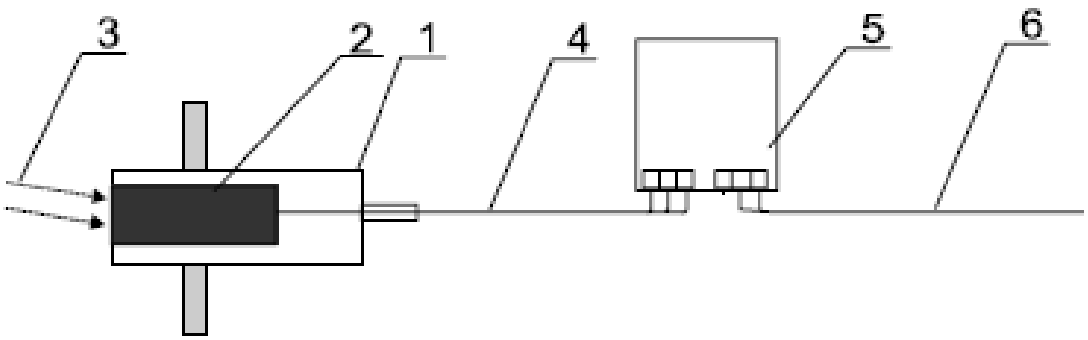


Obr. 15 Fáze zabezpečení sítě pomocí WPA2[14]

3.5 Senzory

Se senzory se setkáváme u propojovacích systémů signální úrovně. Jak již bylo uvedeno, na této úrovni se sbírají naměřená data, které pak potřebujeme přenést na další propojovací úroveň. Senzory tak patří k jedněm z hlavních prvků pro měření a snímání dat u informačních systémů. S vývojem technologií samozřejmě dochází i k postupnému zlepšování snímačů, jejichž součástí právě senzory jsou. S tím souvisí také rozvoj křemíkové technologie. Dle požadavků na snímání máme velké množství senzorů, které používají nejrůznější fyzikální principy, aby dokázaly snímat kvalitně vstupní data.[19]

Způsob, jakým se dostávají měřené hodnoty pomocí senzoru dál až k uživateli, máme na obrázku (Obr. 16). Jedná se o jednoduchý měřící okruh, kde lze vidět, jakým způsobem jím procházejí data. Hlavní součástí snímače (1) je senzor (2), pomocí něhož snímáme data nebo převádíme vnější podněty (3) na signál (4), o jehož vlastnostech bylo diskutováno v první kapitole – propojovací prostředky signální úrovně. Dále je tento signál vyhodnocován pomocí převodníku (5) a následně převeden na signál měřené veličiny (6). V systémech informatiky má senzor podobnou úlohu. Příkladem mohou být snímače čárových kódů.[19]



Obr. 16 Schéma měřícího okruhu[19]

Je několik skupin senzorů:

- Podle změn elektrické rezistence mění senzor elektrické vlastnosti hmoty.
- Senzor generuje elektrický potenciál.
- Senzor ovlivňuje polovodičový efekt hmoty polovodičů.
- Senzor způsobuje mechanické změny.
- Senzor reaguje na ionizující záření.
- Senzor vytváří změny směru a energie elektromagnetického záření.
- Senzor vytváří chemické změny a reakce.
- Senzor působí pomocí hydraulických účinků na proudění tekutin.[19]

V aplikacích, kde je potřeba více snímacích zařízení, nebo když se snímací zařízení nacházejí jinde než měřící systém, lze využít síťových senzorů. Síťové senzory se skládají ze dvou zařízení, jedno má měřící funkci a to druhé zajišťuje komunikaci. V některých případech se dají tyto dvě zařízení integrovat do jedné jednotky.[20]

V rámci senzorů se často setkáme také s pojmem převodník. Jedná se o zařízení, které získá informace ve formě nějaké fyzikální veličiny a konvertuje ji na elektrický výstupní signál. Převodníky se skládají ze dvou základních částí, primární měřící element, kterým je právě senzor, a vysílací jednotka zodpovědná za vyprodukování elektrického výstupu.[21][22]

I. PRAKTICKÁ ČÁST

4 POROVNÁNÍ PRAKTICKÉ APLIKACE PŘENOSŮ WLAN A WPAN

V této kapitole se budeme zabývat praktickými aplikacemi přenosů WLAN a WPAN. Nejprve si shrneme základní vlastnosti těchto dvou propojovacích úrovní. Poté využijeme znalosti z teoretické části této práce, konkrétně části Možnosti zabezpečení bezdrátového přenosu, a demonstrujeme je při zabezpečení Wi-Fi sítě v domácnosti. V dalších částech za pomocí freeware softwarů provedeme ukázku monitoringu sítě WPAN i WLAN. V závěru si ještě porovnáme WLAN i WPAN v několika parametrech jako jsou dosah, spotřeba a jiné.

K praktickým ukázkám této kapitoly se využije následující hardware:

Notebook Fujitsu Siemens AMILO Pi 3625

Wireless AP Client Router TP-Link TL-WR543G

4.1 WPAN

Bezdrátová privátní síť s malým dosahem nalezla své zastoupení v řadě technologií a využívá se dnes velmi často. Umožňuje propojení několika zařízení bez absence kabelů. Toho se využívá v nejrůznějších odvětvích např. zdravotnictví, průmysl, automatizace.

Běžného uživatele možná ani nenapadne, že se již se sítí WPAN setkal. V síti WPAN můžeme propojit několik zařízení, které pak mohou komunikovat, přeposílat či sdílet data nebo synchronizovat kontakty. Výjimkou není ani vzdálené ovládání počítače pomocí mobilu se zapnutým Bluetooth. Komunikace tzv. ad-hoc ač má své nedostatky, se jeví jako ideální možnost propojení v síti WPAN.

Organizace IEEE vyvíjí standard 802.15 a její dosavadní výsledky jsou prezentovány v tabulce (Tab. 8).

Tab. 8 Standard 802.15[23]

802.15.1	Norma pro WPAN - Bluetooth
802.15.2	Koexistence sítí WPAN s ostatními
802.15.3	High Rate WPAN
802.15.4	Low Rate WPAN
802.15.5	Topologie mesh ve WPAN
802.15.6	Wireless Body Area Network
802.15.7	Optická komunikace pomocí viditelného světla

4.1.1 Monitoring sítě WPAN pomocí softwaru

Pro monitoring WPAN sítě jsem používal freeware software Bluetooth Network Scanner (Obr. 17). Tímto programem získáme přehled nad všemi zařízeními, která se objeví v blízkosti našeho přijímače. Zobrazí se nám jejich název, MAC adresa, typ a také informace spojené s tím, zdali jsme už s ním komunikovali nebo ne.

Obr. 17 Program Bluetooth Network Scanner

4.2 WLAN

WirelessLAN nám umožňuje vyšší mobilnost a komfort. Nemusíme se příliš ohlížet, kam se svým notebookem přejdeme, jsou však určité meze. Ty jsou posunuté dále, než tomu bylo u WPAN. Velkým faktorem, který nám tuhle problematiku ovlivňuje teorie útlumu přes překážky nebo absorpce, které je probrána v kapitole Rádiové vlny. Propojovací úroveň D2, kam WLAN spadá, je aplikována jak v domácnostech, tak v podnicích. Tyto dvě využití vyžadují jiný přístup, a pokud vytváříme síť, měli bychom uvážit kde a za jakým účelem se bude síť využívat.

Jedním z rozdílů je bezpochyby forma zabezpečení. Domácnost, kde je síť tvořena jedním či dvěma počítači, nebude muset být zabezpečena tak jako podniková síť, kde by případný

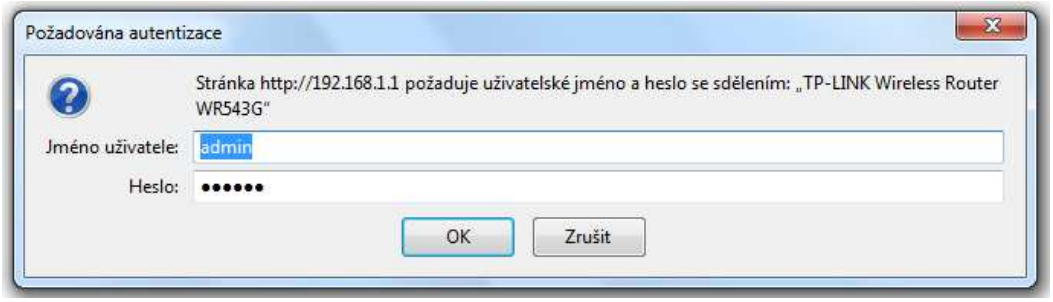
únik informací mohl mít katastrofální dopad. V kapitole Možnosti zabezpečení bezdrátového přenosu jsme se seznámili s nejčastějšími riziky, které počítačové síti hrozí. Dále zde byly zmíněny možné bezpečnostní mechanismy, které lze proti případnému útoku využít. My si v následující kapitole na konkrétním případu předvedeme, jak v rámci domácí sítě aplikovat tyto mechanismy a jak lze jejich kombinací zabezpečit síť.

4.2.1 Aplikace zabezpečení u WLAN

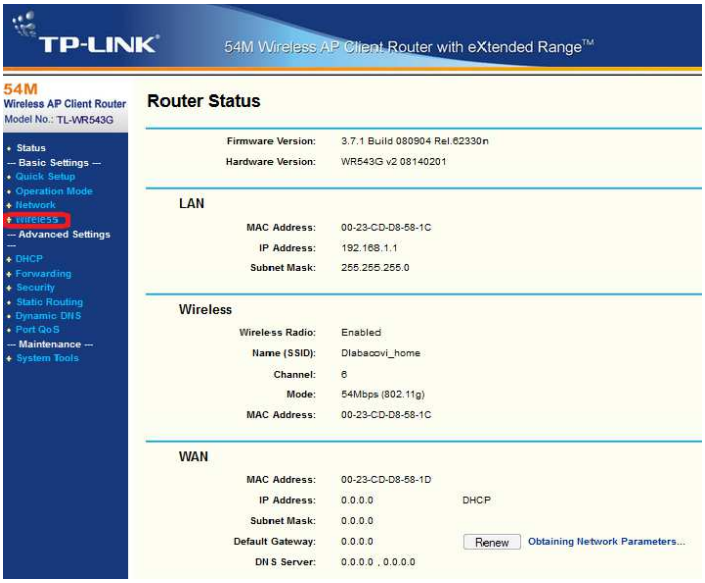
Pro aplikaci zabezpečení Wi-Fi u domácí sítě využijeme notebook a bezdrátový router, jejichž specifikace je uvedena na začátku hlavní kapitoly.

Pro komunikaci s přístupovým bodem musíme otevřít webový prohlížeč a zadat jeho IP adresu, která je defaultně od výrobce nastavena na hodnotu 192.168.1.1. Tím přejdeme k autentizaci, která je zobrazena na obrázku (Obr. 17).

Defaultní přihlašovací údaje jsou Jméno uživatele: admin, Heslo: admin. Proto se doporučuje v rámci bezpečnosti tyto údaje později změnit.



Obr. 18 Autentizace k přístupovému bodu



Obr. 19 Úvodní strana po přihlášení do AP

Po úspěšné autentizaci se dostaneme na úvodní stranu (Obr. 18), kde se nám zobrazí informace o aktuálním nastavení routeru. Nás bude zajímat vlevo kolonka Wireless. Po výběru této volby se nám zobrazí možnosti Wireless Settings (Obr. 19). Nebudeme rozebírat každou část tohoto nastavení, ale poukážeme pouze na parametry, které mají vliv na bezpečnost.

SSID – Název sítě (Pro účely této práce nastavena na Testovací_síť) by neměl vypovídat nic o domácnosti popř. názvu podniku.

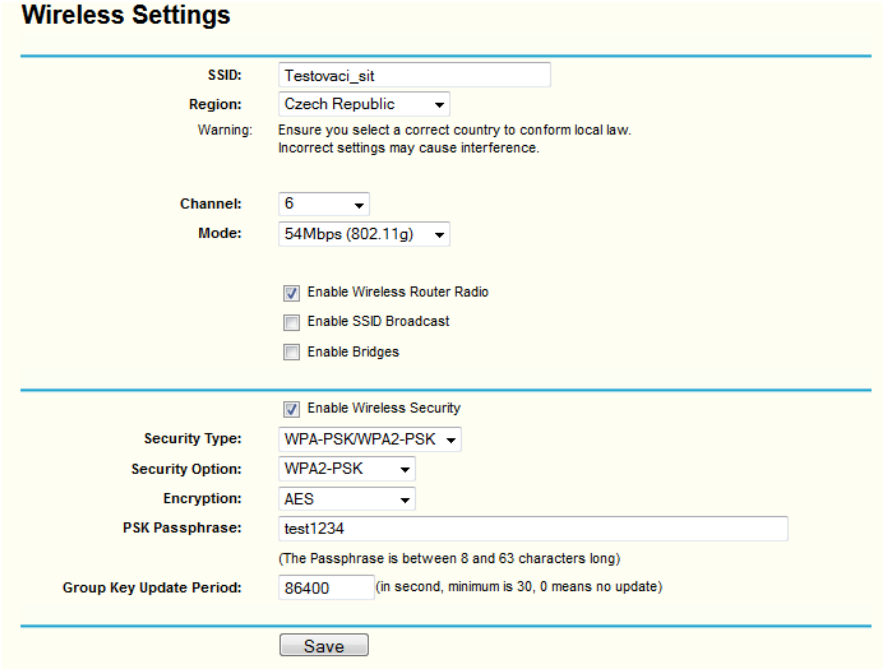
Enable Wireless Router Radio – Znemožní jakékoliv připojení zařízení pomocí bezdrátového připojení Wi-Fi.

Enable SSID Broadcast – Defaultně je SSID broadcast enabled a kdokoliv v dosahu sítě tak může vidět toto vysílání a zjistit název naší sítě. Pro lepší ochranu se doporučuje tuto možnost vypnout. Problémy budou mít zařízení, které se nedokážou připojit k síti i přes skryté SSID. Většina notebooků tuto vlastnost má v síťovém nastavení. U mobilních telefonů jsem tuto možnost nenašel a ty se nemůžou k takové síti připojit.

Enable Wireless Security – Pro co nejlepší zabezpečení samozřejmě musíme tuto položku nechat na Enable. U tohoto modelu AP si můžeme vybrat mezi šifrováním WEP, WPA i WPA2.

Jelikož se jedná o domácí síť, jeví se jako nejvhodnější varianta šifrovacího algoritmu WPA2 s předsdíleným klíčem PSK. Zvolíme-li tuhle možnost, je ještě třeba zvolit šifrování. Lze volit mezi TKIP a AES.

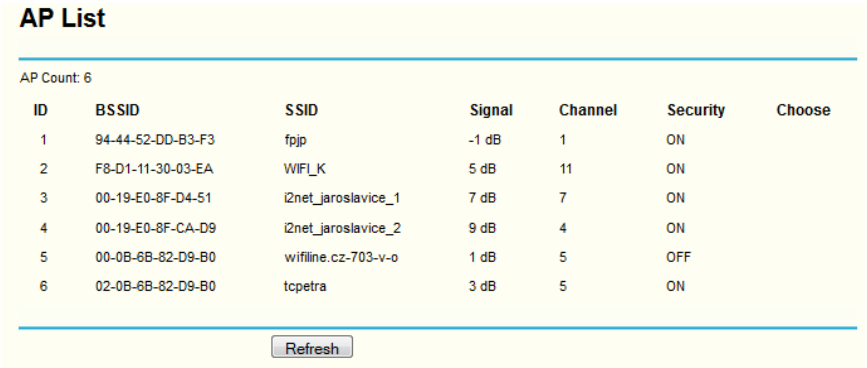
PSK Passphrase – Pro přístup do sítě je třeba zvolit PSK Passphrase, která bude sloužit k autentizaci zařízení.



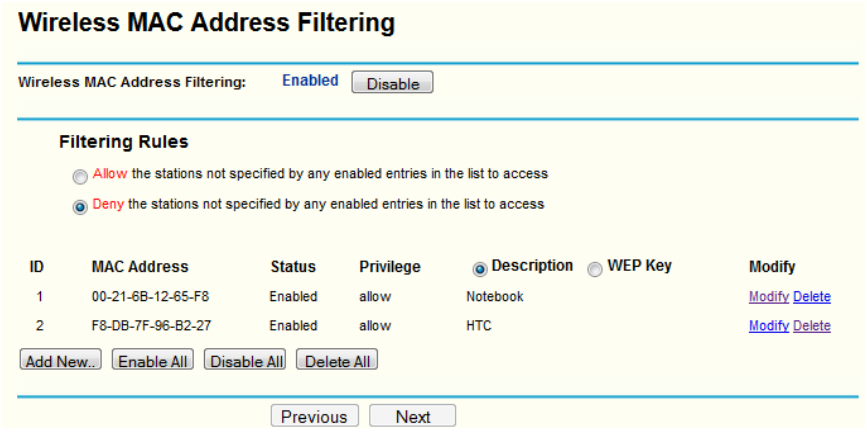
Obr. 20 Nastavení Wireless – základní nastavení a zabezpečení

Pokud přejdeme na další volbu - Site Survey, zobrazí se výpis všech dostupných sítí, ke kterým bychom se mohli připojit. Ukázka takového výpisu je na obrázku (Obr. 20).

Další volba u Wireless je MAC Filtering. Většinou se volí varianta, kdy odepřeme přístup zařízením, které jsme si nepřidali MAC adresu mezi filtry. Ukázka filtrování je na obrázku (Obr. 21). Odtud je vidět, že přístup do této sítě mají pouze dvě zařízení.

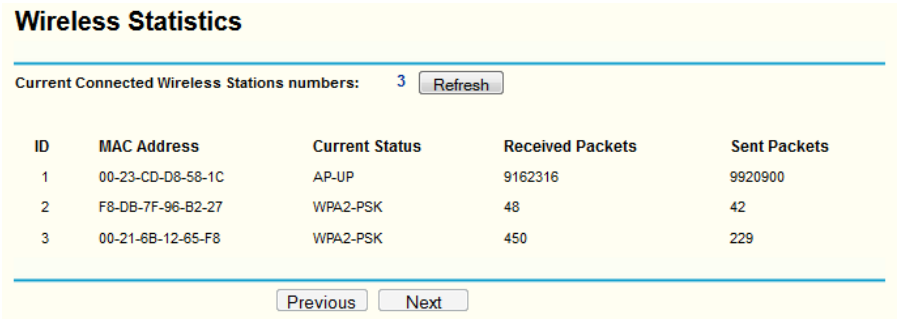


Obr. 21 Seznam všech dostupných sítí



Obr. 22 Filtrování MAC adres

Poslední volbou u Wireless je možnost Wireless Statistics (Obr. 22). Jejím účelem je pouze sledování zařízení, která jsou připojené k naší síti.



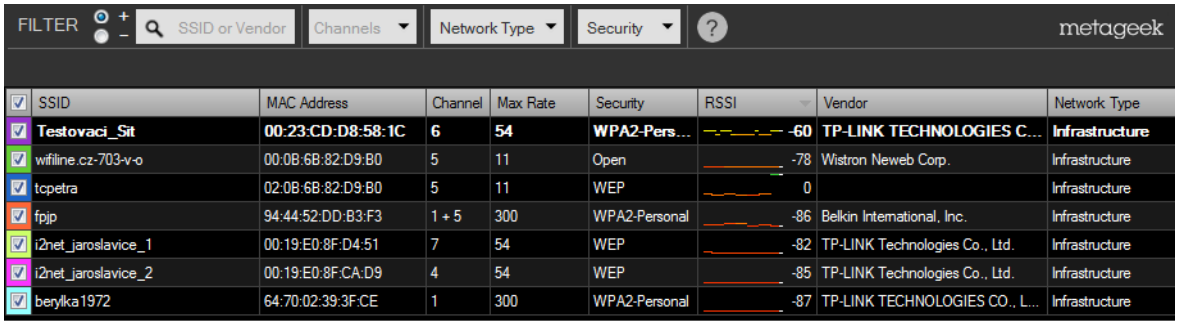
Obr. 23 Statistika připojených zařízení do naší sítě

4.2.2 Monitorování Wi-Fi sítě pomocí softwaru

Existuje velké množství freeware softwaru, který nám umožňuje skenovat či monitorovat počítačové sítě. Ukážeme si proto, jak lze jednoduše pomocí vybraného softwaru monitorovat Wi-Fi síť a zjistit tak o ní veškeré informace. Vyzkoušel jsem několik freeware softwarů a nakonec vybral dva, které se jevily uživatelsky nejrozumnější, a které jednoduše splnily očekávání. Jedná se tedy o programy inSSIDer a Wireless Network View.

inSSIDer – Je software, který nám detailně shrne vlastnosti přilehlých sítí Wi-Fi. Využívá k tomu nejrůznější grafy a vizualizace. Jejich ukázka se také objeví v průběhu kapitoly.

Po spuštění programu se ihned načtou přilehlé přístupové body. Hlavní stránka (Obr. 23) umožňuje vyfiltrovat sítě podle různých vlastností. Filtrovat lze podle názvu sítě, kanálu, frekvence, typu sítě nebo úrovně zabezpečení.

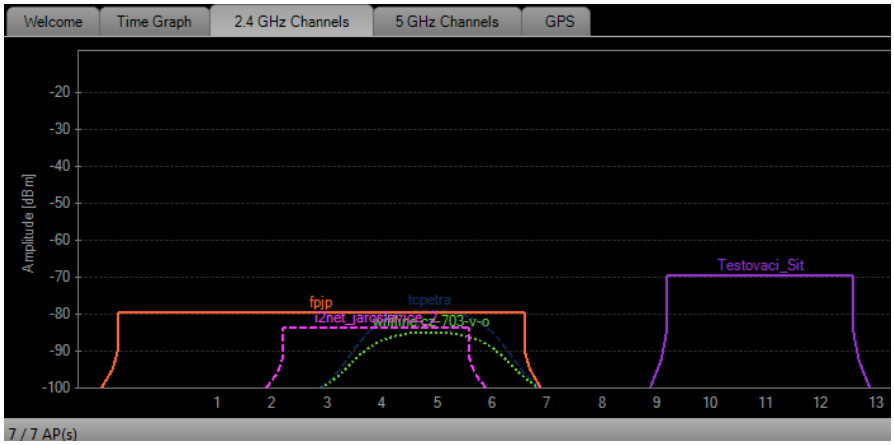


SSID	MAC Address	Channel	Max Rate	Security	RSSI	Vendor	Network Type
Testovaci_Sit	**00:23:CD:D8:58:1C**	**6**	**54**	**WPA2-Pers...**	**-60**	**TP-LINK TECHNOLOGIES C...**	**Infrastructure**
wifiline.cz-703-v-o	00:0B:6B:82:D9:B0	5	11	Open	-78	Wistron Neweb Corp.	Infrastructure
tcpetra	02:0B:6B:82:D9:B0	5	11	WEP	0		Infrastructure
fpjp	94:44:52:DD:B3:F3	1 + 5	300	WPA2-Personal	-86	Belkin International, Inc.	Infrastructure
i2net_jaroslavice_1	00:19:E0:8F:D4:51	7	54	WEP	-82	TP-LINK Technologies Co., Ltd.	Infrastructure
i2net_jaroslavice_2	00:19:E0:8F:CA:D9	4	54	WEP	-85	TP-LINK Technologies Co., Ltd.	Infrastructure
berylka1972	64:70:02:39:3F:CE	1	300	WPA2-Personal	-87	TP-LINK TECHNOLOGIES CO., L...	Infrastructure

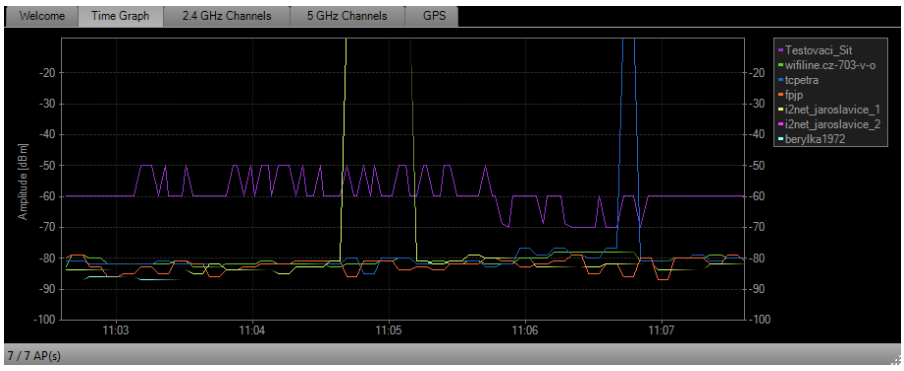
Obr. 24 Výpis přístupových bodů a možnosti filtrace

V dolní části programu máme možnost sledovat grafy vytvořené z hodnot kanálů jednotlivých přístupových bodů (Obr. 24). U testovací sítě jsem nastavil kanál 11 a vidíme, že je to v této oblasti naprosto nevyužívaný kanál. Kanál 5 je oproti tomu hojně využívaný a mohl by u těchto sítí vyústit ve vzájemné rušení.

Zobrazit lze také časový průběh RSSI (Obr. 25), taktéž můžeme nastavit, jestli pro 2,4GHz nebo pro 5GHz.



Obr. 25 Zobrazení využívaných kanálů v dané oblasti

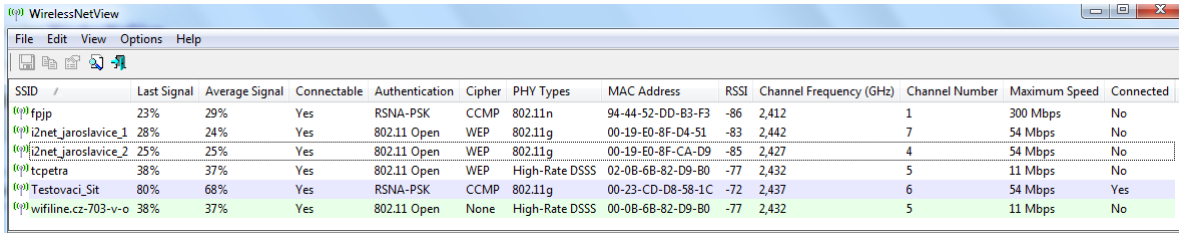


Obr. 26 Časový průběh v pásmu 2,4GHz

Wireless Network View – Jedná se o jednoduchou aplikaci, která nadchne informacemi, které dokáže o okolních přístupových bodech zjistit. Nijak složité uživatelské prostředí ihned po spuštění programu vygeneruje veškeré informace o přilehlých přístupových bodech. Hlavní stránka už s načtenými údaji je uvedena na obrázku (Obr. 26). Na nás je jen nastavení filtrace vlastností, které považujeme za důležité.

Program Wireless Network View zobrazí mimo klasické údaje o sítích jako jsou SSID, MAC adresa, kanál, rychlost, RSSI a zabezpečení, také detailní informace o síle signálu, použitém ověřovacím protokolu, přesné frekvenci kanálu, nebo způsob jakým se přenáší rádiový signál v síti.

Tento program slouží prakticky jen k tomuto účelu, zato odvádí výbornou práci. Na závěr můžeme zjištěné hodnoty exportovat do HTML a uveřejnit třeba na web.



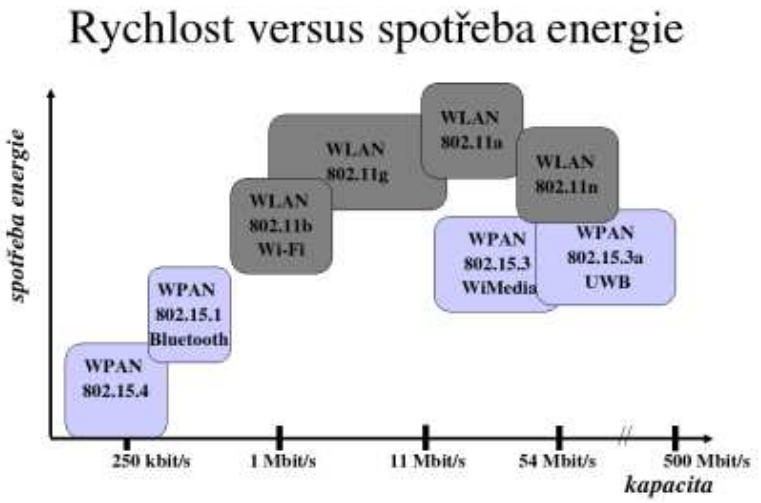
Obr. 27 Wireless Network View – Vyhledávání AP

4.3 Rozdíl WLAN a WPAN

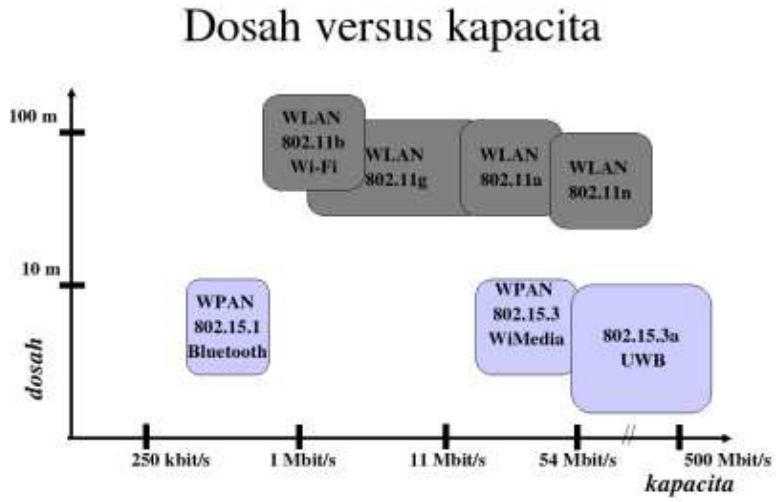
Není lehké srovnat WLAN a WPAN, jelikož se nejedná o stejné úrovně propojování zařízení. Přesto se můžeme podívat, jak proti sobě tyto sítě stojí v některých vlastnostech. Porovnáme si jejich spotřebu, dosah či přenosovou rychlost.

Podíváme-li se blíže na obrázek (Obr. 27) je jasné, že ač se má za to, že WPAN je považována za pomalejší, není tomu vždy tak. Organizace IEEE totiž s příchodem standardů 802.15.3 a 802.15.3a umožnila u sítě WPAN rychlosti přes 50Mb/s a dokázala se tak vyrovnat sítím WLAN.

Zajímavé je srovnání, co se týká spotřeby. Zde dominují sítě WPAN, což je dané nízkým dosahem, kterým tyto sítě disponují. Sítě WLAN pokrývají větší úsek a potřebují k tomu více energie, než je tomu u WPAN. Srovnání dosahu úrovně signálu u WPAN i WLAN je na obrázku (Obr. 28).



Obr. 28 Srovnání rychlosti a spotřeby u WPAN/WLAN[24]



Obr. 29 Srovnání dosahu a kapacity u WPAN/WLAN[24]

Velká část standardů ať u WPAN nebo WLAN pracuje na frekvenci 2,4GHz. Pokud bychom brali v zřetel jen sítě WLAN, pak je možné na přístupových bodech vybírat kanály tak, aby se vzájemně tyto sítě nerušily. I přesto, že se v blízkosti sítě WLAN nachází síť WPAN, tak k téměř žádnému rušení nedochází, protože např. Bluetooth využívá modulační techniku FHSS.

5 MOŽNOSTI MĚŘENÍ KVALITY PŘENOSU DAT

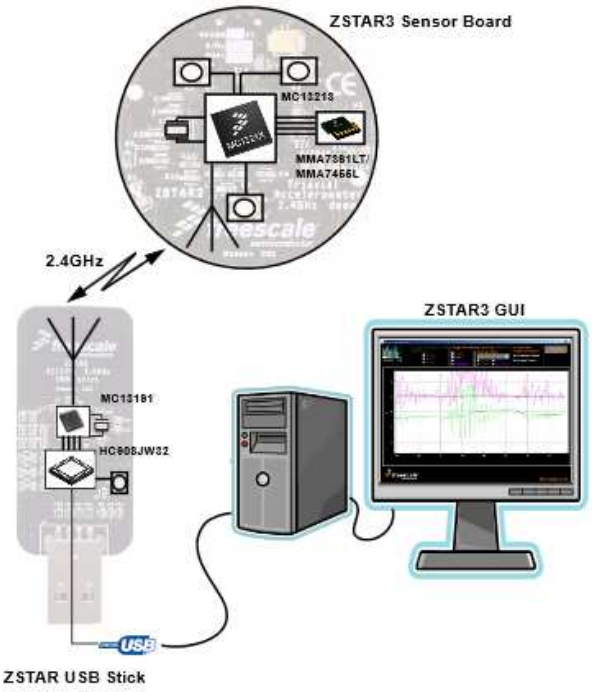
Provedli jsme měření kvality přenosu dat pomocí vývojových modulů ZSTAR3 a ZSTAR2. Jedná se o seznámení s těmito moduly a také jejich grafickým uživatelským prostředí.

5.1 Měřící zařízení

5.1.1 ZSTAR3

Tento vývojový modul od firmy Freescale pracuje na frekvenci 2,4GHz za využití bezdrátové technologie ZigBee. Systém měří akceleraci ve třech osách a snímá data pomocí analogového nebo digitálního senzoru. ZSTAR3 využívá bezdrátový čip MC1321x a může volit mezi dvěma typy senzorů. MMA7361LT pro analogový nebo MMA7455L pro digitální akcelerometr. Senzor je spolu s přijímačem vidět na obrázku (Obr. 30). Jde o jednoduché schéma komunikace v tomto systému.[25]

Více informací o celém systému nebo jednotlivých komponentech je k nalezení v manuálu ZSTAR3, který je k dispozici na stránkách společnosti Freescale.



Obr. 30 Schéma měřícího zařízení ZSTAR3[25]

5.1.2 ZSTAR2

Jde o starší verze oproti ZSTAR3. Svými vlastnostmi jsou si ale velmi podobné. Oba moduly jsou kompatibilní pro s jedním USB přijímačem, u kterého došlo pouze ke změně v softwaru.[25]

Liší se pouze v několika vlastnostech:

- Bezdrátový čip - MC1319x
- Typu senzoru - MMA7360L[25]

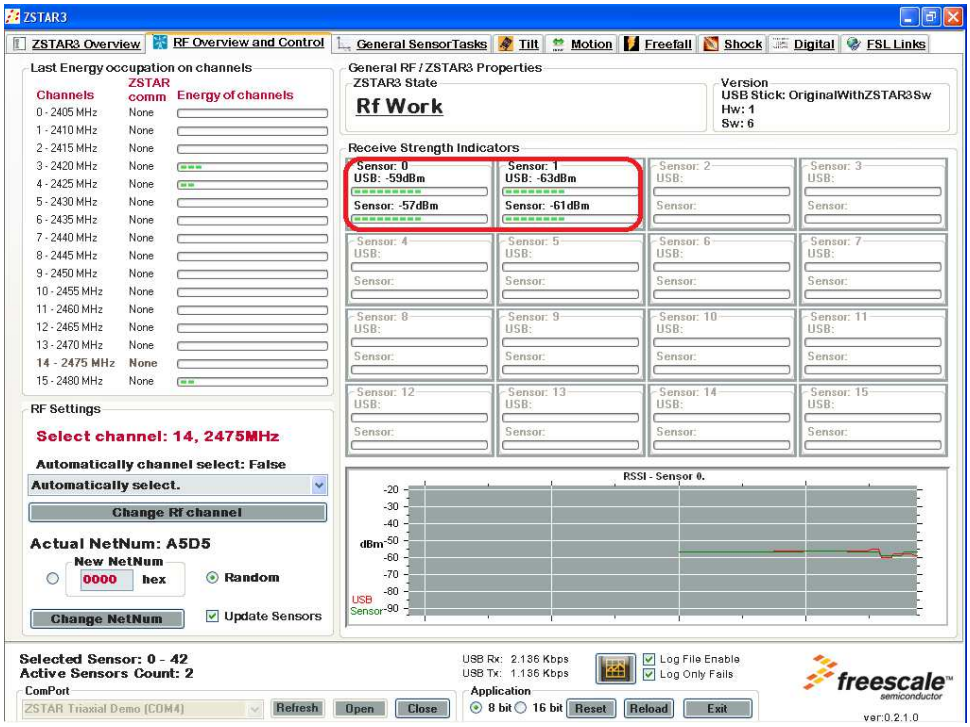
Vysílač ZSTAR2 je na obrázku (Obr. 33).

5.2 Průběh měření

Stejně jako v předchozích kapitolách jsme využili k praktickým ukázkám notebook. Bylo potřeba na něj nainstalovat ovladače zařízení a grafické uživatelské rozhraní ZSTAR3 GUI (Obr. 31). Připojili jsme přijímač pomocí USB k notebooku. Po vložení baterií do vysílačů došlo k navázání kontaktu s přijímačem a ihned jsme mohli sledovat průběh přenosu. Oba moduly jsou kompatibilní s jedním uživatelským prostředím.

Při každém měření jsme nechali USB přijímač ve statické poloze na jednom bodě a vysílač jsme přesunuli na určené místo. Po zapsání a uložení naměřených hodnot jsme pouze přesunuli vysílač na další požadované místo a pokračovali v zjišťování hodnot. Pro každou pozici jsme provedli tři měření modulem ZSTAR2 a tři měření modulem ZSTAR3. Vždy pro různé natočení antény vysílače k přijímači.

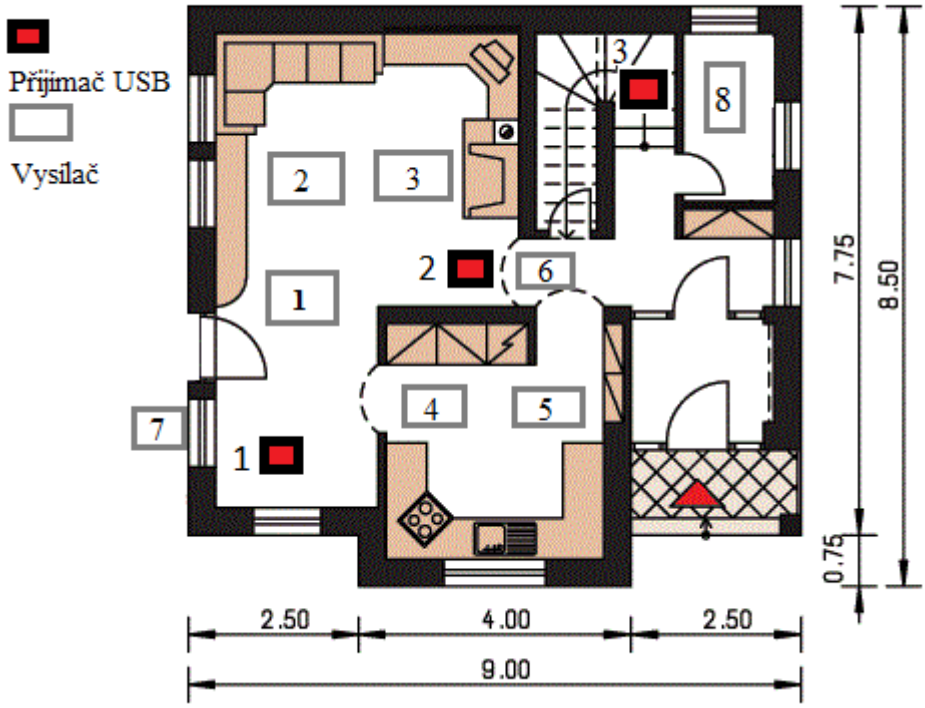
Zjišťovanými údaji byla síla signálu, kterou přijal USB přijímač, a také síla signálu přijatá vysílačem. Hodnoty jsou zobrazeny pomocí uživatelského rozhraní v jednotkách decibel (dB).



Obr. 31 Grafické uživatelské rozhraní pracující na 32bit Windows XP

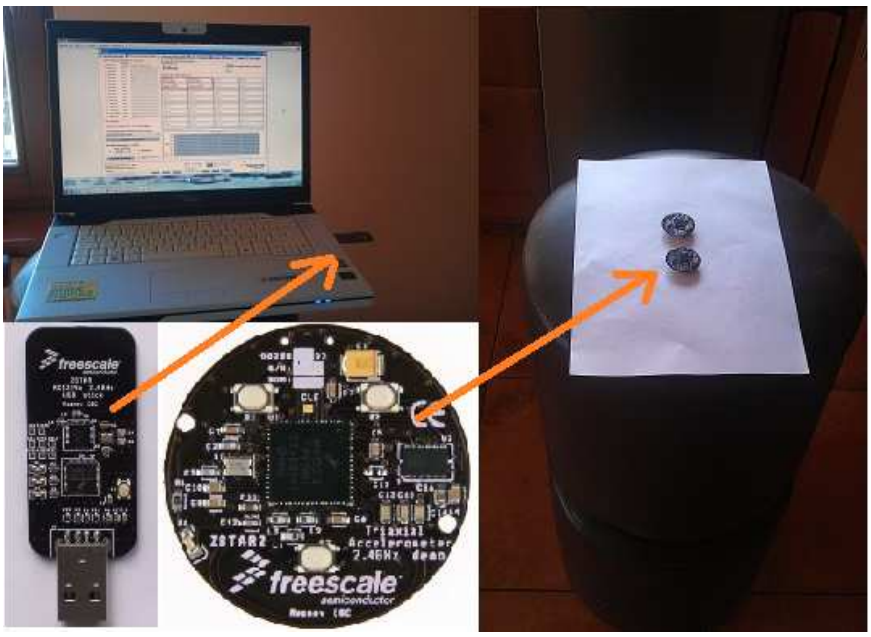
Měření proběhlo v rodinném domu v obci Jaroslavice u Zlína. V den měření byla teplota uvnitř 21,5 °C a venkovní teplota 17 °C. Vlhkost vzduchu byla 64 %. V místnostech, kde jsme měřili, byly vypnuty zařízení pracující na frekvenci 2,4GHz. USB přijímač i tak zaznamenal z okolní zástavby zdroje energie v tomto pásmu. V programu jsme proto nechali zapnutou možnost automatického výběru RF kanálu.

Umístění USB přijímače a i jednotlivých stanovišť s umístěným vysílačem je na obrázku (Obr. 32). Jde o půdorys rodinného domu Perla. Zakresleny jsou tři stanoviště s USB přijímačem. V pozicích 1, 2 jsme umístili USB přijímač do výšky 140cm. U pozice 3 jsme pracovali na schodech a USB přijímač byl ve výšce 160cm. Vysílač byl vždy umístěn ve stejné výšce. Měnilo se pouze natočení antény vysílače. Při první pozici byla anténa vysílače nasměrována k přijímači (pozice 0 °), poté jsme změnili polohu antény vysílače o 120 °, třetí a poslední pozice bylo opět pootočení o 120 °, vždy ve směru hodinových ručiček. Vzdálenost USB přijímače od vysílače je pak uvedena pro jednotlivá stanoviště v tabulkách (Tab. 9., Tab. 10.).



Obr. 32 Rozmístění prvků při měření

Ukázku stanoviště s vysílačem vidíme na obrázku (Obr. 33). K notebooku je připojen USB vysílač a je připraveno uživatelské rozhraní. Oba dva moduly, ZSTAR2 i ZSTAR3 jsou nachystány na svém místě, a je tedy možné přistoupit k měření.



Obr. 33 Stanoviště – vlevo USB přijímač a vpravo vysílač[25]

5.3 Měření v místnosti

Měřili jsme útlum v obytné místnosti v přízemí. Umístění USB přijímače odpovídalo pozici 1 dle obrázku (Obr. 32). Postupně jsme provedli měření pro umístění vysílače v pozicích 1 až 5. Vždy celkově 3 hodnoty pro jeden vysílač ZSTAR v různém nasměrování jeho antény. Vzdálenost jednotlivých umístění USB přijímače od vysílače se pohybovala od 2 do 6 metrů. Konkrétní vzdálenosti jsou diskutovány při zhodnocení výsledků.

5.4 Měření přes překážky

V první fázi měření měly rádiové vlny téměř volnou cestu k přijímači. V této kapitole jim v cestě bude stát překážka. Konkrétně půjde o okno, dveře a stěnu.

5.4.1 Skleněné okno

Pro měření, kdy šlo o zjištění útlumu přes okenní tabuli, bylo využito opět pozici USB přijímače v pozici 1. Vysílač se nacházel na pozici 7. Celková vzdálenost mezi vysílačem a USB přijímačem činila pro toto měření 80cm. Tloušťka okna má hodnotu 4+16+4, dohromady tedy 24mm.

5.4.2 Dřevěné dveře

Další měření bylo provedeno z pozice 2 pro USB přijímač a z pozice 6 pro vysílač. Podobně jako u okna, jsme nastavili vzdálenost mezi zařízeními na 80cm. Naměřené hodnoty vypovídají o situaci, kdy v cestě signálu stojí dřevěné dveře tloušťky 37 mm.

5.4.3 Betonová stěna

K poslednímu měření byla využita pozice 3 pro USB přijímač a 8 pro vysílač. Překážkou pro vysílání byla betonová stěna bez absence železa tloušťky 100mm. Vysílač byl od USB přijímače vzdálen 80cm. Specifikace dle manuálu ZSTAR3 uvádí možnost průchodu přes dvě stěny a jeden strop.

5.5 Zhodnocení výsledků

Oba moduly spolehlivě pracují při přímé viditelnosti uvnitř budovy na minimálně 10 metrů s uspokojivou kvalitou signálu. Hodnota pro 0 ° značí přímou viditelnost a pozici antény vysílače nasměrovanou k USB přijímači. Hodnoty 120 ° a 240 ° vyjadřují pootočení antény vysílače o právě tolik stupňů. Nejlepších výsledků jsme dosáhli při natočení 0 °, jak je patrné z výsledků v tabulkách (Tab. 9, Tab. 10). Vzdálenost je měřena od pozice USB přijímače k pozici vysílače v metrech. Měření proběhlo pro ZSTAR2 i ZSTAR3 totožně. Hodnoty jsme zapisovali pro dvě varianty. USB, kdy nám uživatelské rozhraní zobrazuje hodnoty přijaté USB přijímačem od vysílače. Senzor, kdy se nám zobrazují hodnoty přijaté vysílačem od USB přijímače. Všechny naměřené hodnoty jsou vyjádřeny jednotkou decibel (dB).

Tab. 9 Naměřené hodnoty RSSI pro modul ZSTAR2

USB - Senzor	ZSTAR2	0 °[dB]	120 °[dB]	240 °[dB]	Vzdálenost [m]
1 - 1	USB	-63	-68	-74	2
	Senzor	-67	-66	-72	
1 - 2	USB	-69	-76	-83	5
	Senzor	-75	-72	-79	
1 - 3	USB	-73	-71	-82	6
	Senzor	-78	-73	-83	
1 - 4	USB	-67	-68	-72	1,8
	Senzor	-75	-68	-77	
1 - 5	USB	-75	-77	-85	4,5
	Senzor	-81	-78	-83	
2 - 6	USB	-59	-69	-68	0,8
	Senzor	-62	-71	-70	
1 - 7	USB	-74	-69	-72	0,8
	Senzor	-83	-67	-75	
3 - 8	USB	-61	-64	-71	0,8
	Senzor	-63	-64	-74	

Tab. 10 Naměřené hodnoty RSSI pro modul ZSTAR3

USB - Senzor	ZSTAR3	0 °[dB]	120 °[dB]	240 °[dB]	Vzdálenost [m]
1 - 1	USB	-61	-60	-66	2
	Senzor	-68	-61	-64	
1 - 2	USB	-64	-68	-79	5
	Senzor	-72	-70	-71	
1 - 3	USB	-69	-71	-79	6
	Senzor	-75	-69	-77	
1 - 4	USB	-59	-64	-79	1,8
	Senzor	-66	-66	-72	
1 - 5	USB	-69	-75	-78	4,5
	Senzor	-76	-71	-75	
2 - 6	USB	-55	-60	-66	0,8
	Senzor	-60	-63	-68	
1 - 7	USB	-65	-62	-69	0,8
	Senzor	-75	-63	-72	
3 - 8	USB	-56	-58	-65	0,8
	Senzor	-61	-61	-70	

Srovnáme-li výsledky ze stanoviště 2 a 3, pak i přesto, že se jedná o změnu v posunu o jeden metr, vidíme větší nárůst zhoršení kvality signálu. Pravděpodobně ho má za následek zeď uprostřed, která je velmi blízko přenosové cestě. Zajímavě se také jeví pozice 5, kdy při pohybu vysílače jen trochu blíž k pozici 6 ztrácíme signál na obou modulech.

Dvojité sklo, se jeví jako mnohem horší překážka, než dřevěné dveře nebo dokonce betonová zeď. U těchto tří variant jsme měřili ze stejné vzdálenosti a útlum u okna byl mnohem větší. Měření pro dveře a zeď dosahovaly velmi podobných hodnot u obou modulů.

Dosah by se měl pohybovat do vzdálenosti až 70 metrů na volném prostranství, jak uvádí specifikace od Freescale. Uvnitř budovy nepředstavovalo 10 metrů při přímé viditelnosti žádný problém v kvalitě signálu, a tak jsou jejich hodnoty pravděpodobné. Závěrem bych vyzdvihl modul ZSTAR3, který dostál pozice novějšího zařízení a ve všech měřeních starší typ porazil.

ZÁVĚR

V teoretické části se čtenář seznamuje s metodami a způsoby bezdrátového přenosu dat ze snímače na centrální jednotku. Provedli jsme analýzu stávajících řešení přenosu dat, se zaměřením na ty nejrozšířenější, nejpoužívanější a nejperspektivnější. Jednotlivé metody jsme rozdělili podle jejich úrovní, tedy od signální úrovně až po datovou úroveň LAN. Zhodnotili jsme také výhody a nevýhody těchto řešení.

V další části práce jsme uvedli seznam teorie, která se k bezdrátovému přenosu dat váže. Zmínili jsme rádiové vlny a vlivy na bezdrátový přenos dat jako jsou absorpce a odrazy od překážek. Dále jsme rozebrali teorii modulačních technik. Jednotlivé standardy Wi-Fi totiž využívají jiné modulační techniky. Ruku v ruce s vývojem standardů jde i vývoj právě modulačních technik. Uvedli jsme také možnosti zabezpečení bezdrátového přenosu dat. Jelikož lze bezdrátový přenos lehce odposlouchávat, vyvstala nutnost jej zabezpečit. Výčet možných rizik včetně způsobů, jak jím předejít nebo je minimalizovat jsme probrali teoreticky a taky později jako ukázku. V závěru této kapitoly jsme se dostali k problematice senzorů, které jakožto důležitá součást při měření v průmyslu a průmyslové automatizaci nemohli chybět.

V praktické části jsme se věnovali porovnání WPAN a WLAN a taky jejich praktickými aplikacemi. U WLAN jsme využili znalosti z teoretické části pro provedení zabezpečení domácí sítě Wi-Fi. Poté jsme využili software pro monitoring a skenování Wi-Fi sítí a předvedli jeho ukázku.

Na závěr jsme provedli měření na vývojových modulech ZSTAR2 a ZSTAR3, kdy jsme pomocí nich řešili problematiku kvality signálu vevnitř budovy. Testovali jsme šíření signálu přes překážky, jako jsou okna, dveře nebo stěna. Oba moduly splnily vlastnosti dané svou specifikací pro šíření v budově. O jejich vlastnosti fungovat uspokojivě přes dvě stěny a strop by se dalo ale spekulovat. Není totiž uvedena šířka těchto zdí ani stropu. A při měření jsme zjistili, že pokud do cesty zasáhne velmi silná stěna, signál se ztrácí.

Problematika senzorů a s nimi související měření kvality signálů je atraktivní téma, o kterém se bude ještě hodně diskutovat. Rád bych se věnoval tomuto tématu podrobněji i při psaní své diplomové práce.

ZÁVĚR V ANGLIČTINĚ

In the theoretical part the reader becomes familiar with methods and processes of wireless data transmission between sensors and central units. We conducted an analysis of existing data transmission solutions with focus on the most popular, the most used and the most promising. Different kind of methods were divided according to their levels, thus from the signal level to the data level D2. Advantages and disadvantages of these solutions were also evaluated.

In the next section we introduced the theory that binds to the wireless data transmission. We mentioned radio waves and influence on the wireless data transmission such as absorption and reflection from obstacles. Furthermore, we analyzed the theory of modulation techniques. Different modulation techniques are being used by all of Wi-Fi standards. Hand in hand with the development of standards goes as well the development of modulation techniques. The possibilities of wireless security were presented as well. Wireless transmission can be easily tapped, therefore it needs to be secured. The list of potential risks, but also ways how to prevent or minimize them, was discussed theoretically and examples were made. At the end of this chapter we aim at the issue of sensors that is an important part of the measurement in the industry and industrial automation.

In the practical part, we focused on comparing WPAN and WLAN, and also their practical applications. For WLAN, we used the knowledge from the theoretical part for the implementation of Wi-Fi security. Then we used the software for monitoring and scanning Wi-Fi networks and performed an illustration.

Finally, we made measurements on development modules ZSTAR2 and ZSTAR3. We used them to solve the issue of signal quality inside the building. We tested the signal propagation through obstacles such as window, door or wall. We could speculate about their attribute to operate satisfactorily through two walls and the ceiling. There is not given width of these walls or ceiling. During the measurement, we found that if the path reaches a very thick wall, the signal is lost.

The isme of sensors and signal quality measurement are attractive themes, of which will be a lot of discussion. Iwould like to pursue to these issues in more detail in thesis.

SEZNAM POUŽITÉ LITERATURY

[1] HRUŠKA, František. Projektování řídících a informačních systémů. První. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. 175 s. ISBN 978-80-7318-979-2.

[2] HRUŠKA, František. Technické prostředky informatiky a automatizace. Učební texty. 1.vyd. Zlín: UTB ve Zlíně, duben 2007, s. 193. ISBN 978-80-7318-535-0.

[3] HYNČICA, Ondřej. Bezdrátové sítě typu mesh. Automa [online]. 2005, roč. 2005, č. 12, s. 2[cit. 2013-05-17]. Dostupné z: http://www.odbornecasopisy.cz/index.php?id_document=30826

[4] Tumanski, S. Principles of electrical measurement. Taylor &Francis, Boca Raton, s. 472, ISBN 0-7503-1038-3.

[5] LEGG, Gary. ZigBee: Wireless Technology for Low-Power Sensor Networks. EE Times [online]. 2004, 5. 6. 2004 [cit. 2013-05-17]. Dostupné z: http://www.eetimes.com/design/communications-design/4017853/ZigBee-Wireless-Technology-for-Low-Power-Sensor-Networks

[6] Product ZT-2550. In: Icpdas.com [online]. [cit. 2013-05-17]. Dostupné z: http://www.icpdas.com/root/product/solutions/industrial_wireless_communication/wireless_solutions/zt-2550.html

[7] EnOcean Wireless Standard. EnOcean [online]. 2012 [cit. 2013-05-17]. Dostupné z: http://www.enocean.com/en/enocean-wireless-standard/

[8] LOHMANN, Gerrit. První výrobky s rozhraním WirelessHART budou zanedlouho uvedeny na trh. Automa [online]. 2009, roč. 2009, č. 1, s. 2 [cit. 2013-05-17]. Dostupné z: http://www.odbornecasopisy.cz/res/pdf/38453.pdf

[9] HYNČICA, Ondřej a Karel PAVLATA. Bezdrátové komunikační systémy založené na IEEE 802.15.4 v automatizaci. Automa [online]. 2011, roč. 2011, č. 6, s. 3 [cit. 2013-05-17]. Dostupné z: http://www.odbornecasopisy.cz/res/pdf/43749.pdf

[10] BOURKE, Tim. SA 100.11 a zcela odstraňuje potřebu standardu WirelessHART. Automa [online]. 2010, roč. 2010, č. 7, s. 4 [cit. 2013-05-17]. Dostupné z: http://www.odbornecasopisy.cz/res/pdf/41653.pdf

[11] CAROLL, Brandon James. Bezdrátové sítě Cisco: Autorizovaný výukový průvodce. První. Holandská 3, 639 00 Brno: Compure Press, a.s., 2011. ISBN 978-80-251-2884-8.

[12] Gigabitové Wi-Fi příští generace: 802.11ac. NetGear [online]. 2012, s. 4 [cit. 2013-05-17]. Dostupné z: http://www.netgear.cz/images/80211acFinal66-54105.pdf

[13] ŠALANDA, Marek. Bezdrátová síť WiFi čtvrté generace pro náročné průmyslové podmínky. Automa [online]. 2009, roč. 2009, č. 10, s. 2 [cit. 2013-05-17]. Dostupné z: http://www.odbornecasopisy.cz/res/pdf/39716.pdf

[14] Bezdrátové sítě. [online]. [cit. 2013-04-05]. Dostupné z: http://bezdratovesite.wz.cz/

[15] KÖHRE, Thomas. Stavíme si bezdrátovou síť Wi-Fi. první. Nám. 28. dubna 48, 635 00 Brno: Computer Press, 2004. ISBN 80-251-0391-9.

[16] HartComm: Wireless HART - How it works. [online]. [cit. 2013-05-17]. Dostupné z: http://www.hartcomm.org/protocol/wihart/wireless_how_it_works.html

[17] Bezdrátové technologie. In: BLÁBOLIL, Roman. Blabik [online]. 2010, 15. července 2010 [cit. 2013-05-17]. Dostupné z: http://www.blabik.cz/vyuka/ict/29_Bezdratove_technologe.pdf

[18] GSM Technologies. In: TechGSM [online]. [cit. 2013-05-17]. Dostupné z: http://www.techgsm.com/page/gsm-technologies/gsm-technologies-network-tdma-cdma-umts.html

[19] HRUŠKA, F. Senzory pro systémy informatiky a automatizace. Učební texty. 1.vyd. Zlín: UTB ve Zlíně, prosinec 2007, s. 177. ISBN 978-80-7318-630-2.

[20] WEBSTER, J., G. The measurement, instrumentation, and sensor handbook. New York: CRC Press LLC; Springer-Verlag, 1999, s. 1932. ISBN 3-540-64830-5.

[21] Altmann W. Practical Process Control for Engineers and Technicians. ELSEVIER, 2006, s. 290, ISBN 978-0-7506-6400-4.

[22] DYER, S., A. Survey of istrumentation and measurement. John Wiley and Sons, 2001, s. 1096. ISBN 0-471-39484-X.

[23] IEEE standards association: IEEE 802.15™: WIRELESS PERSONAL AREA NETWORKS (PANs). [online]. [cit. 2013-05-17]. Dostupné z: http://standards.ieee.org/about/get/802/802.15.html

[24] PUŽMANOVÁ, Rita. Přehled novinek v normalizaci LAN. [online]. 20. 1. 2005 [cit. 2013-05-17]. Dostupné z: http://www.lupa.cz/clanky/prehled-novinek-v-normalizaci-lan/

[25] DRM103 Designer Reference Manual. In: Freescale.com [online]. 2009 [cit. 2013-05-20]. Dostupné z: http://www.freescale.com/files/microcontrollers/doc/ref_manual/ZSTAR3RM.pdf?fpsp=1

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

LAN	Advanced Encryption Standard
SIA	Systém Informatiky a Automatizace
GSM	Groupe Speciál Mobile
Wi-Fi	Wireless Fidelity
USB	Universal Serial Bus
PAN	Private Area Network
IEEE	The Institute of Electrical and Electronics Engineers
ISM	Indutstrial, Scientific and Medical
MAC	Media Access Control
FHSS	Frequency Hopping Spread Spectrum
IrDA	Infrared Data Association
LED	Light-Emitting Diode
DSSS	Direct Sequence Spread Spectrum
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
AES	Advanced Encryption Standard
IEC	International Electrotechnical Commission
HART	Highway Addressable Repote Transducer
TDMA	Time Division Multiple Access
DCS	Distributed Control System
ISA	The International Society of Automation
TCP/IP	Transmission Control Protocol/Internet Protocol
CCK	Complementary Code Keying
MIMO	Multiple-Input and Multiple-Output
FDMA	Frequency Division Multiple Access

CDMA	Code Division Multiple Access
GPRS	General Packet Radio Service
OFDM	Orthogonal Frequency Division Multiplex
RSSI	Received Signal Strength Indication
HTML	Hyper Text Markup Language
SSID	Service Set Identifier
MFP	Management Frame Protection
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
TKIP	Temporal Key Integrity Protocol
EAP	Extensible Authentication Protocol
EAP-FAST	EAP – Flexible Authentication via Secure Tunel
EAP-TLS	EAP – Transport Layer Security
LEAP	Lightweight Extensible Authentication Protocol
PEAP	Protected Extensible Authentication Protocol
AP	Access Point
BPSK	Binary Phase Shift Keying
DBPSK	Differential Binary Phase Shift Keying
DQPSK	Differential Quaternary Phase Shift Keying
DES	Data Encryption Standard
PSK	Pre Shared Key
UNII	Unlicensed National Information Infrastructure
WLAN	Wireless Local Area Network
WPAN	Wireless Private Area Network

SEZNAM OBRÁZKŮ

SEZNAM TABULEK