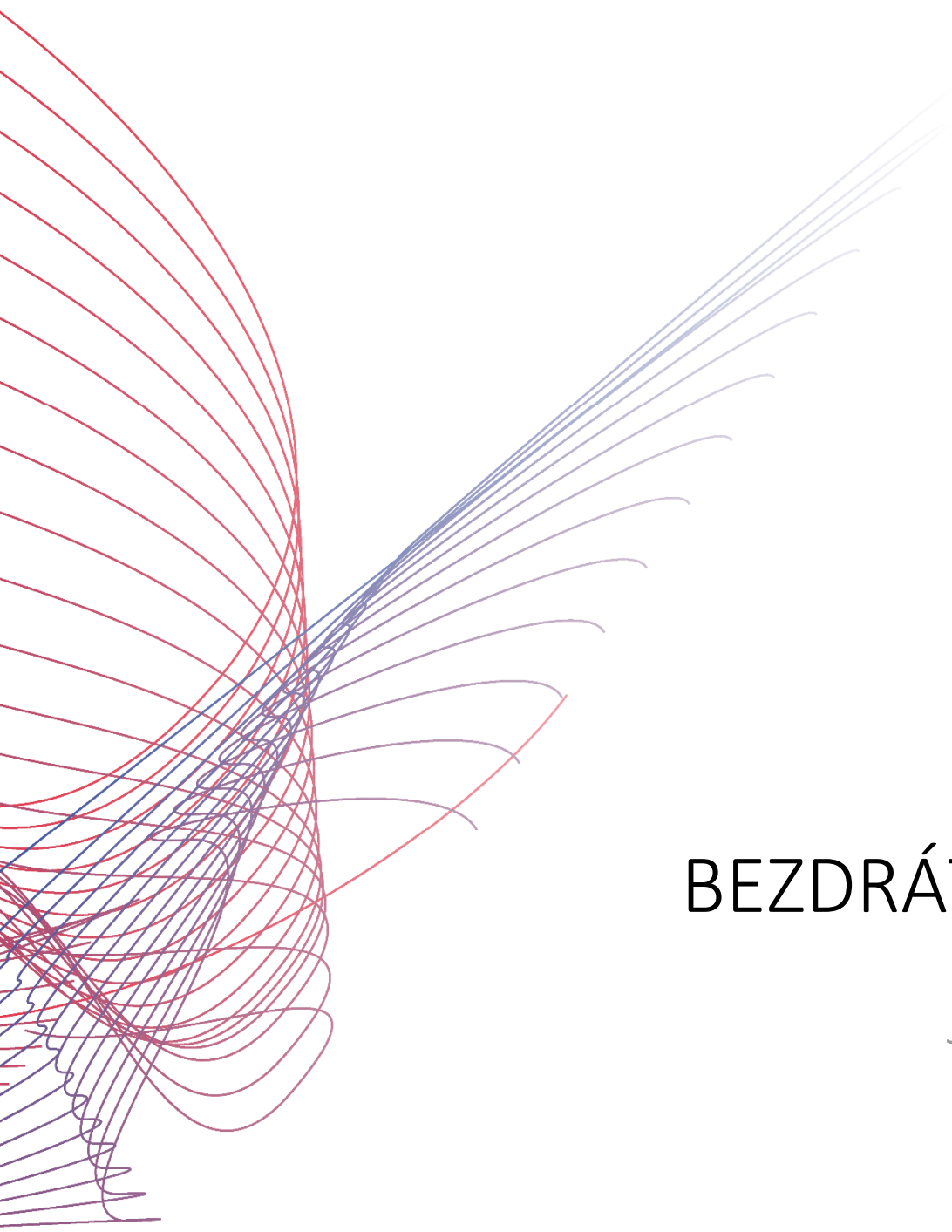
en
cs de
sk es

TECH
pedia



BEZDRÁTOVÉ SÍTĚ

JORDI SALAZAR

Název díla: Bezdrátové sítě
Autor: Jordi Salazar
Přeložil: Ivan Pravda
Vydalo: České vysoké učení technické v Praze
Fakulta elektrotechnická
Kontaktní adresa: Technická 2, Praha 6
Tel.: +420 224352084
Tisk: (pouze elektronicky)
Počet stran: 41
Edice (vydání): 1. vydání, 2017

ISBN 978-80-01-06196-1

TechPedia
European Virtual Learning Platform for Electrical and Information Engineering
http://www.techpedia.eu

Tento projekt byl realizován za finanční podpory Evropské unie.
Za obsah publikací odpovídá výlučně autor.
Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

Vysvětlivky

	Definice
	Zajímavost
	Poznámka
	Příklad
	Shrnutí
	Výhody
	Nevýhody

ANOTACE

Tento modul poskytuje aktuální přehled bezdrátových sítí s primárním zaměřením na bezdrátové sítě typu LAN. Popisuje a vysvětluje základy různých typů bezdrátových technologií užívaných u moderních komunikačních systémů se zaměřením na jejich hlavní charakteristiky, problematiku bezpečnosti, výhody a nevýhody a jejich možné uplatnění v konkrétních síťových aplikacích.

CÍLE

Modul se zaměřuje na specifika a odlišnosti síťových architektur u různých typů bezdrátových technologií, dále se zabývá bezpečnostními aspekty bezdrátových sítí a závěrem seznamuje s výhodami a nevýhodami bezdrátových sítí.

LITERATURA

[1] STALLINGS, W.: *Wireless Communications and Networks*, Second Edition, Pearson Prentice Hall, Upper Saddle River, NJ, 2005. ISBN 0-13-191835-4.

[2] CIUBOTARU, B.; MUNTEAN, G. M.: *Advanced Network Programming. Principles and Techniques*, Springer-Verlag London, 2013. ISBN 978-1-4471-5292-7.

[3] SHARMA, K.; DHIR, N.: *A study of wireless networks: WLANs, WPANs, WMANs, and WWANs with comparison*, International Journal of Computer Science and Information Technologies, vol. 5 (6), pp. 7810-7813, 2014.

[4] POTHUGANTI, K.; CHITNENI, A.: *A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi*, Advance in Electronic and Electric Engineering, vol. 4 (6), pp. 655-662, 2014.

[5] *An introduction to Wi-Fi*, Rabbit product manual, Digi International Inc., 2007-2008. (www.rabbit.com)

[6] IEEE Standards Association web site (http://standards.ieee.org/index.html) [on-line].

Obsah

1 Úvod do bezdrátových sítí

Tento modul je možné chápat jako přehledový pohled na problematiku bezdrátových sítí s primárním zaměřením na bezdrátové sítě typu **LAN** (*Local Area Network*). Popisuje a vysvětluje základy různých typů bezdrátových technologií užívaných u moderních komunikačních systémů se zaměřením na jejich hlavní charakteristiky, problematiku bezpečnosti, výhody a nevýhody a jejich možné uplatnění v konkrétních síťových aplikacích.

Bezdrátové sítě jsou takovým typem sítí, které propojují koncová zařízení bez nutnosti instalace jakékoliv kabeláže a pro přenos signálu využívají volný prostor a rádiové vlny.

Zařízeními běžně využívanými v bezdrátových sítích mohou být přenosné počítače (laptopy, notebooky atd.), stolní počítače, různé typy handheldů (Gameboy, Nintendo DS, Sony PSP a další), palmtopy **PDA** (*Personal Digital Assistant*), mobilní telefony, tablety a pagery. Na první pohled pracují bezdrátové sítě stejným způsobem jako sítě pevné, nicméně u bezdrátových sítí je nutné převést přenášené signály do podoby a formátu vhodného pro přenos volným prostorem.

Bezdrátové sítě slouží mnoha účelům. V některých případech jsou využívány jako alternativa nebo náhrada klasického pevného připojení, v jiných případech mohou zajišťovat přístup k uživatelským datům z odlehlých lokalit, kde není k dispozici klasické připojení k datovým sítím.

Bezdrátová infrastruktura může být vybudována s velmi nízkými náklady v porovnání s tradičními klasickými pevnými přípojkami. Avšak samotné budování bezdrátových sítí přináší úsporu nejen finančních nákladů. Další úspora souvisí s využitelností přímého přístupu na Internet a do datových sítí připojenými účastníky, kteří tak získávají levnější a uživatelsky komfortnější přístup k požadovaným informacím. Úspora času a vynaloženého úsilí k získání požadovaných informací a dat se následně promítá do globální míry bohatství dané společnosti, jelikož lze uskutečnit více práce za mnohem kratší čas a s vynaložením menšího úsilí.

Bezdrátové sítě umožňují připojení vzdálených zařízení bez potíží a ohledu na to, zda jsou od dostupného přístupového bodu vzdálena jen metry či kilometry. Není zde také nutno budovat kabeláž ani instalovat rozvody. Tyto rysy činí bezdrátové technologie velmi oblíbenými a populárními a urychlují tak jejich masové rozšíření k velkému počtu uživatelů.

V bezdrátových sítích je využívána celá řada různých technologií, které se odlišují využívanými frekvenčními pásmy, maximální přenosovou rychlostí a dostupným dosahem jejich vysílání.

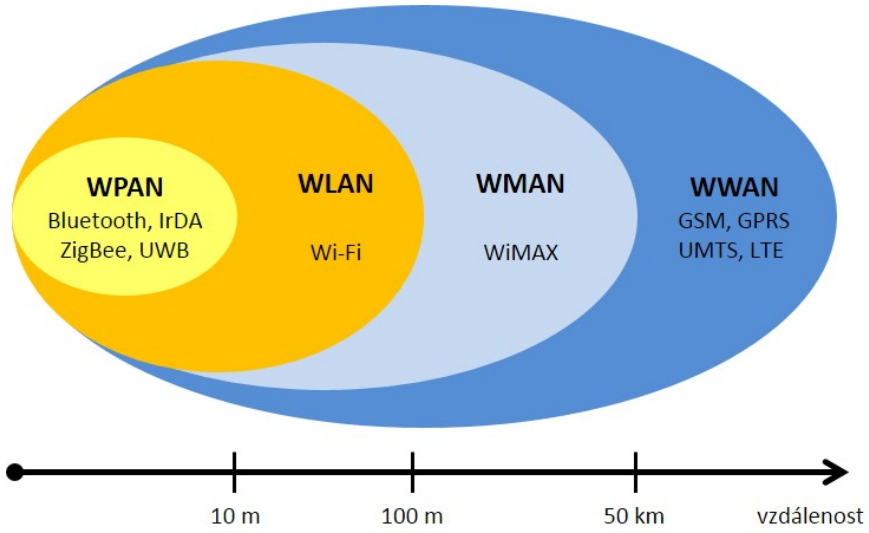
Na druhou stranu je zde nutno řešit specifické právní otázky související se správou elektromagnetického spektra. Elektromagnetické vlny jsou vysílány různými typy zařízení, avšak jejich provoz je velmi citlivý na rušení. Z tohoto důvodu potřebují všechny země určité legislativní předpisy a závazná doporučení, která přesně

definují použitelný frekvenční rozsah a povolené vysílací výkonové úrovně pro jednotlivé typy kooperujících bezdrátových technologií.

Kromě toho nejsou elektromagnetické vlny jednoduše ze svého principu spojeného se šířením volným prostorem geograficky a prostorově omezitelné. Z tohoto principu mohou hackeři velmi snadno a jednoduše odposlouchávat datový provoz, pokud nejsou vysílaná data řádně zakódována a zašifrována. Proto je nutné, aby byla podniknuta veškerá možná a dostupná opatření k zajištění utajení dat přenášených prostřednictvím bezdrátových sítí.

2 Bezdrátové sítě a technologie

Bezdrátové sítě mohou být rozděleny do čtyř specifických skupin v závislosti na účelu jejich použití a použitelném dosahu signálu [1-3]: sítě **WPAN** (*Wireless Personal Area Network*), sítě **WLAN** (*Wireless Local Area Network*), sítě **WMAN** (*Wireless Metropolitan Area Network*) a sítě **WWAN** (*Wireless Wide Area Network*). Obrázek 1.1 graficky znázorňuje zmíněné čtyři kategorie a příklady některých technologií užívaných v daném typu sítí.



Obr. 1.1 Klasifikace bezdrátových sítí s příklady provozovaných technologií

Kromě toho mohou být bezdrátové sítě rozděleny do dvou kategorií dle svého dosahu – sítě krátkého dosahu **SR** (*Short Range*) a sítě dlouhého dosahu **LR** (*Long Range*). Bezdrátové sítě s krátkým dosahem **SR** jsou vlastně sítě s omezeným dosahem na vymezeném prostoru. Tato definice se týká především bezdrátových sítí typu **LAN**, které nalezneme v administrativních budovách, školních areálech, výrobních závodech ale i v domácnostech, ale zároveň i bezdrátových sítí typu **PAN** (*Personal Area Network*), díky kterým mohou mezi sebou komunikovat přenosná zařízení avšak jen s výrazně omezeným dosahem. Sítě typu **WPAN** obvykle pro svůj provoz využívají nelicencované frekvenční pásmo **ISM** (*Industrial, Scientific and Medical*) vyhrazené pro průmyslové, vědecké a lékařské využití. Dostupné frekvence jsou v různých zemích odlišné. Nejužívanějšími frekvenčními pásmy jsou pásma okolo 2,4 GHz a 5 GHz, která jsou volně dostupná ve většině zemí. Snadná dostupnost těchto pásem umožňuje řadě uživatelů provozovat bezdrátové sítě bez nutnosti získání licence a zcela bezplatně. Obě předešlé skutečnosti mají velmi významný vliv na rychlost expanze tohoto typu sítí do každodenního života obyvatel naší planety.

Bezdrátové sítě dlouhého dosahu jsou typicky realizovány společnostmi (tzv. providery), které poskytují bezdrátové připojení k Internetu a s ním spojené doplňkové služby. Tyto sítě pokrývají signálem rozsáhlé oblasti, jakými jsou například velká města, okresy, kraje nebo celé území státu. Hlavním úkolem sítí dlouhého dosahu je tedy poskytování bezdrátového připojení v globálním měřítku.

Do kategorie sítí dlouhého dosahu oprávněně patří bezdrátové sítě typu **WMAN** a **WWAN**. Pokud je vyžadováno skutečné globální pokrytí, pak jsou pro tento účel k dispozici tzv. satelitní sítě.

2.1 Personální bezdrátové sítě (WPAN)

Bezdrátové personální sítě jsou založeny na standardu IEEE 802.15 [http://en.wikipedia.org/wiki/IEEE_802.15] [3-4]. Svou koncepcí umožňují komunikaci na velmi krátkou vzdálenost přibližně do 10 metrů. V porovnání s ostatními typy bezdrátových sítí vyžadují sítě **WPAN** pro účely externího propojení s těmito sítěmi pouze malou nebo vůbec žádnou podpůrnou infrastrukturu. To umožňuje realizovat malá, výkonná a nenákladná řešení, která mohou být realizována pomocí široké škály zařízení, jakými jsou např. smartphony a palmtopy **PDA**.

Tyto sítě jsou charakterizovány nízkými energetickými nároky a relativně nízkou přenosovou rychlostí. Tento typ sítí využívá technologií jako je Bluetooth, **IrDA** (*Infrared Data Association*), ZigBee nebo **UWB** (*Ultra Wide Band*). Z aplikačního hlediska je technologie Bluetooth vhodná pro zařízení jako jsou bezdrátové myši, klávesnice a hands-free headsety, technologie **IrDA** pro komunikaci typu bod-bod mezi dvěma zařízeními se zaměřením na jednoduché datové přenosy a synchronizaci souborů, technologie ZigBee je navržena pro účely spolehlivého bezdrátového monitorování stavu sítě a jejího řízení a technologie **UWB** je zaměřena na oblast širokopásmových multimediálních přenosů.

Přenosová rychlost udává počet přenesených nebo přijatých bitů za jednotku času (*bps* nebo *bit/s*).

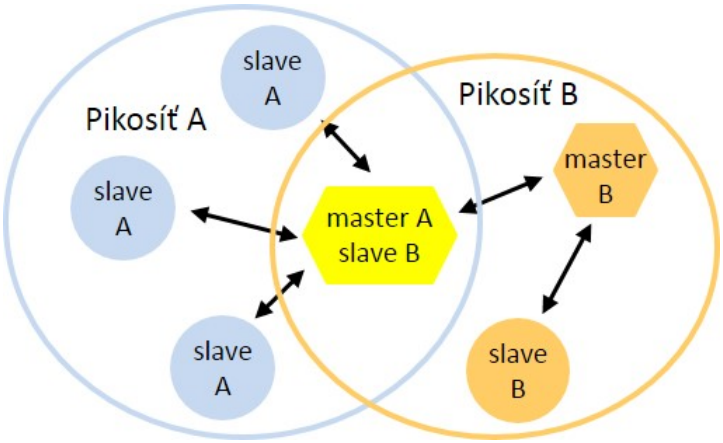
Modem je zařízení umožňující počítači vysílat a přijímat data.

Technologie Bluetooth

Technologie Bluetooth je založena na standardu IEEE 802.15.1. Původně byla technologie Bluetooth navržena pro komunikaci s nízkou spotřebou, krátkým dosahem, využívající všesměrový režim vysílání (typ *Point-to-Multipoint*) a cenově dostupná zařízení a propojující jednotlivá zařízení pomocí sítí typu Ad-hoc. V současnosti navrhují vývojáři Bluetooth komponenty a podpůrné systémy pro celou řadu nových aplikací. Technologie Bluetooth specifikuje tři odlišné třídy zařízení: *třída 1* (dosah do 100 metrů), *třída 2* (dosah do 10 metrů) a *třída 3* (dosah do 1 metru). Využitím pásma 2,4 GHz mohou dvě zařízení v dosahu pokrytí signálu sdílet až 720 kbit/s své kapacity, resp. přenosové rychlosti. Nejčastěji používanou třídou je *třída 2*.

Topologie sítě Bluetooth se skládá z pikosítí a může propojovat až 8 aktivních zařízení v uspořádání *Master-Slave*. První zařízení Bluetooth v pikosíti je *Master*, všechna ostatní zařízení jsou zařízení podřízená (typ *Slave*), která komunikující v síti pomocí zařízení *Master*. Typický dosah pikosítě je 10 metrů, za ideálních podmínek však může dosáhnout až 100 metrů. Všechna propojení jsou z důvodu zajištění bezpečnosti kódována a chráněna proti odposlechu a vlivu rušení. Dvě pikosítě mohou vytvořit topologii nazývanou Scatternet. Zařízení Bluetooth se pak mohou vyskytovat v několika pikosítích současně, což umožňuje přenášet a sdílet

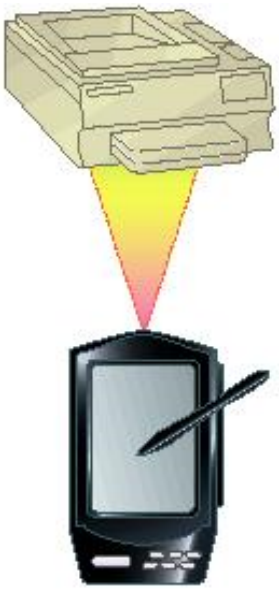
informace i mimo dosah původní pikosítě. Zařízení může být na pozici *Slave* v několika pikosítích, jako *Master* však pouze v jediné.



Obr. 1.2 Bluetooth Scatternet topologie. Master v pikosíti A je slave v pikosíti B.

Technologie IrDA

Asociace **IrDA** specifikuje ucelený soubor infračervených komunikačních standardů. Technologie **IrDA** se na tento soubor norem odkazuje a díky nim je schopna vytvořit bezdrátové propojení dvou zařízení, která by za normálních okolností byla propojena kabelem. Technologie **IrDA** má nízkou spotřebu, nízké provozní náklady, úzký vyzařovací úhel (< 30º), vytváří jednosměrná propojení typu *Point-to-Point*, data jsou přenášena v konceptu Ad hoc sítí s dosahem až 1 metr a rychlostmi od 9600 bit/s do 4 Mbit/s (v současnosti), 16 Mbit/s (ve vývoji). Rozhraní **IrDA** jsou integrována do notebooků, palmtopů **PDA**, tiskáren a kamer.

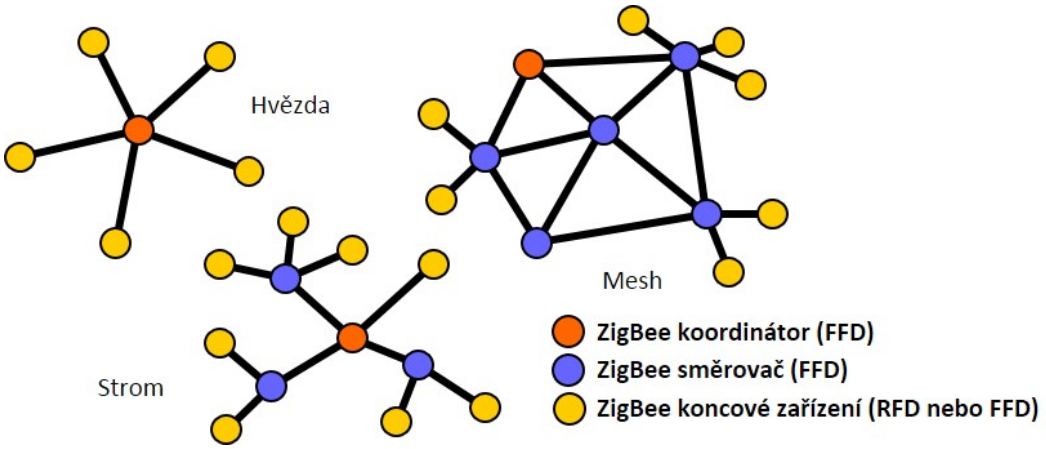


Obr. 1.3 Komunikace IrDA mezi palmtopem PDA a tiskárnou (typ bod-bod)

Technologie ZigBee

Technologie ZigBee je založena na standardu IEEE 802.15.4. Byla vyvíjena jako otevřený globální standard řešící požadavky v oblasti snadné implementace, vysoké spolehlivosti, nízkých provozních nákladů, nízké spotřeby a vývoje nízkorychlostních síťových bezdrátových datových zařízení. Technologie ZigBee pracuje v nelicencovaných pásmech zahrnující kmitočty 2,4 GHz, 900 MHz a 868 MHz s maximální dostupnou přenosovou rychlostí až 250 kbit/s, která je plně dostačující pro bezdrátové přenosy u senzorů a v automatizačních systémech.

Technologie ZigBee také slouží pro vytváření rozlehlejších bezdrátových sítí s nízkými nároky na datovou propustnost. V síti ZigBee mohou spolupracovat dva odlišné typy zařízení – plně funkční zařízení **FFD** (*Full-Function Device*) a funkčně omezené zařízení **RFD** (*Reduced-Function Device*). Zařízení **FFD** může pracovat ve třech nezávislých provozních režimech, a to jako **WPAN** koordinátor, obecný koordinátor (*ZigBee Router*) nebo koncové zařízení. Zařízení **RFD** je určeno pouze pro aplikace, které jsou extrémně jednoduché (např. vypínač světla). Technologie ZigBee podporuje tři odlišné síťové topologie – hvězda, MESH a strom (*Cluster Tree*), které jsou znázorněny na Obrázku 1.4. V topologii hvězda je komunikace mezi zařízeními realizována a koordinována jedním centrálním kontrolérem, nazývaným **WPAN** koordinátor. V topologii MESH může jakékoliv zařízené komunikovat s jiným zařízením, pokud jsou obě ve vzájemném dosahu. Sítě se stromovou topologií jsou speciálním případem MESH sítí, ve kterých pracuje většina zařízení jako typ **FFD** a zařízení typu **RFD** mohou být připojena do síťové infrastruktury pouze jako koncová zařízení bez možnosti dalšího větvení. Kterékoliv zařízení typu **FFD** může pracovat jako směrovač a poskytovat synchronizaci ostatním zařízením a směrovačům. Pouze jeden z těchto směrovačů však může být koordinátorem **WPAN**.



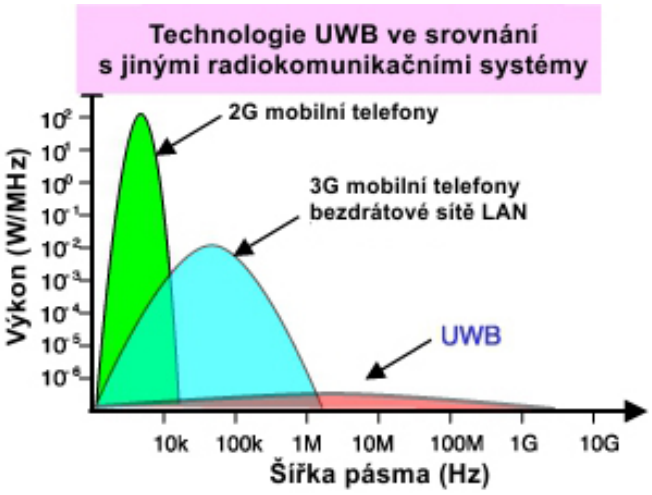
Obr. 1.4 Síťový diagram ZigBee

Technologie UWB

Technologie **UWB** (*Ultra Wide Band*), založená na standardu IEEE 802.15.3, je v současnosti velmi zajímavou technologií pro účely vysokorychlostní bezdrátové komunikace realizované ve vnitřních prostorech (např. budovy, domácnosti,…) s omezeným dosahem. Technologie **UWB** slouží zcela odlišnému účelu než ostatní

technologie zmíněné v této části. Technologie **UWB** totiž umožňuje přenos objemných datových souborů vysokými přenosovými rychlostmi na krátkou vzdálenost. Technologie **UWB** disponuje robustními datovými přenosy s rychlostmi řádově od 110 Mbit/s do 480 Mbit/s na vzdálenost až několika metrů, které jsou schopny uspokojit potřeby většiny multimediálních aplikací (např. audio a video aplikace provozované v rámci domácnosti). Dále může fungovat také jako bezdrátová náhrada klasické sériové sběrnice rozhraní USB 2.0 nebo IEEE 1394. V Americe bylo pro účely technologie **UWB** vyhrazeno kmitočtové pásmo od 3,1 GHz do 10,6 GHz. V Evropě je situace odlišná. Frekvenční pásmo je totiž složeno ze dvou dílčích subpásem. První subpásmo začíná na frekvenci 3,4 GHz a končí frekvencí 4,8 GHz, druhé subpásmo pak pokračuje v pásmu od frekvence 6 GHz do frekvence 8,5 GHz.

Přenosy **UWB** jsou realizovány generováním rádiového signálu jen ve vyhrazených časových intervalech, které však zabírají velkou šířku kmitočtového pásma (viz Obrázek 1.5), a to použitím pulsně-polohové nebo pulsně-šířkové modulace. Uživatelská data mohou být také modulována na UWB signály (pulsy) zakódováním polarity pulsu a/nebo jeho amplitudy pomocí ortogonálních pulsů. UWB pulsy mohou být vysílány nepravidelně s relativně nízkou pulsní rychlostí s podporou pulsně-šířkové nebo pulsně-polohové modulace, ale mohou být také vysílány rychlostmi úměrnými šířce pásma vyhrazené těmto **UWB** pulsům.



Obr. 1.5 Využití výkonového a frekvenčního spektra technologií UWB

2.2 Lokální bezdrátové sítě (WLAN)

Bezdrátové lokální sítě **WLAN** jsou navrženy tak, aby byly schopny zajistit bezdrátový přístup v oblastech s typickým dosahem do 100 metrů (měřeno ve volném prostoru), a jsou tak využívány převážně v domácnostech, školách, počítačových laboratořích nebo kancelářském prostředí (viz Obrázek 1.6). Tato koncepce tedy umožňuje prostorově omezený pohyb uživatelů daný pokrytím signálem, avšak s možností být na vymezeném území neomezeně připojen k síti [2,5]. Sítě **WLAN** jsou založeny na standardech IEEE 802.11 a marketingově označovaných zkratkou **Wi-Fi** (*Wireless Fidelity*). Díky masivnímu rozšíření tohoto standardu nebyly jiné standardy, jako je např. HiperLAN, komerčně realizovány. Standardy IEEE 802.11 byly snadněji implementovatelné a dostaly se tak rychleji na trh. Kompletní přehled tohoto standardu je realizován podrobněji v kapitole 4 tohoto modulu.

Označením IEEE 802.11 je tedy vymezena celá skupina standardů určených pro bezdrátové lokální sítě. Standard IEEE 802.11b byl prvním přijatým standardem této skupiny standardů, který podporuje datové přenosy rychlostmi až 11 Mbit/s v nelicencovaném pásmu 2,4 GHz. Následně byl jako nástupce standardu IEEE 802.11b přijat standard IEEE 802.11g, který pro přenosy využívá rozšířené kmitočtové pásmo. Přístupový bod založený na standardu IEEE 802.11g je schopen připojit do sítě klienty obou režimů, tj. 802.11b i 802.11g. Podobně je tomu i naopak, kdy klient se síťovou kartou dle standardu IEEE 802.11g může být připojen do sítě prostřednictvím přístupového bodu založeného „pouze“ na standardu 802.11b, avšak s rychlostním omezením daným použitým standardem. To vše je možné díky tomu, že bezdrátové sítě typu **LAN** založené na standardu 802.11g používají stejné nelicencované pásmo 2,4 GHz, jaké využívá standard 802.11b. Maximální přenosová rychlost u standardu IEEE 802.11g je 54 Mbit/s, která je však automaticky snižována v případě, pokud je detekován slabší rádiový signál nebo pokud je zjištěna interference s ostatními přenosovými kanály.

Obr 1.6 Diagram domácí sítě typu WLAN

2.3 Metropolitní bezdrátové sítě (WMAN)

Bezdrátové metropolitní sítě **WMAN** jsou třetí kategorií bezdrátových sítí. Sítě typu **WMAN** jsou založeny na standardu IEEE 802.16, který bývá často označován termínem **WiMAX** (*Worldwide Interoperability for Microwave Access*). Technologie **WiMAX** je komunikační technologií, která využívá architektury bod-mnoho bodů (*Point-to-Multipoint*) se zaměřením na vysokorychlostní bezdrátový přenos dat v metropolitních sítích [1-3]. Tato koncepce umožňuje, aby menší bezdrátové sítě typu **LAN** propojené pomocí technologie **WiMAX** vytvářely výše zmíněné metropolitní sítě typu **WMAN**. To znamená, že je možné vytvořit sofistikované meziměstské sítě bez nutnosti budování nákladné kabeláže a podpůrné pevné infrastruktury.

Technologie **WiMAX** je podobná technologii **Wi-Fi**, ale poskytuje pokrytí mnohem většího a rozsáhlejšího území. Technologie **Wi-Fi** je totiž koncepčně určena pro pokrytí pouze relativně malého území, například kanceláří nebo hot spotů, technologie **WiMAX** využívá dvou kmitočtových pásem, které jsou kombinací licencovaného a nelicencovaného pásma. První pásmo začíná na frekvenci 2 GHz a končí frekvencí 11 GHz a druhé pásmo je vymezeno od 10 GHz do 66 GHz. Kombinace dvou kmitočtových pásem umožňuje realizovat datové přenosy rychlostmi až 70 Mbit/s na vzdálenost až 50 km pro tisíce uživatelů připojených k jedné základnové stanice, jak je znázorněno na Obrázku 1.7. Jelikož technologie **WiMAX** využívá dvě zcela odlišná kmitočtová pásma, může být nasazena u systémů vyžadujících přímou viditelnost, stejně tak jako u systémů, které přímou viditelnost nevyžadují. Pásmo od 2 GHz do 11 GHz je možné využít pro systémy bez přímé viditelnosti, kdy základnová stanice „nevidí“ koncový terminál. Přenos na těchto kmitočtech totiž není příliš ovlivňován fyzickými překážkami. Naopak kmitočty v pásmu od 10 GHz do 66 GHz jsou užívány u systémů s přímou viditelností. Přímá viditelnost pak zajišťuje vzájemnou komunikaci mezi koncovým zařízením a základnovou stanicí na mnohem větší vzdálenost.

Obrázek 1.7 Síťový diagram technologie WiMAX

2.4 Páteřní bezdrátové sítě (WWAN)

Rozlehlé bezdrátové sítě **WWAN** dokáží překlenout vzdálenosti větší než 50 kilometrů a typicky užívají licencovaná kmitočtová pásma. Tento typ bezdrátových sítí pokrývá rozsáhlé oblasti, jakými jsou např. metropole nebo celé státy, a to pomocí vícenásobných satelitních systémů nebo anténními systémy provozovanými poskytovateli **ISP** (*Internet Service Provider*). Pro tyto účely jsou k dispozici dvě dostupné technologie – digitální buňkové systémy a satelitní systémy [1-3].

Buňkové telefonní sítě

Buňkový (celulární) systém rozděluje oblast pokrytí na menší elementární celky, které se označují pojmem buňka (*Cell*). Základnová stanice **BS** (*Base Station*) umístěná ve středu každé buňky je navržena tak, aby byla schopna pokrýt svými přenosovými prostředky celou vyhrazenou buňku. Každý zapnutý koncový terminál je připojen k některé ze základnových stanic v dosahu a základnové stanice jsou pak propojeny s telefonní ústřednou, která je schopna zpracovat provoz jak z mobilní tak i pevné telefonní sítě. Koncept buňkového uspořádání telefonní sítě je efektivní ve využívání dostupných přenosových prostředků s ohledem na nízkou energetickou náročnost přenosu a zároveň vytváří tzv. frekvenční plán, který umožňuje využívání omezeného počtu dostupných kmitočtů ve spojení s menší plochou jednotlivých buněk.

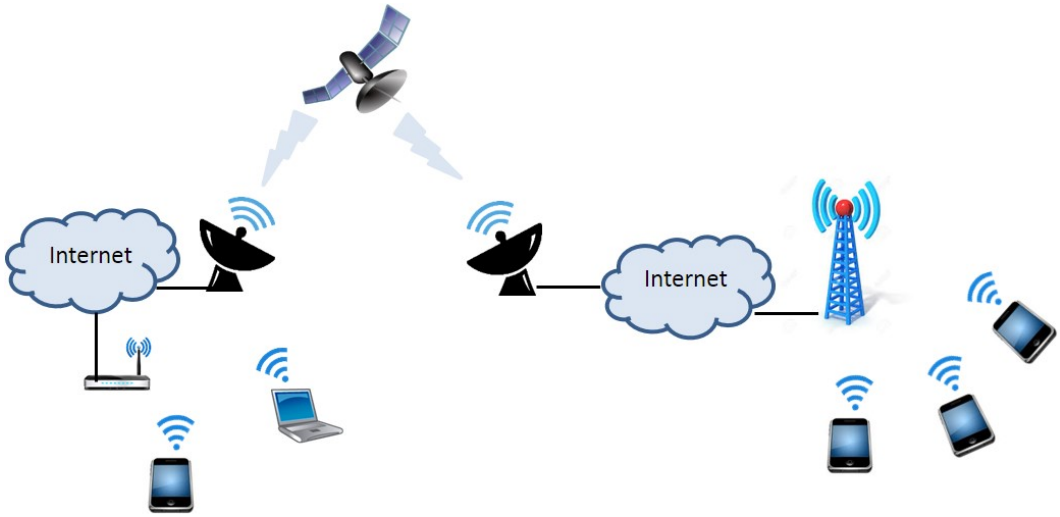
Od roku 1980 byly vyvíjeny různé typy buňkových systémů. První generace (1G) byla čistě analogová a byla vytvořena a navržena výhradně pro zajištění telefonní služby bez ohledu na požadavky služeb datových. Přenosová rychlost tohoto typu sítí byla pouhých 2,4 kbit/s. Druhá generace (2G) byla založena na plně digitální technologii a síťové infrastruktuře a bývá často označována zkratkou **GSM** (*Global System for Mobile Communications* nebo *Groupe Spécial Mobile*). Tato generace buňkových (celulárních) systémů umožňuje vedle telefonní služby i přenos krátkých textových zpráv **SMS** (*Short Message Service*) rychlostí až 64 kbit/s. Generace buňkových systémů označovaná zkratkou 2,5G je vývojovým mezistupněm mezi systémy druhé (2G) a třetí generace (3G). Někdy bývá tato generace označována jako 2G+**GPRS** (*General Packet Radio Service*), a jde v podstatě o vylepšenou původní síť typu 2G s dostupnou přenosovou rychlostí až 144 kbit/s. Třetí generace buňkových systémů (3G) byla představena v roce 2000 s rychlostí přenosu dat až 2 Mbit/s. Generace označená jako 3,5G je vylepšenou verzí sítí 3G, která využívá technik **HSDPA** (*High-Speed Downlink Packet Access*) a **HSUPA** (*High-Speed Uplink Packet Access*) k navýšení dostupné přenosové rychlosti (v sestupném směru až 14 Mbit/s (*downstream*), ve vzestupném směru až 5,76 Mbit/s (*upstream*)). Konečně aktuální čtvrtá generace buňkových systémů (4G) je schopna poskytnout rychlosti až 1 Gbit/s a jakýkoliv typ služby kdykoliv a kdekoliv dle požadavku uživatele. Pátá generace (5G) je očekávána v roce 2020.

Satelitní sítě

Bezdrátová komunikace může být zajišťována také pomocí sítě spolupracujících satelitů. Díky výhodné poloze satelitů, které jsou vysoko nad zemským povrchem,

mohou satelitní přenosy pokrýt rozsáhlá území. Tento typ pokrytí může být velmi užitečný pro uživatele, kteří se nacházejí buď v odlehlých oblastech, nebo na ostrovech, kde není dostupné klasické pevné připojení realizované pomocí podmořských kabelů. Pro tyto případy jsou satelitní telefony velkým přínosem.

Každý satelit je vybaven různými transpondéry skládajícími se z vysílače a antény. Vstupní signál je zesílen a následně přeposlán na odlišné frekvenci od původní, na které byl signál přijat.



Obrázek 1.8 Satelitní a buňkové sítě

3 Síťová architektura

3.1 Klíčové pojmy and terminologie

Tato kapitola obsahuje definice různých pojmů užívaných v architekturách bezdrátových sítí. Nicméně definice pojmů, které můžete nalézt ve všeobecných architekturách bezdrátových sítí a technologií, nelze vždy brát zcela doslovně, protože jejich výklad se ve spojení s konkrétní technologií může více či méně odlišovat od obecné definice daného pojmu.

Logická architektura dle IEEE 802.11 je složena z několika důležitých komponent – stanice **STA** (*Station*), bezdrátový přístupový bod **AP** (*Access Point*), nezávislý soubor základních služeb **IBSS** (*Independent Basic Service Set*), soubor základních služeb **BSS** (*Basic Service Set*), distribuční systém **DS** (*Distribution System*) a rozšířený soubor služeb **ESS** (*Extended Service Set*). Některé komponenty logické architektury dle IEEE 802.11 souvisejí přímo s konkrétními zařízeními, jako jsou např. stanice **STA** a bezdrátové přístupové body **AP**. Bezdrátová stanice **STA** obsahuje přístupovou kartu, PC kartu nebo jiné vestavěné zařízení zajišťující bezdrátové připojení. Bezdrátový přístupový bod **AP** funguje jako most (*Bridge*) mezi bezdrátovou stanicí **STA** a páteřní sítí a umožňuje tak přístup k dostupným síťovým prostředkům.

Stanicí **STA** může být klasický osobní počítač **PC** (*Personal Computer*), přenosný počítač (notebook,…), palmtop **PDA**, tablet, „chytrý“ telefon (*Smartphone*) nebo jakékoliv další jiné zařízení, které má schopnost využívat přístupu na bezdrátové médium.

Přístupový bod **AP**, někdy také označovaný jako základnová stanice **BS**, je zařízení, které poskytuje ostatním bezdrátovým zařízením připojení ke klasické kabelové síti pomocí různých přístupových technologií, např. **Wi-Fi** nebo dalších standardů využívaných v bezdrátových sítích.

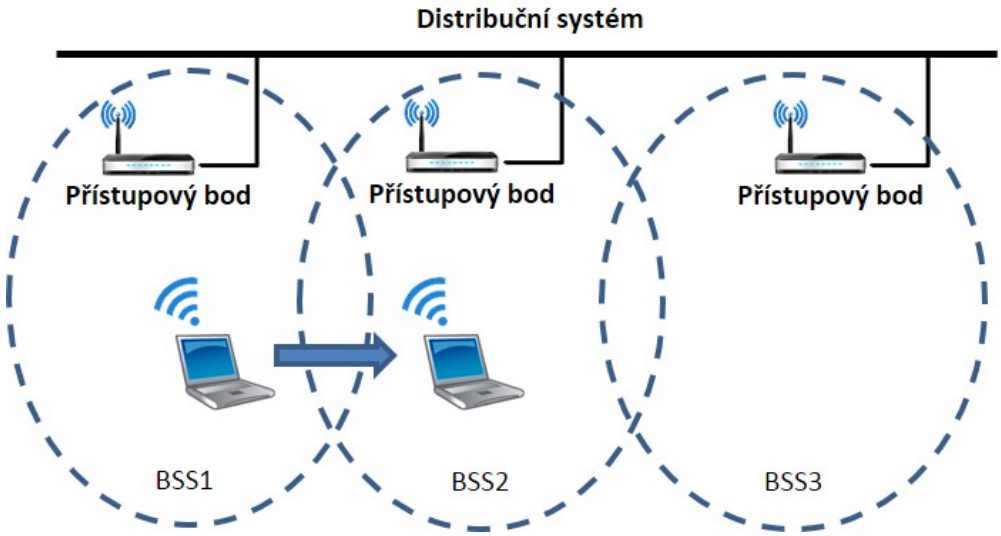
Soubor základních služeb **BSS** je tvořena přístupovým bodem **AP** spolu se všemi přidruženými stanicemi **STA**. Přístupový bod **AP** funguje v pozici *Master*, který řídí přidružené stanice **STA** v rámci souboru základních služeb **BSS**. Nejjednodušší soubor základních služeb **BSS** se skládá z jednoho přístupového bodu **AP** a jedné stanice **STA**.

Rozšířený soubor služeb **ESS** je sadou jednoho nebo více souborů základních služeb **BSS** navzájem propojených, které se z hlediska logického uspořádání a řízení na úrovni spojové vrstvy jeví jako jediný soubor základních služeb **BSS** pro každou stanici **STA** z libovolného souboru základních služeb **BSS** začleněného do rozšířeného souboru služeb **ESS**.

V případě pokud jsou všechny stanice **STA** začleněny do souboru základních služeb **BSS** a není dostupné připojení k pevné síti, pak je soubor základních služeb **BSS** označován jako nezávislý soubor základních služeb **IBSS**. Nezávislý soubor základních služeb **IBSS** tvoří v podstatě nestrukturovanou (*Ad hoc*) síť, tj. síť, která neobsahuje žádné přístupové body **AP**, což znamená, že není možné se připojit k jinému souboru základních služeb **BSS**.

Distribuční systém **DS** je ve své podstatě mechanismus, jakým si přístupové body **AP** vyměňují jednotlivé rámce mezi sebou a s pevnou sítí, pokud je připojena. Distribuční systém **DS** nemusí být svou podstatou sítí v pravém smyslu slova, nicméně standard IEEE 802.11 nepředepisuje konkrétní technologii, která má být pro distribuční systém **DS** využita. Téměř u všech komerčně dostupných produktů a řešení je však využíván kabelový Ethernet jako nosná technologie pro páteřní sítě.

Obrázek 1.9 Strukturovaný a nestrukturovaný soubor základních služeb BSS



Obrázek 1.10 Rozšířený soubor služeb ESS a podpora mobility

3.2 Architektury

V bezdrátových sítích jsou dostupné dva režimy používané pro účely konfigurace bezdrátových architektur, strukturovaný a nestrukturovaný (*Ad hoc*) [1-2]. U nestrukturovaného režimu (*Ad hoc*) si zařízení mezi sebou vyměňují data přímo, tzn. je využita rovnocenná síťová komunikace, zatímco ve strukturovaném režimu spolu zařízení komunikují prostřednictvím přístupového bodu **AP**, který zároveň slouží jako most (*Bridge*) do ostatních sítí.

Nestrukturovaný (Ad hoc) režim

Využitím nestrukturovaného (*Ad hoc*) režimu spolu mohou všechna zařízení v bezdrátové síti komunikovat přímo jako rovný s rovným na úrovni spojení bod-bod (*Point-to-Point*). Architektura sítě tedy nemá žádnou pevně definovanou strukturu, tj. nejsou definovány žádné pevné body infrastruktury, resp. není vyžadována integrace přístupových bodů **AP** pro vytvoření komunikace mezi jednotlivými začleněnými zařízeními.

Nestrukturovaný (*Ad hoc*) režim je velmi výhodný pro malé skupiny zařízení, podmínkou však je, že všechna zařízení musí být fyzicky přítomna a musí spolupracovat v těsné součinnosti. Výkon bezdrátové sítě v nestrukturovaném režimu se úměrně snižuje s rostoucím počtem zařízení začleněných do sítě. V tomto režimu se velmi často vyskytují nahodilá odpojení zařízení. Díky tomu tento režim klade vysoké nároky na správu sítě a kvalitu síťových administrátorů. Nestrukturovaný (*Ad hoc*) režim má i svá další omezení, mezi která patří nedostupnost přímého propojení s pevnými lokálními sítěmi, a také zde není k dispozici přímý přístup k Internetu, který je možné získat pouze instalací speciálních bran (*Gateways*).

Nicméně nestrukturovaný (Ad hoc) režim je s výhodou uplatnitelný na omezeném prostoru, kdy představuje nejjednodušší a nejlevnější alternativu, jak vybudovat plně funkční bezdrátovou síť.

Strukturovaný režim

Druhou dostupnou architekturou bezdrátových sítí je tzv. strukturovaný režim. Všechna zařízení jsou připojena k bezdrátové síti prostřednictvím přístupového bodu **AP**. Bezdrátové přístupové body **AP**, obvykle jde o směrovače (*Routers*) nebo přepínače (*Switches*), která konvertují rádiová data na Ethernetová data pevných sítí a pracují jako most (*Bridge*) mezi pevnými sítěmi **LAN** a bezdrátovými uživateli. Propojení vícenásobných přístupových bodů prostřednictvím pevných páteřních sítí založených na technologii Ethernet umožňuje rozšířit dosah pokrytí bezdrátových sítí. To znamená, že pokud se mobilní zařízení dostane z dosahu jednoho přístupového bodu **AP**, pak se s velkou mírou pravděpodobnosti dostane do dosahu jiného spolupracujícího přístupového bodu **AP**. Díky tomu se může bezdrátový klient volně pohybovat a přecházet od jednoho přístupového bodu dané domény k jinému v jiné doméně, a tím udržovat bezproblémové připojení k síti.

Strukturovaný režim poskytuje vyšší úroveň zabezpečení a stabilitu spojení, větší rozšiřitelnost ve spojení s jednoduchou správou. Nicméně u strukturovaného

režimu je však nutno počítat s dodatečnými vícenáklady vyplývajícími ze začlenění přístupových bodů **AP**, jakými jsou směrovače (*Routers*) a přepínače (*Switches*), do architektury bezdrátové sítě.

Identifikátor rozšířeného souboru služeb (ESSID)

Identifikátor rozšířeného souboru služeb **ESSID** (*Extended Service Set IDentification*) je jedním ze dvou identifikátorů souboru služeb **SSID** (*Service Set IDentification*). V případě nestrukturovaných Ad hoc bezdrátových sítí bez přístupových bodů **AP** je využíván tzv. identifikátor základního souboru služeb **BSSID** (*Basic Service Set IDentification*). U strukturovaných bezdrátových sítí, které využívají přístupových bodů **AP**, je využíván identifikátor rozšířeného souboru služeb **ESSID**, zjednodušeně však může být označen jen jako identifikátor souboru služeb **SSID**.

Identifikátor souboru služeb **SSID** je dvaatřicetiznakový (maximálně) alfanumerický klíč identifikující název, resp. označení bezdrátové lokální sítě.

Někteří obchodníci zaměňují identifikátor souboru služeb **SSID** za název bezdrátové sítě. Identifikátor souboru služeb **SSID** je však důležitý pro bezdrátová zařízení, která spolu v rámci jedné sítě komunikují, a musí jej tedy mít nastaven na stejnou hodnotu.

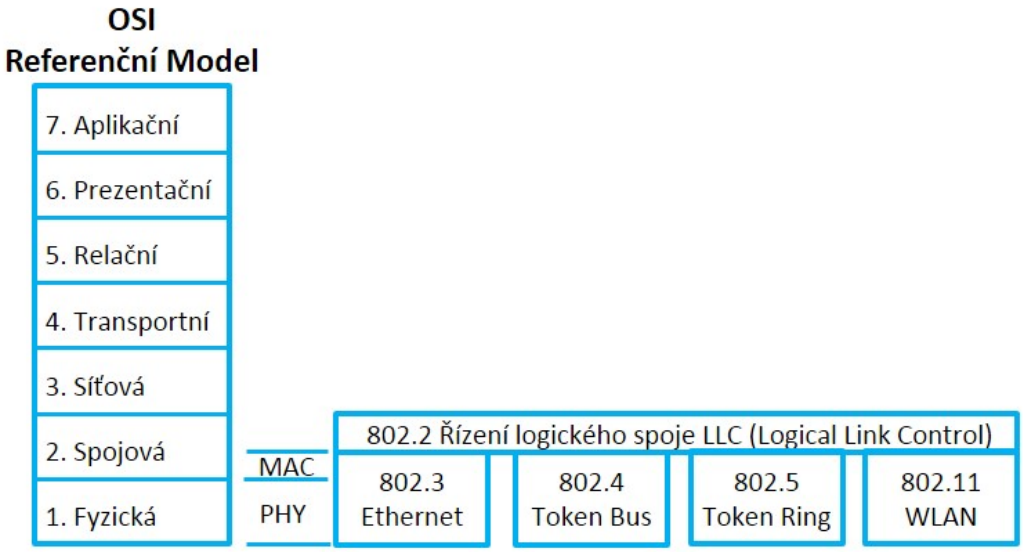
4 Standard IEEE 802.11

Standard IEEE 802.11 je souborem prostředků a norem umožňujících řízení přístupu k médiu **MAC** (*Medium Access Control*) a k fyzické vrstvě **PHY** (*Physical Layer*) a následně využívaných pro budování lokálních bezdrátových sítí ve frekvenčních pásmech 2,4, 5 a 60 GHz [1-2].

Tyto normy a předpisy jsou vytvářeny a spravovány pracovní skupinou IEEE 802.11. Základní verze standardu byla vydána v roce 1997, byla však následně doplněna o další dodatky a vylepšení. Standard IEEE 802.11 se svými dodatky a vylepšeními tak představuje základ pro vývoj komponent bezdrátových sítí označovaných obchodní značkou **Wi-Fi**.

4.1 Protokol 802.11

Výbor pro vývoj standardu IEEE 802.11 definoval v rámci standardu dvě oddělené vrstvy, řízení logického spoje **LLC** (*Logical Link Control*) a řízení přístupu k médiu **MAC**, které jsou součástí spojové vrstvy (*Data Link Layer*) referenčního modelu **RM-OSI** (*Reference Model of Open System Interconnection*). Bezdrátový standard IEEE 802.11 definuje soubor prostředků a norem umožňujících řízení přístupu k médiu **MAC** a k fyzické vrstvě **PHY**, které komunikují s vrstvou **LLC**, jak je znázorněno na Obrázku 1.11.



Obrázek 1.11 Standard IEEE 802.11 a referenční model RM-OSI

Všechny komponenty architektury dle IEEE 802.11 přináleží buď ke složkám řízení přístupu k médiu **MAC** (podvrstva spojové vrstvy) nebo k vrstvě fyzické **PHY**.

4.2 MAC rámec dle IEEE 802.11

Standardní IEEE 802.11 **MAC** rámec, zobrazený na Obrázku 1.12, se skládá ze záhlaví **MAC**, vlastního těla rámce a zabezpečovací sekvence **FCS** (*Frame Check Sequence*). Formát **MAC** rámce je složen z devíti polí, která se vyskytují v pevném pořadí a složení ve všech **MAC** rámcích.

Kontrolní pole rámce

Kontrolní pole rámce, zobrazené na Obrázku 1.12, obsahuje řídicí informace používané pro rozlišení typu **MAC** rámce (dle IEEE 802.11) a poskytuje tak důležité informace pro ostatní pole rámce, aby byly schopny zpracovat obsah daného **MAC** rámce.

Popis dílčích částí kontrolního pole rámce je uveden níže:

- Pole **Verze protokolu** poskytuje informaci o aktuálně používané verzi protokolu IEEE 802.11. Přijímací stanice **STA** používá tuto hodnotu pro identifikaci, zda je daná verze protokolu přijatého rámce stanicí podporována.

- Pole **Typ a podtyp** určuje funkci rámce. Existují tři různé typy rámce – řídicí, datový a dohlížecí. Pro každý typ rámce existuje několik vnořených podtypů. Každý podtyp určuje specifickou funkci, kterou vykonává pro jemu přidružený typ rámce.

- Pole **Směrem k DS a Směrem od DS** indikují, zda je rámec přenášen směrem od nebo do distribučního systému **DS** (*Distributed System*) a jsou používány pouze u datových rámců stanic **STA** propojených s přístupovým bodem **AP**.

- Pole **Více fragmentů (částí)** signalizuje, že přijatý rámec je rozdělen na více částí (fragmentů), a to buď datových, nebo dohlížecích, které budou zaslány následně po přijatém rámci s touto indikací.

- Pole **Opakovat** označuje, zda je možné data v rámci datového nebo dohlížecího rámce opětovně zaslat.

- Pole **Správa napájení** označuje, zda je vysílací stanice **STA** v aktivním nebo úsporném režimu.

- Pole **Další data** oznamuje stanici **STA** v úsporném režimu, že přístupový bod **AP** má k dispozici data určená k doručení. Toto pole tedy umožňuje přístupovému bodu **AP** signalizovat, že budou ve vysílání následovat další rámce typu *broadcast* nebo *multicast*.

- Pole **WEP** indikuje, zda je či není v rámci použito šifrování a autentizace. Tento příznak lze nastavit pro všechny datové a dohlížecí rámce, které mají nastaven příznak **Podtyp** oznamující autentizaci u přenášených rámců.

- Pole **Pořadí** označuje, že všechny přijaté datové rámce musí být zpracovány dle určeného pořadí.

Doba trvání/Identifikační pole

Toto pole se používá u všech řídicích rámců, s výjimkou úsporného rámce **PSP** (*Power Save Poll*), a to k indikaci zbývající doby trvání vyžadované pro příjem nebo vyslání dalšího přenášeného rámce. V případě úsporného rámce **PSP** pak toto pole obsahuje identifikaci přidružení **AID** (*Association IDentity*) k vysílací stanici **STA**.

Adresní pole

V závislosti na typu rámce může adresní pole obsahovat čtyři kombinace následujících typů adres:

- Identifikátor souboru základních služeb **BSSID** (*Basic Service Set Identifier*) jednoznačně označuje každý soubor **BSS**. Pokud pochází vysílaný rámec od stanice **STA** v infrastruktuře **BSS**, pak identifikátor **BSSID** je MAC adresa příslušného nadřazeného přístupového bodu **AP**. Pokud pochází rámec od stanice **STA** v infrastruktuře **IBSS**, pak je identifikátor **BSSID** generován náhodně, lokálně spravován **MAC** adresou stanice **STA**, která iniciovala vznik infrastruktury **IBSS**.

- Cílová adresa **DA** (*Destination Address*) specifikuje **MAC** adresu cílového místa určení rámce.

- Zdrojová adresa **SA** (*Source Address*) udává **MAC** adresu původního zdroje, který rámce vytvořil a odeslal.

- Adresa přijímače **RA** (*Receiver Address*) označuje **MAC** adresu nejbližší sousední stanice **STA** sdílející bezdrátové médiu, která je připravena přijmout odeslaný rámec.

- Adresa vysílače **TA** (*Transmitter Address*) indikuje **MAC** adresu stanice **STA**, která odeslala rámec ne bezdrátové médium.

Další podrobnější informace o typech adres a obsahu jednotlivých adresních polí obsažených v záhlaví **MAC** rámce standardu IEEE 802.11 najdete v dokumentaci standardu IEEE 802.11 na webových stránkách organizace IEEE [6].

Pole sekvenčního řízení

Pole sekvenčního řízení (*Sequence Control Field*) obsahuje dvě části, pole s číslem fragmentu přenášeného rámce a pole s označením sekvence přenášených rámců, jak je znázorněno na Obrázku 1.12.

Význam každého z výše uvedených polí pole sekvenčního řízení je následující:

- Číslo sekvence (*Sequence Number Field*) označuje pořadové číslo každého přenášeného rámce. Toto číslo je stejné u všech fragmentů rámce, který bylo nutné pro přenos rozdělit. Jinak je tento identifikátor inkrementován vždy o jedničku, dokud nedosáhne hodnoty 4095, následně je vynulován a může být opětovně inkrementován.

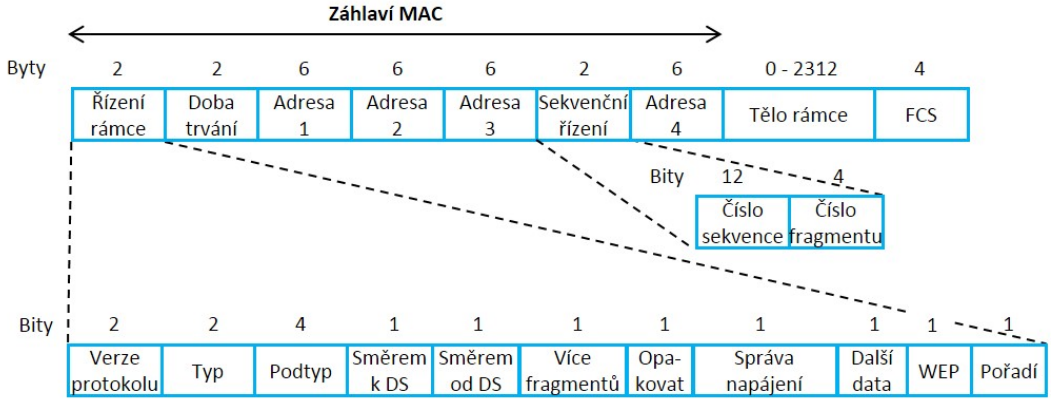
- Číslo fragmentu (*Fragment Number Field*) udává počet fragmentů, na který byl původní přenášený rámec rozdělen. Počáteční hodnota je nastavena na hodnotu 0 a poté je inkrementována vždy o jedničku u každé následující části přenášeného rámce.

Tělo rámce

Tělo rámce přenáší údaje nebo informace vyšších vrstev komunikace začleněné buď do řídících, nebo do datových rámců.

Zabezpečovací sekvence FCS

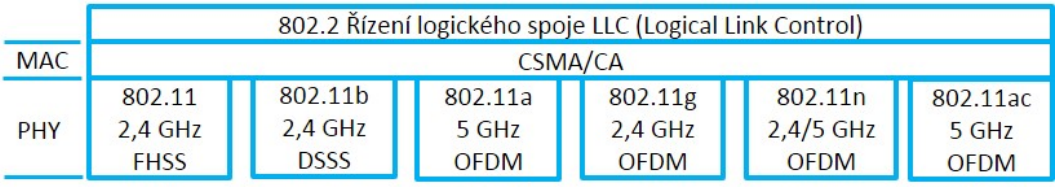
Vysílací stanice **STA** používá zabezpečení na bázi cyklického kódu **CRC** (*Cyclic Redundancy Check*) pro všechna pole záhlaví **MAC** rámce a tělo rámce prostřednictvím hodnoty zabezpečovací sekvence **FCS**. Přijímací stanice **STA** pak využívá stejný princip výpočtu **CRC** k získání zabezpečovací sekvence **FCS** tak, aby bylo možné ověřit, zda došlo během přenosu rámce k jeho narušení, tj. zda došlo během přenosu ke vzniku chyby.



Obrázek 1.12 Formát MAC rámce dle standardu IEEE 802.11. Řídicí pole a pole sekvenčního řízení rámce jsou zobrazeny detailně.

4.3 Fyzická vrstva dle standardu 802.11

Standard IEEE 802.11 definuje na fyzické vrstvě **PHY** několik kódovacích přepisů a přenosových metod vhodných pro bezdrátovou komunikaci. Mezi jedny z nejpoužívanějších metod oprávněně patří technika kmitočtového přeskakování nosné vlny **FHSS** (*Frequency Hopping Spread Spectrum*), technika přímého rozprostřeného spektra **DSSS** (*Direct Sequence Spread Spectrum*) a ortogonální multiplex s frekvenčním dělením **OFDM** (*Orthogonal Frequency Division Multiplexing*). Obrázek 1.13 zobrazuje standardy IEEE 802.11, IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11n a IEEE 802.11ac, které jsou v současné době využívány na fyzické vrstvě **PHY**. Tyto standardy budou ve zkratce popsány v následujících kapitolách.



Obrázek 1.13 Standardy IEEE 802.11 používané na fyzické vrstvě

Standard IEEE 802.11

Přenosová rychlost prvotního standardu IEEE 802.11 je 2 Mbit/s, kdy je využívána metoda přenosu **FHSS** a frekvenční pásmo **ISM**, které pokrývá pásmo kmitočtů od 2,4 do 2,5 GHz. Nicméně reálně dostupná přenosová rychlost je pouze okolo 1 Mbit/s (poloviční než původní teoretická hodnota, která je uváděna pro případ přenosu realizovaného za ideálních podmínek).

Standard IEEE 802.11b

Hlavním vylepšením standardu IEEE 802.11 ve verzi IEEE 802.11b jsou začlenění nových specifikací fyzické vrstvy **PHY** podporujících vyšší přenosové rychlosti. Standard IEEE 802.11b podporuje další dvě přenosové rychlosti, a to 5,5 Mbit/s a 11 Mbit/s, které využívají kmitočtové pásmo 2,4 GHz. Pro účely navýšení přenosových rychlostí byla zavedena nová metoda přenosu, tj. technika přímého rozprostřeného spektra **DSSS**. Přenosové rychlosti 11 Mbit/s je možné dosáhnout pouze za ideálních podmínek. V případě zhoršených podmínek jsou využívány nižší přenosové rychlosti 5,5 Mbit/s, 2 Mbit/s a 1 Mbit/s.

Možná je vhodné na tomto místě pro zajímavost připomenout, že standard IEEE 802.11b využívá identické frekvenční pásmo, jaké využívají i další spotřebiče např. mikrovlnné trouby, bezšňůrové telefony (*Cordless Telephone*), dětské chůvičky, bezdrátové videokamery a zařízení Bluetooth.

Standard IEEE 802.11a

Standard IEEE 802.11a může pracovat s přenosovými rychlostmi až 54 Mbit/s a pro svůj provoz využívá frekvenční pásmo 5 GHz. Namísto techniky **DSSS** využívá ortogonální multiplex s frekvenčním dělením **OFDM**, který ve svém principu umožňuje paralelní přenos dat v rámci přidělených subkanálů a poskytuje tak větší odolnost proti rušení a zároveň vyšší propustnost. Vyšší dostupná přenosová rychlost poskytuje bezdrátovým sítím **LAN** lepší výkon pro zajištění videokonferenčních hovorů a multimediálních aplikací.

Díky pracovní frekvenci odlišné od jiných bezdrátových zařízení (např. bezšňůrové telefony - frekvence 2,4 GHz), poskytuje standard IEEE 802.11a díky metodě přenosu na bázi **OFDM** vyšší přenosovou rychlost a čistější signál. Přenosové rychlosti 54 Mbit/s je však možné dosáhnout pouze za ideálních podmínek. V případě zhoršených podmínek jsou využívány nižší přenosové rychlosti 48 Mbit/s, 36 Mbit/s, 24 Mbit/s, 18 Mbit/s, 12 Mbit/s a 6 Mbit/s.

Standard IEEE 802.11g

Standard IEEE 802.11g může pracovat s přenosovými rychlostmi až 54 Mbit/s, využívá původní frekvenční pásmo 2,4 GHz, ale novou metodu přenosu na bázi **OFDM**. Standard IEEE 802.11g je zpětně kompatibilní se standardem IEEE 802.11b, to znamená, že může využívat přenosové rychlosti jako standard IEEE 802.11b a metodu přenosu typu **DSSS**. Bezdrátové síťové karty standardu IEEE 802.11g je možné bez potíží propojit s bezdrátovými přístupovými body **AP** standardu IEEE 802.11b a bezdrátové síťové karty standardu IEEE 802.11b je možné bez problémů propojit s bezdrátovými přístupovými body **AP** standardu IEEE 802.11g.

Standard IEEE 802.11g tedy umožňuje migraci sítě založené na standardu IEEE 802.11b na kmitočtově kompatibilní technologii avšak s podporou vyšší přenosové rychlosti.

Stávající bezdrátové síťové karty pracující dle standardu IEEE 802.11b nelze upgradovat na standard IEEE 802.11g pouhou aktualizací firmwaru karty, ale je bohužel nutná jejich výměna. Avšak porovnáme-li migraci ze standardu IEEE 802.11b na standard IEEE 802.11a u níž je nutné vyměnit všechny bezdrátové síťové karty obou bezdrátových klientů a všechny bezdrátové přístupové body **AP** současně, migraci ze standardu IEEE 802.11b na standard IEEE 802.11g lze provést postupně třeba s ohledem na dostupné finanční prostředky.

Stejně jako standard IEEE 802.11a i standard IEEE 802.11g dosahuje přenosové rychlosti 54 Mbit/s pouze za ideálních podmínek. V případě zhoršených podmínek jsou využívány nižší přenosové rychlosti 48 Mbit/s, 36 Mbit/s, 24 Mbit/s, 18 Mbit/s, 12 Mbit/s a 6 Mbit/s.

Standard IEEE 802.11n

Standard IEEE 802.11n vylepšil především dosah (až 250 m) a výrazně vzrostla i propustnost sítě v porovnání s předchozími standardy IEEE 802.11a a IEEE 802.11g (z 54 Mbit/s až na 600 Mbit/s za ideálních podmínek). Tato vylepšení jsou možná díky integraci techniky **MIMO** (*Multiple Input Multiple Output*) a rozšířením přenosového kanálu na 40 MHz v rámci využívaného kmitočtového pásma. Technika **MIMO** umožňuje zpracování většího množství rádiových signálů díky integraci více antén do vysílače i přijímače. Může využívat frekvenční pásma 2,4 GHz nebo 5 GHz.

Standard IEEE 802.11ac

Standard IEEE 802.11ac je vylepšením standardu IEEE 802.11n, poskytuje podobný dosah, ale výrazně zvyšuje propustnost. Pracuje na frekvenci 5 GHz, využívá techniky tvarování vyzařovacího diagramu (*Beamforming*) a širšího frekvenčního pásma s vícenásobnými anténami k dosažení teoretické přenosové rychlosti až 1,3 Gbit/s, což je více než dvojnásobek přenosové rychlosti, kterou je možné dosáhnout u standardu IEEE 802.11n (teoreticky až 600 Mbit/s).

5 Bezpečnost

Bezdrátové sítě obecně nejsou tak bezpečné jako pevné (kabelové) sítě. Pevné sítě na své nejnižší úrovni přenášejí data mezi dvěma body A a B, které jsou fyzicky propojeny síťovým kabelem. Naopak bezdrátové sítě vysílají svá data všemi směry a ke všem zařízením, která mohou toto vysílání zachytit. Omezení je zde pouze v dostupném dosahu. Pevné sítě mohou být účinně zabezpečeny již na svých vstupních rozhraních, například omezením fyzického přístupu k síťovým zařízením a instalací firewallů. Bezdrátová síť je i přes zavedení stejných opatření jako v případě pevné sítě stále náchylná k nelegálnímu odposlechu. Proto bezdrátové sítě vyžadují mnohem propracovanější a důmyslnější přístup k zajištění bezpečnosti svého provozu.

5.1 Bezpečná komunikace

Pojem bezpečná komunikace je velmi často spojován s následujícími třemi procesy: identifikace (*Authentication*), zabezpečení (*Confidentiality*) a celistvost (*Integrity*) [1].

Proces identifikace (*Authentication*) ověřuje identitu jednotlivých uzlů a prvků sítě.

Proces identifikace je obvykle založen na ověření přístupových údajů pověřenou autoritou. Přístupovými údaji může být například dvojice ve formátu uživatelské jméno a heslo. U složitějších (komplexnějších) systémů může být proces identifikace založen na prokázání vlastnictví určitého klíče či charakteristického znaku či prvku, který je obtížné odcizit nebo zfalšovat. K těmto prostředkům patří například certifikáty nebo čipové karty.

Proces zabezpečení(*Confidentiality*) omezuje (znemožňuje) možnost odposlechu síťového provozu.

Procesem zabezpečení je typicky zabezpečení obsahu zprávy pomocí šifrování. Proces šifrování aplikuje známou oboustrannou metodu transformace (nazývanou též šifra nebo šifrovací algoritmus) na původní (originální) obsah zprávy (označovaný též pojmem prostý (nešifrovaný) text (*Plain Text*) a touto transformací je z něj vytvořen šifrovaný text. Obnovit původní obsah zprávy (tj. dešifrovat zprávu) mohou pouze ti, kteří znají metodiku zvolené transformace. Mezi nejběžněji používané metody šifrování jsou matematické transformace, které používají jako vstupní proměnnou klíč, který je nedílnou součástí transformačního procesu. Cílový příjemce musí být informován o typu použité metody a hodnotě klíče tak, aby byl schopen správně dešifrovat obsah přijaté zprávy. Standardní šifrovací metody a jejich principy jsou veřejně známé. Ochrana a utajení použitého klíče je tak pro kvalitu procesu zabezpečení zcela zásadní.

Proces celistvost (*Integrity*) zajišťuje, že přenášené zprávy jsou doručovány bez dodatečných změn.

V souvislosti s procesem zabezpečení komunikace je tedy nutné doplnit schopnost systému, která umožňuje ověřit, že přijatá zpráva nebyla žádným způsobem pozměněna a je tedy shodná (identická) se zprávou, která byla odeslána. Byty zabezpečovací sekvence **FCS** jsou jednou z metod zajišťujících integritu dat, bohužel však nejsou těmi nejbezpečnějšími. Obvykle totiž nejsou byty **FCS** odvozeny z vlastního obsahu přenášené zprávy a samy o sobě nejsou chráněny dodatečným šifrováním. Častěji jsou odvozeny z již zašifrovaného obsahu zprávy, navíc některou z veřejně známých metod, a odesílány jsou v přímé, tj. nezašifrované podobě. Byty **FCS** napomáhají identifikaci jednotlivých paketů, které byly poškozeny při přenosu omylem, nikoliv úmyslně. Útočník (*Hacker*) totiž může velmi snadno dopočítat správnou hodnotu bytů **FCS** pro zamaskování úmyslné změny informačního obsahu paketů, které přijal a následně přeposlal. Mnohem složitější je pro útočníka správně dopočítat kontrolu integrity přenášené

sekvence nebo bezpečnostní „hash“ funkci, čím spolehlivějším a propracovanějším je test integrity.

Koncepce procesu celistvosti (resp. integrity) bývá často doplněna o ověřovací nástroje, které umožňují rozpoznat zdroj zprávy a následně jej porovnat s údaji o zdroji zprávy uvedenými ve zprávě doručené. Časové značky (*Timestamps*) a index pořadí jednotlivých zpráv mohou účinně chránit před opakovanými útoky, ale opět nejsou považovány za nejbezpečnější, pokud nejsou chráněny dodatečným šifrováním.

Pojem bezpečnost je vždy pojmem relativním, nikdy absolutním. Každý typ resp. druh ochrany bude jednou zcela jistě překonán úspěšným útokem. Každý typ, resp. druh útoku vyvolá jako svůj následek vývoj účinné ochrany. Absolutními veličinami nutnými pro úspěšný útok tak zůstávají pouze dvě veličiny – míra vynaloženého úsilí a čas. Čím je totiž ochrana dokonalejší, tím více času a větší míry úsilí je třeba vynaložit pro její narušení.

Dostatečný typ ochrany je takový, který je vyvážený, a který odpovídá očekávané skupině možných útoků. Vyváženost je důležité vnímat ve dvou odlišných úhlech pohledu. Za prvé, nejslabší článek přenosového řetězce musí být dostatečně bezpečný. Za druhé, pasivní prvky použité pro potřeby identifikace, šifrování a kontroly integrity musí být vhodně a úměrně doplněny prvky aktivními, jakými jsou např. monitorování síťového provozu a sledování pokusů o jeho narušení, důsledné dodržování bezpečnostních pravidel (nesdělovat nikomu svá hesla, nepoužívat jednoduchá hesla, apod.) a řada dalších. Dostatečnou ochranou je tedy takový typ ochrany, který pro své překonání vyžaduje jen o trochu více času a úsilí, než které jsou útočníci ochotni vynaložit. Náklady na vytvoření bezpečnostních opatření lze vyčíslit formou finančních nákladů a jistou mírou omezení obránce, který daný systém využívá. Jako jakákoliv jiná obchodní rozhodnutí, musí být i tyto kompromisy související s bezpečností komunikace, realizována po zralé úvaze a se zohledněním míry všech možných aspektů.

5.2 Zabezpečení a šifrování

Ochrany, která účinně zabraňuje neoprávněnému a neautorizovanému přístupu k obsahu zprávy, je dosaženo zabezpečením dat pomocí šifrování. Šifrování je volitelným doplňkem sítí **WLAN**, ale bez jeho využití může jakékoliv kompatibilní zařízení v dosahu sítě **WLAN** a podporující její přenosový standard odposlouchávat veškerý síťový provoz.

Existují a jsou využívány tři základní typy zabezpečení pro sítě **WLAN**. Od roku 1990 prošly bezpečnostní algoritmy **Wi-Fi** sítí několika zásadními upgrady a vylepšeními. Některé původní bezpečnostní algoritmy byly zcela odstraněny, a ty které zůstaly zachovány, jsou dnes výkonnější a z hlediska zabezpečení mnohem efektivnější. V chronologickém pořadí jde o tyto algoritmy:

- metoda **WEP** (*Wired Equivalent Privacy*)
- metoda **WPA** (*Wi-Fi Protected Access*)
- metoda **WPA2** (*Wi-Fi Protected Access version 2*)

Metoda WEP

Metoda **WEP** byla schválena jako bezpečnostní standard **Wi-Fi** sítí v září roku 1999. První verze metody **WEP** nebyla nikterak robustní, a to ani v době, kdy byla publikována. Existovala zde totiž jistá omezení za strany **USA** (*United States of America*), která zakazovala výrobcům **Wi-Fi** zařízení vývoz některých vybraných kryptografických technologií. Důsledkem toho bylo omezování bezpečnostních funkcionalit těchto zařízení na úroveň šifrování v řádu 64 bitů. Po zrušení těchto omezení byla tato úroveň navýšena na 128 bitů. I přesto, že je již dnes zavedeno šifrování dle metody **WEP** na úrovni 256 bitů, úroveň šifrování 128 bitů zůstává stále jednou z nejužívanějších implementací této bezpečnostní metody.

Navzdory dalším vylepšením metody **WEP** a prodloužením délky používaného klíče, byly v průběhu času objeveny ve standardu **WEP** četné bezpečnostní chyby. Díky nárůstu výpočetního výkonu se poté staly i jednodušeji zneužitelné. Již v roce 2001 byl zpochybněn základní koncept metody **WEP** a v roce 2005 úřad **FBI** (*Federal Bureau of Investigation*) uspořádal veřejnou ukázku, ve snaze zvýšit povědomí veřejnosti o slabinách metody **WEP**, kde bylo demonstrováno prolomení **WEP** hesel během několika málo minut, a to pomocí zcela volně dostupného softwaru.

I přes různá vylepšení a další pokusy o podporu a modernizaci metody **WEP**, jsou systémy využívající tuto metodu stále velmi zranitelné. Systémy, které se spoléhají na metodu **WEP**, by měly být co nejdříve aktualizovány nebo v případě, kdy tato aktualizace není možná, pak by tato zařízení měla být zcela vyměněna. Aliance **Wi-Fi** opustila oficiálně metodu **WEP** v roce 2004.

Metoda WPA

Řešením problému se zranitelností systémů využívajících metodu **WEP**, byl na začátku roku 2003 vznik skupiny **WPA** v rámci aliance **Wi-Fi**. Nejběžnější konfigurací **WPA** je metoda **WPA-PSK** (*Wi-Fi Protected Access Pre-Shared Key*). Délka klíče používaného metodou **WPA** je 256 bitů, což značí výrazný nárůst délky klíče v porovnání s délkou 64 bitů a 128 bitů u metody **WEP**.

Několika významnými změnami zavedenými u metody **WPA** jsou kontrola integrity zprávy (umožňuje identifikaci, zda útočník zachytil a pozměnil obsah paketů přenášených mezi přístupovým bodem **AP** a klientem) a protokol **TKIP** (*Temporal Key Integrity Protocol*). Protokol **TKIP** používá systémový klíč pro každý přenášený paket, který je mnohem bezpečnější než pevný klíč užívaný u metody **WEP**. Protokol **TKIP** byl později nahrazen standardem **AES** (*Advanced Encryption Standard*).

Navzdory významnému vylepšení zabezpečení komunikace metodou **WPA** v porovnání s metodou **WEP**, metoda **WEP** stále konkuruje metodě **WPA**. Protokol **TKIP**, základní komponenta metody **WPA**, byl navržen tak, aby bylo možné jej jednoduše začlenit prostřednictvím aktualizace firmwaru u stávajících **WEP** zařízení. Měl tedy umožnit využití některých starších zařízení používajících metodu **WEP**, což se v konečném důsledku povedlo.

Základní koncept metody **WPA** byl, stejně jako u její předchůdkyně metody **WEP**, zpochybněn veřejnou ukázkou, ve které byla úspěšně narušena její integrita útočníkem. Zajímavé je, že proces, při kterém je integrita metody **WPA** narušena, není přímým útokem na algoritmus **WPA** (i když i tyto útoky byly úspěšně testovány), ale vektorovým útokem na podpůrný systém **WPS** (*Wi-Fi Protected Setup*), který spolupracuje s metodou **WPA** a který byl navržen tak, aby bylo snadné připojit koncová zařízení k moderním přístupovým bodům **AP**.

Metoda WPA2

Metoda **WPA** byla od roku 2006 oficiálně nahrazena metodou **WPA2**. Jednou z nejvýznamnějších změn oproti metodě **WPA** je zavedení povinného použití algoritmu **AES** a protokolu **CCMP** (*Counter Cipher Mode with Block Chaining Message Authentication Code Protocol*) jako náhrady za protokol **TKIP** (zachován jako záložní systém pro metodu**WPA2** a případnou součinnost se systémy pracujícími výhradně s metodou **WPA**).

V současné době se bezpečnostní rizika aktuálně používané metody**WPA2** jeví jen jako velmi malá (útočník totiž musí mít ještě před vlastním útokem přístup k zabezpečené **Wi-Fi** síti, aby tak mohl získat přístup k bezpečnostním klíčům a mohl následně uskutečnit útok na ostatní zařízení v síti). Díky tomu je dopad takových útoků ve spojitosti s metodou **WPA2** omezen téměř výhradně na úroveň podnikových sítí a není třeba realizovat žádná protiopatření, pokud jde o zabezpečení malých domácích sítí.

Bohužel i u metody **WPA2** zůstalo zachováno riziko vektorového útoku spojeného s podpůrným systémem **WPS** na úrovni přístupových bodů **AP**. Ačkoliv vniknutí do sítí zabezpečených metodami **WPA/WPA2** prostřednictvím zranitelnosti

systému **WPS** vyžaduje časově dlouhý (2 až 14 hodin) a náročný útok realizovaný moderními počítači, jedná se stále o legitimní bezpečnostní riziko a systém **WPS** by měl být pro jistotu zakázán (pokud je to možné, firmware přístupového bodu by měl být pozměněn na verzi, která vůbec systém **WPS** nepodporuje, a tím lze s jistotou zajistit úplné odstranění tohoto typu rizika).

Níže je uveden základní přehled v současné době používaných metod zabezpečení **Wi-Fi** sítí a jejich možných kombinací s bezpečnostními algoritmy (řazení je od nejlepšího k nejhoršímu):

1. **WPA2** + **AES**
2. **WPA** + **AES**
3. **WPA** + **TKIP**/**AES** (**TKIP** je zde jako záložní metoda)
4. **WPA** + **TKIP**
5. **WEP**
6. Otevřená síť (bez zabezpečení)

V ideálním případě bude systém **WPS** zakázán a úroveň zabezpečení sítě bude přednastavena na kombinaci **WPA2** + **AES**. Ostatní kombinace bezpečnostních algoritmů z předchozího seznamu jsou nepoužitelné.

6 Výhody a nevýhody

Bezdrátové sítě mají řadu zásadních výhod v porovnání se sítěmi pevnými. Mezi tyto výhody patří především mobilita, hospodárnost výdajů a adaptabilita. Mají ale také některé nevýhody, k těm nejdůležitějším patří bezpečnost. Níže je uveden přehled hlavních výhod a nevýhod bezdrátových sítí v porovnání se sítěmi pevnými.

Následující seznam shrnuje některé z hlavních výhod bezdrátových sítí:

Vyšší efektivita

Vylepšení datové komunikace umožňuje zvýšit dostupnou rychlost přenosu informací v sítích provozovatelů a také přímo mezi uživateli. Například, díky tomu mohou obchodníci na dálku kontrolovat stav zásob a upravovat ceny, zatímco vyřizují obchodní telefonáty.

Lepší pokrytí a mobilita

Instalace pevných sítí nás omezují v pohybu a fixují naši pozici na konkrétní přístupové místo. Přechodem k bezdrátovým sítím získáte svobodu pohybu bez ztráty připojení, bez nutnosti budování podpůrné kabeláže nebo konfigurace adaptérů nutných pro přístup k síťovým prostředkům.

Flexibilita

Administrativní pracovníci připojení k bezdrátovým sítím mohou pracovat, aniž by seděli v kanceláři u stolních počítačů, a mohou být ve své práci i nadále velmi produktivní, i přesto že se nacházejí mimo kancelář. Tato výhoda přináší nový styl práce do mnoha oborů lidské činnosti. Například je možné pracovat z domova nebo máme možnost přístupu k firemním datům během návštěvy u zákazníka (klienta).

Úspora nákladů (Hospodárnost výdajů)

Bezdrátové sítě jsou snadněji konfigurovatelné a budování jejich infrastruktury je levnější, a to zejména v památkově chráněných objektech nebo všude tam, kde pronajímatel nepovolil instalaci potřebné kabeláže. Absence vodičů a kabelů výrazně snižuje celkové náklady. Této skutečnosti je dosaženo i kombinací několika jiných faktorů, např. nízkými náklady na pořízení bezdrátových směrovačů, není třeba realizovat instalaci přívodních kabelů do zdiva nebo jiné typy instalací nutných pro vytvoření fyzického připojení. Kromě toho není vyžadována údržba této infrastruktury.

Adaptabilita

Rychlá a snadná integrace nových zařízení do již fungující bezdrátové infrastruktury spojená s vysokou flexibilitou změny konfigurace a nastavení bezdrátové sítě.

Nové příležitosti/aplikace

Bezdrátové sítě nabízejí nové produkty a služby. Například na mnoha letištích v odletových halách, na nádražích, v hotelech, kavárnách a restauracích jsou umístěny přístupové body **AP** k bezdrátovým službám tzv. *Hotspoty*, které umožňují klientům připojit jejich mobilní zařízení do síťové infrastruktury a využívat dostupné služby a aplikace bezdrátových sítí i během cestování.

Existují však i některé nevýhody spojené s použitím bezdrátových sítí. Zde je přehledově uvedeno několik z nich:

Úroveň zabezpečení

Bezdrátový přenos je mnohem více náchylný na útok ze strany neoprávněných uživatelů (*Hackerů*), takže této problematice musí být věnována mimořádná pozornost.

Problémy s instalací a vlastním provozem

Provoz bezdrátových zařízení může být silně ovlivněn interferencí (rušením) nebo provozem jiných zařízení, které jsou v jeho blízkém dosahu (např. ve stejné místnosti nebo budově) a využívají stejnou bezdrátovou technologii nebo pokud jsou v blízkosti silné zdroje rádiových signálů. Všechny tyto faktory mohou vést ke zhoršení kvality komunikace nebo v extrémním případě až ke ztrátě bezdrátové konektivity.

Kvalita pokrytí

V některých budovách je velmi obtížné, někdy i zcela nemožné, udržet odpovídající (konzistentní) míru pokrytí mobilním signálem, což vede ke vzniku oblastí bez pokrytí, tj. bez dostupného signálu. Například v betonových budovách využívajících ocelové výztuhy velmi brzy zjistíte, že je místy velmi obtížné získat kvalitní mobilní signál.

Dostupná přenosová rychlost

Bezdrátový přenos může být pomalejší a méně efektivní v porovnání s rychlostmi pevných sítí. U rozsáhlých bezdrátových sítí pak bude jejich páteřní část obvykle realizována pevnou infrastrukturou než infrastrukturou bezdrátovou.

7 Aplikace a další možnosti využití

Dosah bezdrátových komunikačních systémů u vestavěných zařízení stále roste. Společnost Forrester Research, která se zaměřuje na zkoumání vlivu technologických změn na ekonomiku, uvedla, že během několika málo let bude až 95 % všech zařízení využívat přístup k Internetu a budou to většinou nepočítačová zařízení využívající vlastní vestavěný operační systém.

Existuje mnoho aplikací pro vestavná zařízení s **Wi-Fi** rozhraním:

- Průmyslové procesy a řízení aplikací, u kterých je pevné připojení příliš nákladné nebo nevhodné, např. v případě častého stěhování strojů z místa na místo.
- Záchranné (pohotovostní) aplikace vyžadující okamžité a dočasné (časové omezené) nastavení, jako jsou např. bojiště nebo oblasti přírodních katastrof.
- Mobilní aplikace využívané např. pro ostrahu budov nebo hlídání majetku.
- Dohledové kamery (určitě byste si nepřáli, aby si jich kdokoliv snadno všiml, kabely však skryjete jen obtížně).
- Oblast specifických služeb (*Vertical Markets*) jakými jsou lékařství, vzdělávání a průmyslová výroba.
- Komunikace s ostatními Wi-Fi zařízeními, jakými jsou např. přenosná zařízení (notebooky, tablety nebo palmtopy **PDA**).
- Komunikace mezi stroji (**M2M** (*Machine to Machine*) aplikace).

V souvislosti s posledním bodem předchozího výčtu (M2M aplikace) je nutné uvést, že se vztahuje k technologiím, které umožňují mobilním i pevným komunikačním systémům výměnu informací mezi zařízeními stejného typu. [http://en.wikipedia.org/wiki/Machine_to_machine] Jinou charakteristikou M2M komunikace je, že toto propojení umožňuje především automatizovanou komunikaci mezi vzdálenými stroji a jednou nebo více vrstvami centrálně řízených aplikací, např. zajištění monitorování v reálném čase a řízení bez nutnosti lidského zásahu.

V bezdrátovém **M2M** prostoru existují dvě hlavní třídy propojení – krátkého dosahu a dlouhého dosahu. Převládající je technologie dlouhého dosahu, která využívá vestavěných mobilních modulů pro připojení vzdálených zařízení k Internetu nebo aplikačním serverům. Mobilní modul zajišťuje řadu obdobných funkcí, jaké můžeme nalézt u mobilního telefonu, včetně hlasové a datové komunikace, a je tedy ideálním prostředkem pro vestavěné aplikace.

M2M aplikace lze nalézt v celé řadě průmyslových odvětví, mezi něž patří např. automatický sběr dat **AMR** (*Automatic Meter Reading*), prodejní automaty, terminály na pokladních přepážkách **POS** (*Point Of Sales terminals*), dopravní a logistické systémy (např. řízení vozového parku (*Fleet Management*), zdravotnické a bezpečnostní systémy a celá řada dalších aplikací.

Dle ABI Research, firmy provádějící technologický výzkum a poradenskou činnost, bude do roku 2020 více než 30 miliard zařízení bezdrátově připojeno do infrastruktury nazývané Internet věcí (*Internet of Things*).

8 Závěr

Bezdrátové síťové technologie dnes propojují technologicky vyspělá zařízení buď přímo mezi sebou, nebo v rámci vysokorychlostních sítí (bez požadavků na budování pevných instalací). V minulosti bylo totiž nutné budovat finančně i časově nákladnou a prostorovým uspořádáním rozsáhlou pevnou infrastrukturu. Všechny tyto nedostatky jsou v případě bezdrátových sítí značně omezeny.

V současné době lze říci, že budování a konfigurace bezdrátových sítí je velmi jednoduchá, síťové prvky jsou snadno dostupné a je možné vybírat z mnoha různých typů a provedení. Navíc jsou dostupné rozsáhlé, podrobné a přehledně zpracované informační zdroje, které vám v případě potřeby pomohou s řešením vzniklého problému.

Dnes je možný i výběr vhodné technologie tak, aby co nejlépe odpovídala požadavkům a potřebám dané aplikace. Dosah datových technologií je v řádu od několika metrů až po několik desítek kilometrů.

Na závěr lze konstatovat, že bezdrátové sítě dnes představují velmi zajímavou a do budoucna zcela jistě perspektivní možnost inovace stávajících průmyslových řešení, avšak s přihlédnutím k zajištění robustní ochrany sdílených informací a odpovídajícího zabezpečení přenosu data uživatelské komunikace srovnatelného s pevnými sítěmi.

Porovnání vlastností u vybraných typů bezdrátových sítí

Typ sítě	Název	Standard	Frekvenční pásmo	Nominální dosah	Maximální rychlost
WPAN	Bluetooth	IEEE 802.15.1	2,4 GHz	10 m	720 kbit/s
	IrDA	IrDA	Infračervené okno vlnová délka 850-900 nm	1 m	16 Mbit/s
	ZigBee	IEEE 802.15.4	868 MHz, 900 MHz, 2,4 GHz	10 m	250 kbit/s
	UWB	IEEE 802.15.3	3,1-10,6 GHz (USA) 3,4-4,8 GHz & 6-8,5 GHz (Evropa)	10 m	480 Mbit/s
WLAN	Wi-Fi	IEEE 802.11	2,4 / 5 GHz	100 m	1 Mbit/s
		IEEE 802.11a	5 GHz	100 m	48 Mbit/s
		IEEE 802.11b	2,4 GHz	100 m	11 Mbit/s
		IEEE 802.11g	2,4 GHz	100 m	54 Mbit/s
		IEEE 802.11n	2,4 / 5 GHz	250 m	600 Mbit/s
		IEEE 802.11ac	5 GHz	250 m	1,3 Gbit/s
WMAN	WiMAX	IEEE 802.16	2-11 GHz+10-66 GHz	50 km	70 Mbit/s
WWAN	Mobilní sítě	AMPS, GSM, GPRS, UMTS, HSDPA, LTE	700 MHz, 850 MHz, 900 MHz, 1800 MHz, 1900 MHz, 2100 MHz, 2600 MHz	> 50 km	1 Gbit/s
	Satelitní sítě	DVB-S2	3-30 GHz	> 50 km	60 Mbit/s