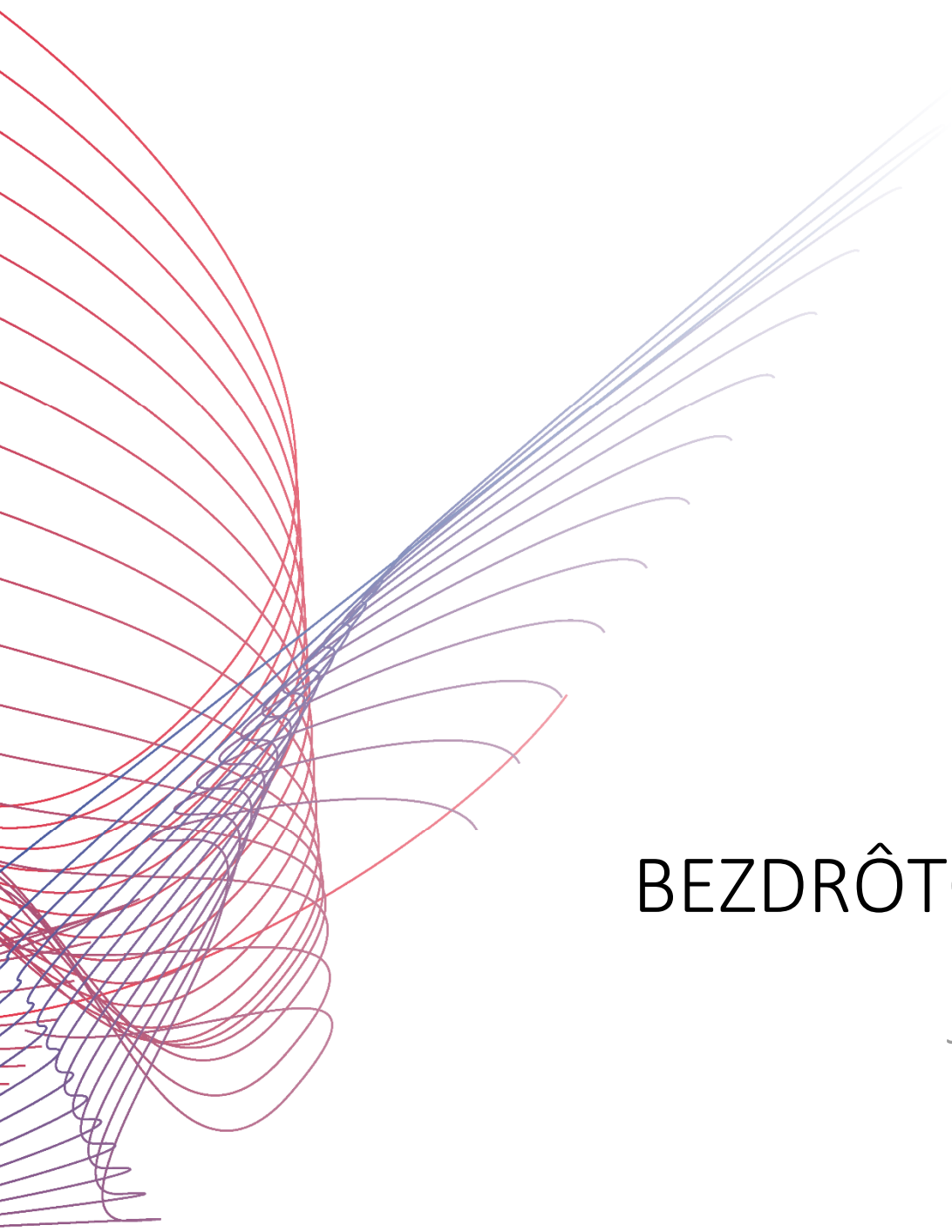
en cs de sk es

TECH pedia



BEZDRÔTOVÉ SIETE

JORDI SALAZAR

Názov: Bezdrôtové siete
Autor: Jordi Salazar
Preložil: Ján Dúha
Vydalo: České vysoké učení technické v Praze
Fakulta elektrotechnická
Kontaktná adresa: Technická 2, Praha 6, Česká republika
Tel.: +420 224352084
Tlač: (iba elektronická)
Počet strán: 36
Edícia (vydanie): 1. vydanie, 2017

ISBN 978-80-01-06200-5

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

Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).

VYSVETLIVKY

	Definícia
	Zaujímavosť
	Poznámka
	Príklad
	Zhrnutie
	Výhody
	Nevýhody

ANOTÁCIA

Tento modul predstavuje všeobecný úvod do problematiky bezdrôtových sietí a podrobnejšie lokálnych prístupových sietí LAN. Sú v ňom opísané a vysvetlené rôzne existujúce bezdrôtové technológie, ich základné vlastnosti, otázky bezpečnosti, výhody, nevýhody a použitie alebo aplikácie.

CIELE

Získať informácie o rozdieloch v architektúre jednotlivých sietí. Získať informácie o bezpečnostných aspektoch bezdrôtových sietí. Poznať prednosti a nedostatky bezdrôtových sietí.

LITERATÚRA

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

[2] B. Ciubotaru, G.M. Muntean, Advanced Network Programming. Principles and Techniques, Springer-Verlag London, 2013. ISBN 978-1-4471-5292-7.

[3] K. Sharma, N. Dhir, "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] K. Pothuganti, A. Chitneni, "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).

Obsah

1 Úvod do bezdrôtových sietí

Tento modul predstavuje všeobecný úvod do problematiky bezdrôtových sietí a podrobnejšie lokálnych prístupových sietí LAN. Sú v ňom opísané a vysvetlené rôzne existujúce bezdrôtové technológie, ich základné vlastnosti, otázky bezpečnosti, výhody, nevýhody a použitie alebo aplikácie.

Bezdrôtové siete sú siete, ktoré používajú na pripojenie zariadení rádiové vlny a nie je potrebné použiť nejaký druh vedení.

Zariadenia, ktoré obyčajne využívajú bezdrôtové pripojenie do siete sú prenosné počítače, stolné počítače, príručné počítače, PDA (osobný digitálny asistent), bunkové telefóny, počítače s grafickým používateľským rozhraním a pagery. Bezdrôtové siete pracujú podobne ako drôtové siete, naviac však musia bezdrôtové siete konvertovať informačné signály do formy vhodnej pre prenos vzduchom.

Bezdrôtové siete sa môžu využívať na rôzne účely. V niektorých prípadoch slúžia ako náhrada káblových vedení, kým v iných prípadoch sa používajú na zabezpečenie prístupu k podnikovým dátam zo vzdialených lokalít.

Bezdrôtová infraštruktúra môže byť vybudovaná s omnoho menšími nákladmi v porovnaní s tradičnými drôtovými alternatívami. Ale budovanie bezdrôtových sietí nepredstavuje len hospodárnosť. Ak majú ľudia v ich lokálnej komunite lacnejší a ľahší prístup k informáciám, tak môžu mať priamy úžitok z toho čo internet ponúka. Čas a námaha ušetrená umožnením priameho prístupu do globálnej informačnej siete sa premieňa na bohatstvo na lokálnej úrovni tým, že sa môže vykonať viac práce za kratší čas a s menšou námahou.

Bezdrôtové siete umožňujú pripojenie vzdialených zariadení bez ťažkostí nezávisle od toho, či ich vzdialenosť je pár metrov alebo niekoľko kilometrov. Nie je tiež potrebné prebúravať otvory v stenách na privedenie kábla alebo inštalovanie konektorov. Preto je táto technológia veľmi populárna a rýchlo sa rozširuje.

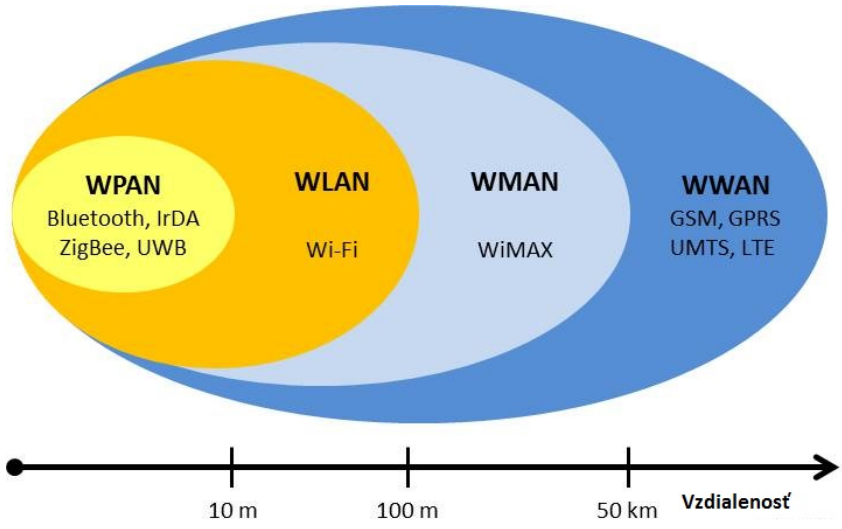
Existuje veľa rozličných technológií, ktoré sa líšia použitou vysielacou frekvenciou, rýchlosťou a dosahom ich vysielania.

Okrem toho sú však isté otázky súvisiace s právnou reguláciou elektromagnetického spektra. Elektromagnetické vlny sú vyžarované veľkým počtom zariadení, čo môže spôsobiť interferencie. Z tohto dôvodu potrebujú všetky krajiny predpisy, ktoré definujú frekvenčné rozsahy a vysielací výkon pre každú technológiu, ktorá je povolená.

Naviac šírenie elektromagnetických vĺn nie je ľahko možné obmedziť na presne vyhradený geografický priestor. Hacker môže ľahko odpočúvať sieť, ak prenášané dáta nie sú zakódované. Preto je potrebné urobiť všetky potrebné kroky na zaistenie utajenia dát prenášaných bezdrôtovými sieťami.

2 Bezdrôtové technológie

Bezdrôtové siete môžeme rozdeliť na štyri špecifické skupiny podľa oblasti ich použitia a dosahu signálu [1-3]: bezdrôtové personálne siete WPAN (Wireless Personal-Area Networks), bezdrôtové lokálne siete WLAN (Wireless Local-Area Networks), bezdrôtové veľkomestské siete WMAN (Wireless Metropolitan-Area Networks) a bezdrôtové rozľahlé siete WWAN (Wireless Wide-Area Networks). Obrázok 1.1 ilustruje tieto štyri kategórie.



Obrázok 1.1 Klasifikácia bezdrôtových sietí

Ďalej môžeme bezdrôtové siete rozdeliť aj na dve veľké skupiny: malého dosahu a veľkého dosahu. Bezdrôtové siete malého dosahu sú siete, ktoré majú pokrytie obmedzené na určitú obmedzenú oblasť. Toto platí pre lokálne siete (LAN) ako sú siete v budovách spoločnosti, školských areáloch, priemyselných závodoch alebo domoch a tiež personálne siete (PAN), v ktorých potrebujú prenosné počítače navzájom komunikovať na krátku vzdialenosť. Tieto siete obyčajne pracujú v nelicencovanom frekvenčnom pásme, vyhradenom na priemyselné, vedecké a medicínske účely (ISM). Tieto frekvenčné pásma sú v jednotlivých krajinách odlišné. Najčastejšie sú tieto frekvenčné pásma v oblasti 2,4 GHz a 5 GHz, ktoré sú väčšinou celosvetovo dostupné. Dostupnosť týchto frekvencií umožňuje používateľom prevádzkovať bezdrôtové siete bez získania licencie a bezplatne. Nakoľko na využívanie nie je potrebná licencia, umožnilo to expanziu týchto sietí.

V sieťach veľkého dosahu je pripojenie obyčajne realizované spoločnosťami, ktoré poskytujú bezdrôtové pripojenie ako platenú službu. Tieto siete pokrývajú veľké oblasti ako je veľkomesto (WMAN), štát alebo celá krajina. Výhodou sietí veľkého dosahu je poskytnutie globálneho pokrytia. Najbežnejšou sieťou veľkého dosahu je bezdrôtová rozľahlá sieť (WWAN). Keď je potrebné globálne pokrytie, je možné použiť aj družicovú sieť.

2.1 Bezdrôtové personálne siete (WPAN)

Bezdrôtové personálne siete sú založené na štandarde IEEE 802.15 [http://en.wikipedia.org/wiki/IEEE_802.15] [3], [4]. Umožňujú komunikáciu na veľmi malú vzdialenosť, približne 10 metrov. Na rozdiel od iných bezdrôtových sietí pripojenie prostredníctvom WPAN vyžaduje malú alebo žiadnu infraštruktúru alebo priame pripojenie k prostrediu mimo siete. To umožňuje miniatúrne, výkonovo efektívne, lacné riešenia, ktoré sa môžu realizovať pre široký okruh zariadení takých ako smartfón a PDA.

Tieto siete sú charakteristické nízkymi požiadavkami na výkon a malou prenosovou rýchlosťou. Tento druh sieťového prenosu využíva technológie ako Bluetooth, IrDA, ZigBee alebo UWB. Z hľadiska použitia je Bluetooth určený pre bezdrôtovú myš, klávesnicu a súpravu voľné ruky. IrDA je určený na spojenia bod – bod medzi dvomi zariadeniami na jednoduchý prenos dát a synchronizáciu súborov. ZigBee je navrhnutý na spoľahlivé bezdrôtové zosieťovanie monitorovacích a riadiacich sietí, UWB je orientovaný na širokopásmové multimediálne spoje.

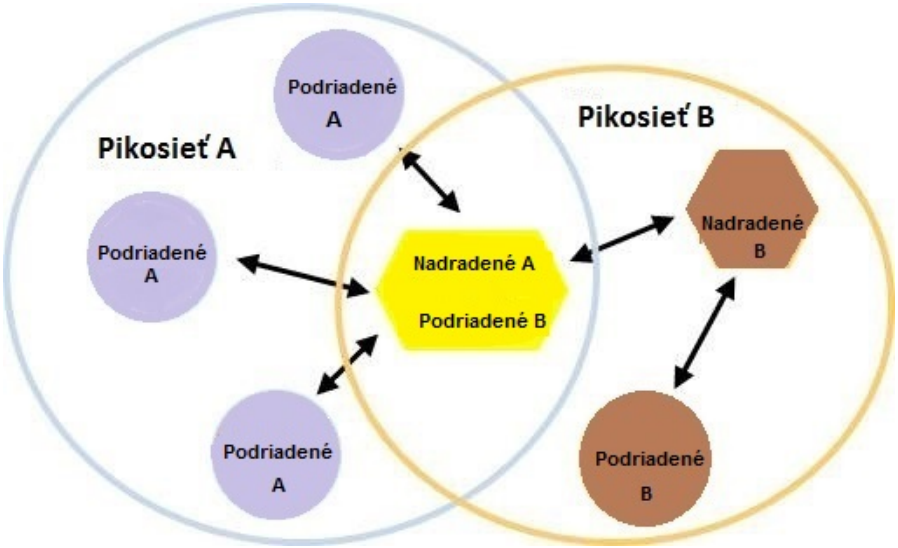
Bitová rýchlosť je počet bitov prenesených alebo prijatých za jednotku času (jednotka: bps alebo bit/s).

Modem je zariadenie, ktoré umožňuje počítaču vysielať a prijímať dáta.

Bluetooth

Bluetooth vyhovuje štandardu IEEE 802.15.1. Pôvodne bol Bluetooth navrhnutý z hľadiska nízkej energetickej náročnosti, všesmerového spojenia malého dosahu (bod – viac bodov), lacných zariadení (použité ako náhrada káblov), prepájania zariadení pomocou rádiového ad-hoc pripojenia. V súčasnosti vývojári navrhli vyhovujúce Bluetooth komponenty a systémy pre rad ďalších aplikácií. Táto technológia môže byť prevádzkovaná v troch odlišných triedach zariadení: Trieda 1, trieda 2 a trieda 3, ktorých dosah je približne 100 metrov, 10 metrov a respektíve 1 meter. Využíva sa pásmo 2,4 GHz, v rozsahu pokrytia môže každé z dvoch zariadení zdieľať kapacitu alebo prenosovú rýchlosť 720 kbit/s. Najčastejšie sa používa trieda 2.

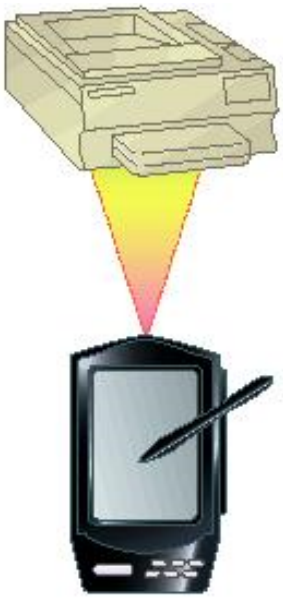
Sieť Bluetooth sa často označuje ako pikosieť a môže mať najviac 8 aktívnych zariadení a ich vzájomný vzťah je nadradené – podriadené zariadenie. Prvé zariadenie Bluetooth v pikosieti je nadradené a všetky ostatné zariadenia, ktoré komunikujú s nadradeným, sú podriadené. Pikosieť má typický dosah do 10 metrov, aj keď dosah 100 metrov je možné pri ideálnych podmienkach dosiahnuť. Pre zaistenie bezpečnosti je každé spojenie zakódovaním chránené pred odpočúvaním a interferenciami. Dve pikosiete je možné vzájomne prepojiť a vytvoriť rozptýlenú sieť. Zariadenia Bluetooth môžu participovať v niekoľkých pikosieťach v rovnakom čase, preto musíme počítať s možnosťou prenosu informácie aj mimo oblasti pokrytia jednej pikosiete. Zariadenie v rozptýlenej sieti môže byť podriadené v niekoľkých sieťach, ale nadradené len v jednej z nich.



Obrázok 1.2 Rozptýlená sieť Bluetooth pozostávajúca z dvoch pikosietí. Nadradené zariadenie v pikosieti A je podriadené v pikosieti B.

IrDA

Asociácia pre infračervený prenos IrDA (Infrared Data Association) špecifikovala kompletný súbor štandardov pre infračervený prenos. IrDA uvádza, že tento súbor štandardov je možné použiť pri poskytovaní bezdrôtového pripojenia zariadení, ktoré normálne používajú na pripojenie káble. IrDA je štandard navrhnutý na ad-hoc prenos dát pre nízkovýkonové, lacné, jednosmerné (bod – bod) zariadenia, vyžarujúce úzky zväzok (< 30º), pracujúce na vzdialenosť do 1 metra a s rýchlosťami od 9,6 kbit/s do 4 Mbit/s (aktuálne), 16 Mbit/s (vo vývoji). Zariadeniami, ktoré využívajú IrDA sú prenosné počítače, PDA, tlačiarne a kamery.

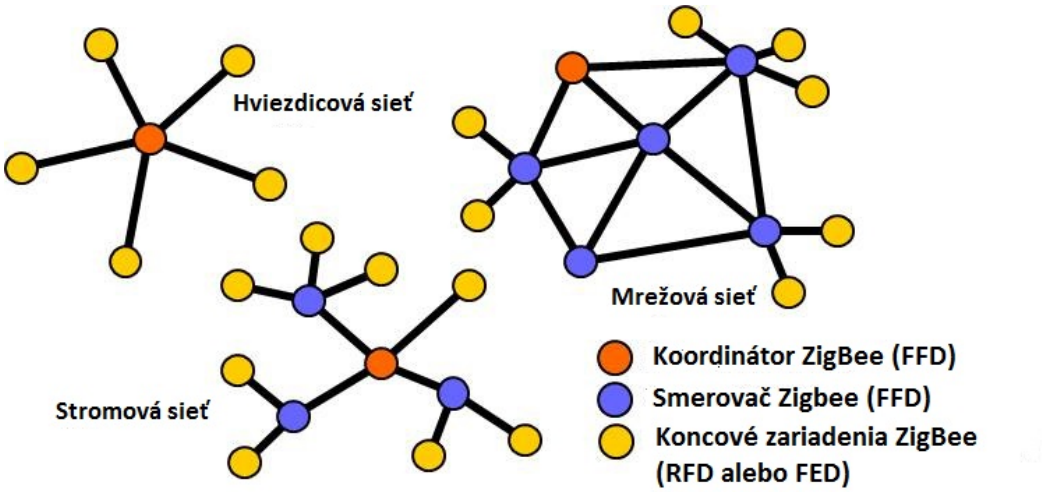


Obrázok 2 Komunikácia IrDA medzi PDA a tlačiarňou (bod - bod)

ZigBee

ZigBee je založený na štandarde IEEE 802.15.4 a bol vyvinutý ako otvorený globálny štandard, aby bolo možné splniť jedinečné požiadavky na ľahkú implementáciu, vysokú spoľahlivosť, nízku cenu, malý výkon a malú rýchlosť prenosu dát sietí bezdrôtových zariadení. ZigBee pracuje v nelicencovaných pásmach vrátane 2,4 GHz, 900 MHz a 868 MHz s maximálnou prenosovou rýchlosťou 250 kbit/s, čo postačuje z hľadiska bezdrôtových snímačov a automatizácie.

ZigBee slúži aj na vytvorenie rozľahlých bezdrôtových sietí nevyžadujúcich vysokú priepustnosť dát. V sieťach ZigBee môžu participovať dva rôzne typy zariadení: zariadenia s plnou funkčnosťou FFD (full-function devices) a zariadenia s redukovanou funkčnosťou RFD (reduced-function devices). FFD môžu pracovať v troch prevádzkových režimoch ako koordinátor WPAN, koordinátor alebo zariadenie. RFD je určené len pre aplikácie, ktoré sú extrémne jednoduché ako je napríklad spínač svetla. ZigBee podporuje tri rozdielne topológie: hviezdicovú, mrežovú a stromovú, ktoré sú uvedené na obrázku 1.4. Pri hviezdicovej topológii sa vytvára spojenie medzi zariadením a centrálnou riadiacou jednotkou, nazývanou WPAN koordinátor. Pri mrežovej topológii môže hociktoré zariadenie komunikovať s každým iným zariadením, ak sú vo vzájomnom dosahu. Stromová sieť je špeciálny prípad mrežovej siete, v ktorej sa väčšina zariadení FFD a RFD môže pripojiť do stromovej siete ako koncový uzol na konci vetvy. Niektorý FED môže pracovať ako smerovač a poskytovať synchronizačné služby iným zariadeniam a smerovačom. Len jeden z týchto smerovačov je WPAN koordinátor.



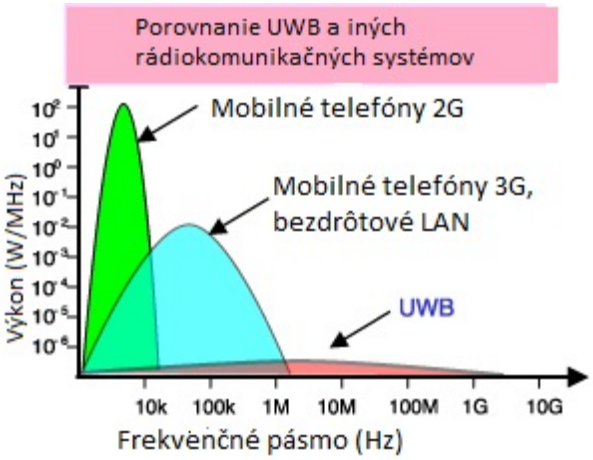
Obrázok 1.4 Schéma štruktúry siete ZigBee

UWB

Technológii ultraširoké pásmo UWB (Ultra Wide Band), založenej na štandarde IEEE 802.15.3, sa v poslednom čase venuje veľká pozornosť nakoľko umožňuje vysokorýchlostnú komunikáciu na krátke vzdialenosti vo vnútri budov. UWB slúži na odlišné účely ako iné technológie uvedené v tejto časti. UWB umožňuje prenos

veľkých súborov vysokými rýchlosťami na krátke vzdialenosti. UWB umožňuje prenos dát rýchlosťou od 110 Mbit/s až do 480 Mbit/s, čo môže vyhovovať väčšine multimediálnych aplikácií ako je doručovanie audia a videa v domácich sieťach. Môže slúžiť aj ako bezdrôtová náhrada káblov vysokorýchlostnej sériovej zbernice ako je napríklad USB 2.0 a IEEE 1394. V Amerike boli pre UWB vyčlenené frekvencie v pásme od 3,1 GHz do 10,6 GHz. V Európe sú však vyčlenené frekvencie rozdelené do dvoch častí: od 3,4 GHz do 4,8 GHz a od 6 GHz do 8,5 GHz.

Pri UWB prenosoch sa informácia prenáša pomocou generovania vysokofrekvenčnej energie v špecifických časových intervaloch a obsadením širokého frekvenčného pásma (obr. 1.5), čo umožňuje impulzovú polohovú alebo časovú moduláciu. Informácia môže byť tiež namodulovaná na UWB signály (impulzy) pomocou kódovania polarity impulzu, jeho amplitúdy a/alebo použitím ortogonálnych impulzov. UWB impulzy môžu byť vysielané sporadicky s relatívne nízkymi frekvenciami impulzov, čo je vhodné pre časovú alebo polohovú moduláciu, ale môžu sa vysielať len frekvenciami, ktoré nie sú vyššie ako prevrátená hodnota šírky pásma UWB impulzu.

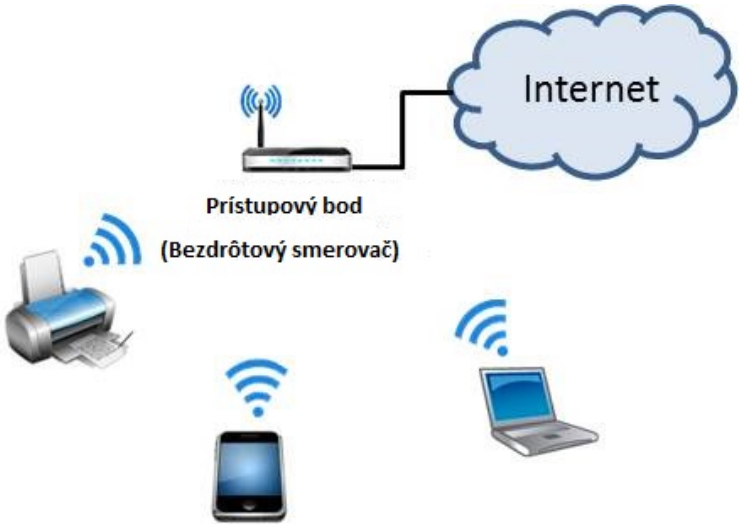


Obrázok 1.5 Využitie výkonu a frekvenčného pásma UWB.

2.2 Bezdrôtová lokálna sieť (WLAN)

Bezdrôtové lokálne siete (WLAN) boli navrhnuté na zabezpečenie bezdrôtového prístupu v oblastiach s typickým rozsahom do 100 metrov a najčastejšie sa používajú v prostredí domov, škôl, počítačových laboratórií alebo úradov (obr. 1.6). Poskytuje to používateľom možnosť pohybovať sa vo vnútri oblasti lokálneho pokrytia, pričom stále zostávajú pripojení do siete [2], [5]. Siete WLAN sú založené na štandardoch IEEE 802.11 a ponúkané sú pod obchodnou značkou Wi-Fi. V dôsledku súťaže iné štandardy ako napríklad HiperLAN nikdy nedosiahli veľa komerčných implementácií. Štandard IEEE 802.11 bol jednoduchší na implementovanie a rýchlejšie sa presadzoval na trhu. Kompletný súbor bude detailnejšie opísaný v časti 4.

IEEE 802.11 je skupina rozdielnych štandardov pre bezdrôtové lokálne siete. Štandard IEEE 802.11b bol prvým prijatým štandardom podporujúcim prenosovú rýchlosť do 11 Mbit/s v nelicencovanom pásme spektra 2,4 GHz. Potom bol navrhnutý štandard IEEE 802.11g ako širokopásmový nasledovník IEEE 802.11b. Prístupový bod IEEE 802.11g musí podporovať klientov 802.11b a 802.11g. Jednoducho, prenosný počítač s kartou IEEE 802.11g musí byť schopný pripojiť sa na existujúce prístupové body 802.11b ako aj na nové prístupové body 802.11g. Je to dané tým, že siete LAN založené na 802.11g používajú rovnaké pásmo 2,4 GHz ako využívajú siete 802.11b. Maximálna prenosová rýchlosť bezdrôtového spoja IEEE 802.11g je 54 Mbit/s, ale automaticky klesá pri nízkej úrovni rádiového signálu alebo keď sú detegované interferencie.



Obrázok 1.6 Schéma domácej WLAN

2.3 Bezdrôtové veľkomestské siete WMAN

Bezdrôtové veľkomestské siete WMAN (Wireless Metropolitan Area Network) sú treťou skupinou bezdrôtových sietí. WMAN sú založené na štandarde IEEE 802.16, ktorý sa často nazýva WiMAX (Worldwide Interoperability for Microwave Access – celosvetová interoperabilita pre mikrovlnový prístup). WiMAX je komunikačná technológia, ktorá podporuje architektúru bod – viac bodov zameraná výhradne na vysokorýchlostný prenos dát sieťami vo veľkomestskej oblasti [1-3]. To umožňuje prepojiť malé siete LAN pomocou siete WiMAX a vytvoriť rozľahlú WMAN. Takto je možné realizovať prepojenie miest bez nutnosti použiť drahú kabeláž.

WiMAX sa podobá Wi-Fi, ale poskytuje pokrytie na podstatne väčšie vzdialenosti. Kým Wi-Fi je určené na zabezpečenie pokrytia relatívne malých oblastí, takých ako sú úrady alebo prístupové miesta, WiMAX pracuje v dvoch frekvenčných pásmach, kombinácii licencovaného a nelicencovaného pásma, od 2 GHz do 11 GHz a od 10 GHz do 66 GHz a môže zabezpečovať prenos rýchlosťou približne 70 Mbit/s do vzdialenosti 50 km tisíckam používateľov z jednej základňovej stanice ako je znázornené na obrázku 1.7. Nakoľko môže operovať v dvoch frekvenčných pásmach, WiMAX môže pracovať v režime s priamou viditeľnosťou a bez priamej viditeľnosti. Vo frekvenčnom rozsahu od 2 do 11 GHz pracuje v režime bez priamej viditeľnosti, kedy počítač vo vnútri budovy komunikuje prostredníctvom veže/antény mimo budovy. Prenos nižšími frekvenciami sa nedá ľahko prerušiť fyzickými prekážkami. Prenos vyššími frekvenciami sa používa u služieb pri priamej viditeľnosti. Umožňuje to veži/anténe komunikovať s ľubovoľnou inou na veľkú vzdialenosť.

Obrázok 1.7 Schéma siete WiMaX

2.4 Bezdrôtová rozľahlá sieť (WWAN)

Bezdrôtové rozľahlé siete WWAN (Wireless Wide Area Networks) majú dosah do 50 kilometrov a obyčajne využívajú licencované frekvencie. Tento typ sietí môže obsluhovať veľmi rozľahlé oblasti ako sú mestá alebo krajiny pomocou niekoľkých družicových systémov alebo stanovíšť antén zamierených na nejakého poskytovateľa internetových služieb. Dostupné sú dve hlavné technológie: digitálne bunkové telefóny a družice [1-3].

Bunkové telefónne siete

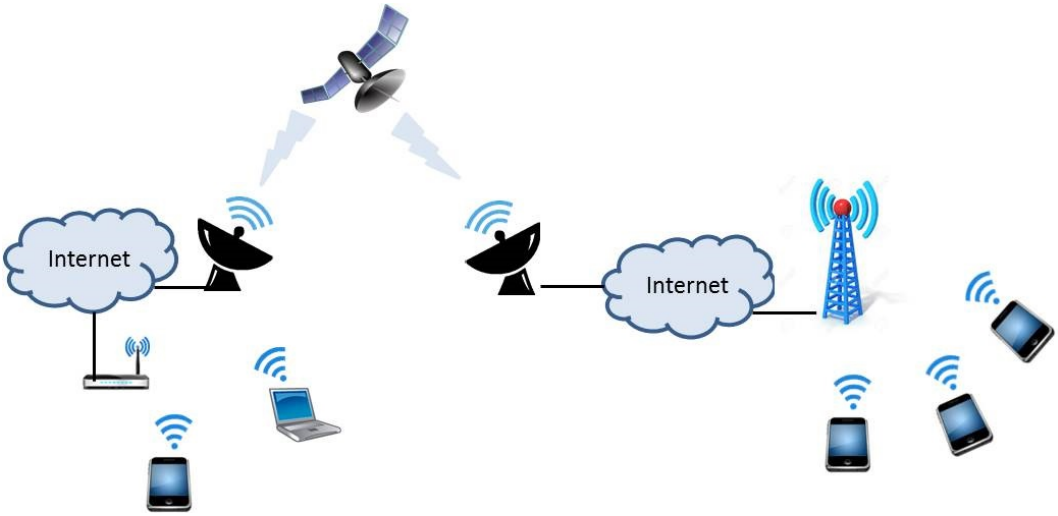
V bunkovom systéme je pokrývaná oblasť rozdelená na bunky. Bunkový vysielač v strede bunky je navrhnutý na obsluhovanie jednej bunky. Všetky vysielače sú pripojené k základňovej stanici a táto je ďalej pripojená na mobilnú telekomunikačnú ústredňu, ktorá prepája bunkovú a klasickú metalickú sieť. Systém sa snaží zabezpečiť efektívne využitie dostupných kanálov použitím nízkovýkonových vysielačov, aby bolo možné opakované použitie frekvencií pri veľmi malých vzdialenostiach.

Od začiatku osemdesiatych rokov boli vyvinuté rôzne bunkové generácie. Prvá generácia 1G bola analógová, koncipovaná a navrhnutá výhradne pre hlasové volania a prakticky sa neuvažovalo o dátových službách s prenosovou rýchlosťou nad 2,4 kbit/s. Druhá generácia 2G bola založená na digitálnej technológii a sieťovej infraštruktúre (GSM) umožňujúcej prenos textových správ a pri prenose dát prenosovú rýchlosť do 64 kbit/s. Generácia 2,5G bola medzi druhou a treťou. Občas bola označovaná ako 2G + GPRS a je to zdokonalená verzia 2G s rýchlosťou prenosu dát do 144 kbit/s. Generácia 3G bola zavedená v roku 2000 s rýchlosťou prenosu dát do 2 Mbit/s. Generácia 3.5G je zdokonalená verzia 3G, ktorá využíva HSDPA na prenos dát rýchlosťou do 14 Mbit/s. Nakoniec štvrtá generácia 4G je schopná poskytovať rýchlosť do 1 Gbit/s a poskytovať akýkoľvek druh služby kedykoľvek podľa požiadaviek používateľa a kdekoľvek. Generácia 5G sa predpokladá v roku 2020.

Družica

Bezdrôtové komunikácie môžu byť vytvorené aj cez družicu. Vďaka jej veľkej výške môže družicový prenos pokryť veľkú oblasť na povrchu Zeme. To môže byť veľmi užitočné pre používateľov, ktorí sa nachádzajú vo vzdialených oblastiach alebo na ostrovoch kde nie sú v prevádzke podmorské káble. V takýchto prípadoch sú potrebné družicové telefóny.

Každá družica je vybavená rôznymi transpondérmi skladajúcimi sa z vysielača, prijímača a antény. Prichádzajúci signál je zosilnený a potom opätovne vysielaný na odlišnej frekvencii.



Obrázok 1.8 Družicové a bunkové siete

3 Architektúra siete

3.1 Termíny a terminológia

Táto časť poskytuje definíciu rôznych termínov používaných v architektúre bezdrôtovej siete. Avšak nie všetky bloky zo všeobecnej architektúry sa vyskytujú vo všetkých technológiách a presná funkčnosť môže byť odlišná.

Logická architektúra 802.11 obsahuje niekoľko hlavných komponentov: stanica (STA), bezdrôtový prístupový bod (AP), sada nezávislej základnej služby (IBSS), sada základnej služby (BSS), distribučný systém (DS) a sada rozšírenej služby (ESS). Niektoré komponenty logickej architektúry 802.11 mapujú priamo také hardvérové zariadenia ako STA a bezdrôtové AP. Bezdrôtová STA obsahuje kartu adaptéra, PC kartu alebo vložené zariadenie na zabezpečenie bezdrôtovej pripojiteľnosti. Bezdrôtový AP slúži ako mostík na prístup do siete medzi bezdrôtovými STA a existujúcou chrbticovou sieťou.

Stanicou (STA) môže byť klasický osobný počítač **PC** (*Personal Computer*), prenosný počítač (notebook), PDA (palmtop), Smartphone, alebo akékoľvek iné zariadenie, ktoré je schopné využívať prístup na bezdrôtové médium.

Prístupový bod (AP), niekedy označovaný ako **základňová stanica (BS),** je zariadenie umožňujúce bezdrôtovým zariadeniam pripojiť sa do drôtovej siete použitím Wi-Fi alebo súvisiacich štandardov.

Sada základnej služby (BSS) pozostáva z prístupového bodu a všetkých k nemu priradených STA. AP pôsobí ako nadradený pri riadení všetkých STA v rámci BSS. Najjednoduchšia BSS sa skladá z jedného AP a jednej STA.

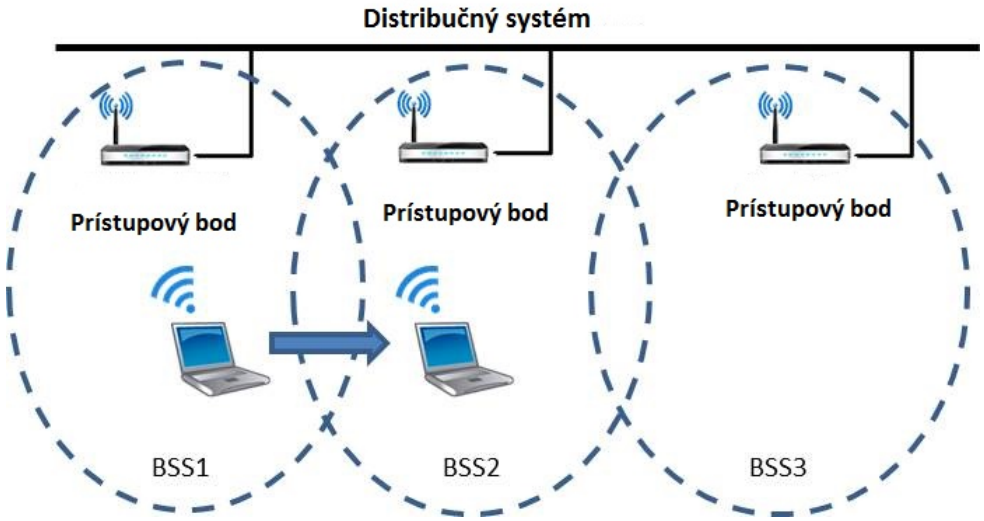
Sada rozšírenej služby (ESS) je sada jednej alebo niekoľkých prepojených sád základnej služby (BSS), ktorá sa javí ako jednoduchá BSS pre vrstvu riadenia logického spoja na nejakej stanici priradenej jednej z týchto BSS.

Ak sú všetky stanice v BSS mobilné stanice a nie je tam pripojenie k drôtovej sieti, BSS sa označuje ako **nezávislá BSS (IBSS)**. IBSS je ad-hoc sieť, v ktorej nie sú prístupové body. To znamená, že sa nemôže pripojiť na nejakú inú sadu základnej služby.

Distribučný systém (DS) je mechanizmus, pomocou ktorého si prístupové body AP vymieňajú rámce medzi sebou a drôtovými sieťami, ak nejaké sú. DS nie je nevyhnutne sieť a štandard IEEE 802.11 nešpecifikuje nejakú konkrétnu

technológiu pre DS. Takmer vo všetkých komerčných produktoch sa ako technológia chrbticových sietí používa drôtový Ethernet.

Obrázok 1.9 Sada nezávislej a infraštruktúrnej služby (BSS)



Obrázok 1.10 Sada rozšírenej služby (ESS) a podpora mobility.

3.2 Architektúry

V bezdrôtových sieťach sú dva módy konfigurácie bezdrôtovej architektúry a to ad-hoc a infraštruktúrny [1], [2]. Pri móde ad-hoc sú zariadenia pri prenose rovnocenné, kým pri inraštruktúrnom móde zariadenia komunikujú prostredníctvom prístupového bodu, ktorý slúži ako mostík k iným sieťam.

Mód ad-hoc

Pri použití módu ad-hoc všetky zariadenia v bezdrôtovej sieti komunikujú priamo medzi sebou (bod – bod). Sieť nemá štruktúru alebo pevné body. Na komunikáciu medzi zariadeniami nie je potrebný prístupový bod.

Mód ad-hoc je vhodný pre malé skupiny zariadení a všetky tieto zariadenia musia byť fyzicky vzájomne dostatočne blízko. Výkonnosť siete sa zhoršuje, keď sa zvyšuje počet zariadení. K odpojeniam ľubovoľného zariadenia môže dochádzať často, preto mód ad-hoc môže byť ťažkou úlohou pre správcu siete riadiaceho takúto sieť. Ďalšie obmedzenie módu ad-hoc je, že siete pracujúce v móde ad-hoc nemôžu byť mostíkom do drôtovej lokálnej siete a teda nemajú prístup k internetu, ak nie sú nainštalované špeciálne sieťové prechody.

Mód ad-hoc však výborne pracuje na malom priestore a poskytuje najľahší a najlacnejší postup na vybudovanie bezdrôtovej siete.

Infraštruktúrny mód

Druhou architektúrou pre mobilné siete je infraštruktúrny mód. Všetky zariadenia sú pripojené do bezdrôtovej siete pomocou prístupového bodu (AP). Prístupové body sú obyčajne smerovače alebo prepínače, ktoré konvertujú rádiovo prenášané dáta na dáta prenositeľné drôtovým ethernetovým spojom. AP je teda mostíkom medzi drôtovou LAN a bezdrôtovými účastníkmi. Prepojenie viacerých prístupových bodov pomocou drôtovej ethernetovej chrbticovej dátovej siete umožňuje ďalšie rozšírenie pokrytia bezdrôtovej siete. Keď sa mobilné zariadenie pohybuje mimo dosah jedného prístupového bodu, dostáva sa do dosahu ďalšieho. Výsledkom je, že bezdrôtový účastník sa môže voľne pohybovať od jednej prístupovej domény k druhej a neprerušovane udržiavať pripojenie ku sieti.

Infraštruktúrny mód poskytuje väčšiu bezpečnosť, ľahšie riadenie, väčšiu rozšíriteľnosť a stabilitu. Infraštruktúrny mód však spôsobí aj zvýšenie nákladov vytvorením prístupových bodov, takých ako sú smerovače a spínače.

Identifikátor sady rozšírenej služby (ESSID)

Identifikácia sady rozšírenej služby ESSID (Extended Service Set Identification) je jeden z dvoch typov identifikácie sady služby SSID (Service Set Identification). V bezdrôtovej sieti ad-hoc bez prístupových bodov sa používa identifikácia sady základnej služby BSSID (Basic Service Set Identification). V infraštruktúrnej

bezdrôtovej sieti, ktorá má prístupový bod sa používa ESSID, ale môže byť požadovaný SSID.

Identifikácia služby (SSID) je 32-znakový (maximálne) alfanumerický kľúč identifikujúci názov bezdrôtovej lokálnej siete.

Niektorí predajcovia označujú SSID ako názov siete. Bezdrôtové zariadenia v sieti musia byť pre zabezpečenie vzájomnej komunikácie nakonfigurované s rovnakým SSID.

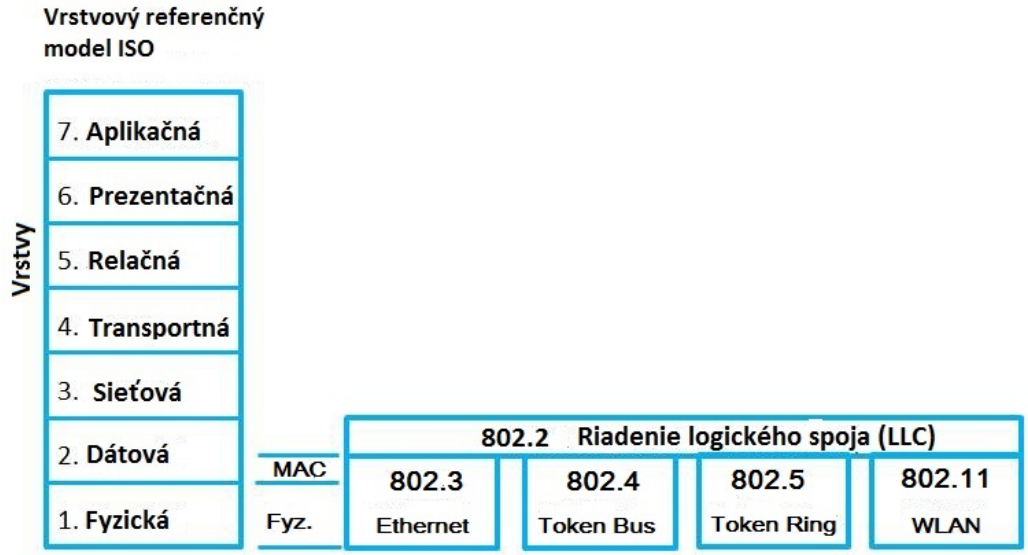
4 Štandard IEEE 802.11

IEEE 802.11 je sada špecifikácií riadenia prístupu k prenosovému médiu (MAC) a fyzickú vrstvu (PHY) pre implementovanie bezdrôtových lokálnych sietí na frekvenčných pásmach 2,4, 5 a 60 GHz [1], [2].

Vytvorené a udržiavané sú Pracovnou skupinou IEEE 802.11. Základná verzia štandardu bola uvoľnená v roku 1997 a má ďalšie dodatky. Štandard aj dodatky predstavujú základ pre produkty používajúce značku Wi-Fi určené pre bezdrôtové siete.

4.1 Protokol 802.11

Výbor štandardov IEEE 802 definuje dve samostatné vrstvy: riadenie logického spoja LLC (Logical Link Control) a riadenie prístupu k prenosovému médiu MAC (Media Access Control) pre vrstvu dátového spoja referenčného modelu OSI. Bezdrôtový štandard IEEE 802.11 definuje špecifikácie pre fyzickú vrstvu a vrstvu riadenia prístupu k prenosovému médiu MAC, ktorá komunikuje po vrstve LLC ako je uvedené na obrázku 1.11.



Obrázok 1.11 Štandard IEEE 802.11 a referenčný model OSI

Všetky komponenty v architektúre 802.11 spadajú buď pod podvrstvu riadenia prístupu k prenosovému médiu (MAC) vrstvy dátového spoja alebo fyzickú vrstvu (PHY).

4.2 Rámec MAC 802.11

Rámec MAC podľa štandardu IEEE 802.11, ako je uvedené na obrázku 1.12, sa skladá zo záhlavia MAC, tela rámca a kontrolnej postupnosti rámca (FCS). Formát rámca MAC sa skladá z deviatich polí, ktoré sa vyskytujú v nezmenenom poradí vo všetkých rámcoch.

Pole riadenia rámca

Pole riadenia rámca, pozri obrázok 1.12, obsahuje riadiacu informáciu používanú na definovanie typu rámca MAC 802.11 a poskytuje potrebnú informáciu o nasledujúcich poliach, aby bolo zrejmé ako má byť rámec MAC spracovaný.

Opis každého subpoľa v poli riadenia rámca je uvedený nižšie:

- **Verzia protokolu** určuje použitú platnú verziu protokolu 802.11. Prijímajúce stanice STA použijú túto veličinu na určenie, či je verzia protokolu prijatého rámca podporovaná.
- **Typ a podtyp** určuje funkciu rámca. Existujú tri odlišné polia typu rámca: riadenia, dát a manažmentu. Existuje niekoľko podtypov polí pre každý typ rámca. Každý podtyp stanovuje špecifickú funkciu na vytvorenie jemu prislúchajúceho typu rámca.
- **Do DS a od DS** indikuje či rámec prichádza alebo odchádza z DS (distribučný systém) a používa sa len v rámcoch dátového typu staníc STA priradených k nejakému AP.
- **Ďalšie fragmenty** indikujú, či bude nasledovať viac fragmentov rámca, buď dátových alebo manažmentu.
- **Zopakuj** indikuje, či bude alebo nebude rámec, buď dátového alebo manažmentového typu, opätovne prenášaný.
- **Manažnent výkonu** indikuje, či je vysielacia STA v aktívnom alebo úspornom režime.
- **Ďalšie dáta** indikuje stanici STA v šetriacom režime, že AP má ďalšie rámce na vysielanie. Používa sa tiež pre stanice AP na indikáciu toho, že nasledujú ďalšie rámce hromadného/skupinového prenosu.
- **WEP** indikuje, či je alebo nie je v rámci použité šifrovanie a autentifikácia. Môže byť nastavený pre všetky dátové rámce a rámce manažmentu, ktoré majú podtyp nastavený na autentifikáciu.
- **Poradie** indikuje, že všetky prijaté dátové rámce musia byť spracované v poradí.

Trvanie/Pole ID

Toto pole sa používa pre všetky rámce riadiaceho typu s výnimkou pri podtype *výzva šetri výkon* (PS), na indikovanie času zostávajúceho do príjmu nasledujúceho rámca. Ak podtyp je výzva PS, pole obsahuje identitu priradenia (AID) vysielacej STA.

Polia adries

V závislosti od typu rámca bude päť polí adries obsahovať kombináciu nasledujúcich typov adries:

- **Identifikátor BSS (BSSID)** jednoznačne identifikuje každú BSS. Ak je rámec od STA v infraštruktúre BSS, BSSID je MAC adresa prístupového bodu AP. Ak je rámec z STA v IBSS, BSSID je náhodne generovaný, lokálne spravovaná MAC adresa STA potom iniciuje IBSS.
- **Cieľová adresa (DA)** indikuje MAC adresu konečného cieľa na prijatie rámca.
- **Zdrojová adresa (SA)** udáva MAC adresu pôvodného zdroja, ktorý pôvodne vytvoril a odoslal rámec.
- **Adresa prijímača (RA)** udáva MAC adresu nasledujúcej priamej STA v bezdrôtovom prostredí na príjem rámca.
- **Adresa vysielača (TA)** udáva MAC adresu STA, ktorá rámec vysiela v bezdrôtovom prostredí.

Pre viac informácií o typoch adries a obsahoch adresových polí v záhlaví MAC 802.11 pozri štandard IEEE 802.11 na webovej stránke IEEE [6].

Riadenie postupnosti

Pole riadenia postupnosti obsahuje dve podpolia: pole počtu fragmentov a pole poradového čísla ako je to uvedené na obrázku 1.12.

Opis každého subpoľa v poli riadenia postupnosti je uvedený nižšie:

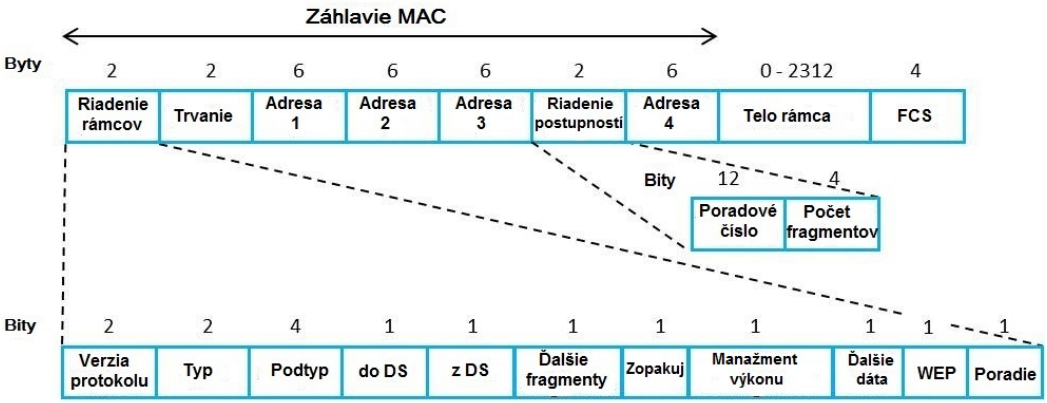
- **Poradové číslo** udáva poradové číslo každého rámca. Poradové číslo je rovnaké pre každý rámec vysielaný pre fragmentovaný rámec alebo je číslo inkrementované, keď dosiahne hodnotu 4095, potom začína znova od nuly.
- **Číslo fragmentu** udáva číslo každého rámca odoslaného ako fragmentovaný rámec. Začiatočná hodnota je nastavená na 0 a potom inkrementovaná o jednotku pri každom jednotlivom rámci fragmentovaného rámca.

Telo rámca

Telo rámca obsahuje dáta alebo informácie začlenené do rámcov manažmentového alebo dátového typu.

Kontrolná postupnosť rámca

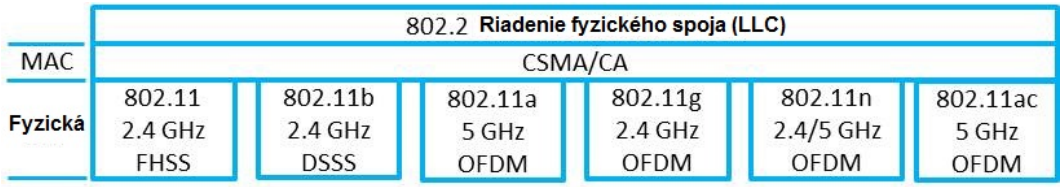
Vysielajúca STA používa cyklickú kontrolu redundancie (CRC) vo všetkých poliach záhlavia MAC a poli tela rámca na generovanie hodnoty FCS. Prijímacia STA potom použije rovnaký výpočet CRC a stanoví jej vlastnú hodnotu poľa FCS na zistenie, či sa vyskytli alebo nevyskytli chyby v rámci počas prenosu.



Obrázok 1.12 Formát rámca MAC štandardu 802.11. Polia riadenia rámca a riadenia postupnosti sú znázornené detailne.

4.3 Fyzická podvrstva 802.11

Na fyzickej podvrstve IEEE 802.11 definuje rad kódovacích a prenosových metód pre bezdrôtovú komunikáciu. Najbežnejšie z nich sú rozprestretie spektra frekvenčnými skokmi FHSS (Frequency Hopping Spread Spectrum), priame rozprestretie spektra postupnosťou DSSS (Direct Sequence Spread Spectrum) a multiplex ortogonálnych frekvencií OFDM (Orthogonal Frequency Division Multiplexing). Na obrázku 1.13 sú uvedené štandardy 802.11, 802.11b, 802.11a, 802.11g, 802.11n a 802.11ac, ktoré existujú na podvrstve PHY. Tieto štandardy sú opísané v nasledujúcich častiach.



Obrázok 1.13 Štandardy IEEE 802.11 na PHY vrstve.

IEEE 802.11

Bitová rýchlosť podľa pôvodného štandardu IEEE 802.11 je 2 Mbit/s pri použití prenosovej metódy FHSS a frekvenčného pásma ISM, v ktorom sa využíva frekvenčný rozsah od 2,4 do 2,5 GHz. Vplyvom horších podmienok ako ideálne sa používa nižšia bitová rýchlosť 1 Mbit/s.

802.11b

Hlavným zlepšením IEEE 802.11 na IEEE 802.11b je štandardizácia fyzickej vrstvy na podporu vyšších bitových rýchlostí. IEEE 802.11b podporuje dve ďalšie rýchlosti 5,5 Mbit/s a 11 Mbit/s pri využití frekvenčného pásma 2,4 GHz. Použitá je prenosová metóda DSSS, aby sa zabezpečili vyššie bitové rýchlosti. Bitová rýchlosť 11 Mbit/s je dosiahnuteľná za ideálnych podmienok, používajú sa nižšie rýchlosti 5,5 Mbit/s, 2 Mbit/s a 1 Mbit/s.

Je dôležité poznamenať, že 802.11b využíva rovnaké frekvenčné pásmo ako mikrovlnové rúry, bezdrôtové telefóny, detské monitory, bezdrôtové videokamery a zariadenia Bluetooth.

802.11a

IEEE 802.11a pracuje s bitovou rýchlosťou dosahujúcou 54 Mbit/s a využíva 5 GHz frekvenčné pásmo. Namiesto DSSS používa 802.11a metódu OFDM, ktorá umožňuje aby sa dáta prenášali paralelne na subfrekvenciách. Je odolnejšia voči rušeniu a má vyššiu priepustnosť. Táto vysokorýchlostná technológia umožňuje vytváranie bezdrôtových LAN, ktoré sú lepšie pre video a konferenčné aplikácie.

Nakoľko to nie sú rovnaké frekvencie, aké používajú iné zariadenia (také ako bezdrôtové telefóny, ktoré pracujú vo frekvenčnom pásme 2,4 GHz), OFDM a IEEE 802.11a poskytuje vyššiu rýchlosť prenosu dát aj lepší signál. Bitová rýchlosť 54 Mbit/s je dosiahnuteľná pri ideálnych podmienkach. Používajú sa nižšie rýchlosti 48 Mbit/s, 36 Mbit/s, 24 Mbit/s, 18 Mbit/s, 12 Mbit/s a 6 Mbit/s.

802.11g

IEEE 802.11g pracuje s bitovou rýchlosťou vyššou ako 54 Mbit/s, ale využíva frekvenčné pásmo 2,4 GHz a OFDM. Štandard 802.11g je preto spätne kompatibilný s 802.11b a môže pracovať s bitovými rýchlosťami 802.11b a používať DSSS. Adaptéry bezdrôtovej siete 802.11g sa môžu pripojiť k bezdrôtovému AP 802.11b a adaptéry bezdrôtovej siete 802.11b sa môžu pripojiť k bezdrôtovému AP 802.11g. Takto poskytuje 802.11g možnosť migrácie sietí 802.11b na frekvenčne kompatibilnú štandardnú technológiu s vyššou bitovou rýchlosťou. Existujúce adaptéry bezdrôtovej siete nie je možné aktualizovať na 802.11g aktualizovaním firmvéru adaptéra, musia byť vymenené. Nie je to však taká ako migrácia z 802.11b na 802.11a pri ktorej musia byť všetky sieťové adaptéry v oboch sieťach bezdrôtových účastníkov a bezdrôtových AP vymenené v rovnakom čase. Migráciu z 802.11b na 802.11g je možné robiť prírastkovo.

Podobne ako 802.11a používa 802.11g rýchlosť 54 Mbit/s pri ideálnych podmienkach a nižšie rýchlosti 48 Mbit/s, 36 Mbit/s, 24 Mbit/s, 18 Mbit/s, 12 Mbit/s a 6 Mbit/s pri podmienkach horších ako ideálne.

802.11n

Cieľom štandardu IEEE 802.11n je zvýšenie dosahu (do 250 m) a priepustnosti siete v porovnaní s dvomi predchádzajúcimi štandardmi 802.11a a 802.11g s významným zvýšením maxima základnej rýchlosti prenosu dát z 54 Mbit/s na 600 Mbit/s pri ideálnych podmienkach pridaním technológie *viacnásobný vstup - viacnásobný výstup* a kanálov s väčšou šírkou pásma 40 MHz. Táto technológia, označovaná ako MIMO, používa viac bezdrôtových signálov a antén vysielača aj prijímača. Môže sa používať vo frekvenčných pásmach 2,4 GHz alebo 5 GHz.

802.11ac

Štandard 802.11ac, aktualizovaný z 802.11n poskytuje rovnaký dosah, ale zvyšuje priepustnosť. Pracuje v pásme 5 GHz a zahŕňa tvarovanie zväzku, široké pásma a viac antén na dosiahnutie teoretickej rýchlosti prenosu dát 1,3 Gbit/s, čo je viac ako dvojnásobok maximálnej rýchlosti 600 Mbit/s pri 802.11n.

5 Bezpečnosť

Bezdrôtové siete nie sú vo všeobecnosti také bezpečné ako drôtové siete. Drôtové siete, na ich základnej úrovni, prenášajú dáta medzi dvomi bodmi A a B, ktoré sú pripojené ku sieťovému káblu. Bezdrôtové siete však vysielajú dáta všetkými smermi ku každému zariadeniu v oblasti limitovaného dosahu, ktoré je schopné odpočúvať. Drôtová sieť môže byť zabezpečená na jej okrajoch, napríklad obmedzením fyzického prístupu alebo inštalovaním bezpečnostných rozhraní (firewallov). Bezdrôtová sieť rovnakého rozsahu je ale napadnuteľná odpočúvaním. Bezdrôtové siete preto vyžadujú väčšie úsilie zamerané na zaistenie bezpečnosti.

5.1 Bezpečné komunikácie

Komunikačná bezpečnosť je často popísaná pomocou troch veličín: Autentifikácia, diskrétnosť a integrita [1].

Autentifikácia zabezpečuje, že uzly sú tým za koho sa vydávajú.

Autentifikácia sa obyčajne zakladá na demonštrovaní vedomosti o nejakom spoločnom tajomstve, takom ako je meno používateľa alebo dvojica hesiel. V zložitejších systémoch môže byť vlastníctvo spoločného tajomstva preukázané pomocou overenia vlastníctva znaku, ktorý je veľmi ťažké ukradnúť alebo sfalšovať, takého ako certifikát alebo inteligentná karta.

Diskrétnosť zabezpečuje, aby odpočúvajúci neoprávnený posluchač nemohol čítať správy prenášané sieťou.

Diskrétnosť sa obyčajne chráni pomocou šifrovania obsahu správy. Šifrovanie využíva známu reverzibilnú metódu transformácie (označovanú ako šifra alebo šifrovací algoritmus) na obsah pôvodnej správy (označovanej ako nešifrovaný text) zakódovaním alebo maskovaním sa potom vytvorí šifrovaný text. Len ten, kto pozná ako realizovať spätný proces (dešifrovať správu), môže získať späť pôvodnú správu. Najbežnejšími formami šifrovania sú matematické transformácie, ktoré používajú rôzne kľúče ako súčasť ich spracovania. Príslušný príjemca musí poznať obidve korekčné metódy a hodnotu kľúča, ktorý bol použitý, aby bol schopný správu dešifrovať. Pre komerčné šifrovacie schémy musí byť metóda verejne známa. Ochrana utajenia kľúča je rozhodujúca.

Integrita zabezpečuje, že správy sú doručené bez zmien.

V kontexte komunikačnej bezpečnosti to znamená schopnosť mať istotu, že prijatá správa nebola zmenená nijakým spôsobom a je zhodná so správou, ktorá bola odoslaná. Bajty kontrolnej postupnosti rámca (FCS) sú príkladom kontroly integrity, ale tieto nie sú považované za zabezpečené. Štandardné bajty FCS nie sú vypočítavané cez nešifrovaný text správy a chránené šifrovaním. Namiesto toho sa vypočítavajú cez šifrovaný text použitím známej metódy a vysielané neupravené (nezašifrované). Bajty FEC pomáhajú identifikovať pakety, ktoré boli náhodne poškodené pri prenose. Útočník však môže spätne vypočítať štandardnú FEC napríklad na zatajenie jeho úmyselnej modifikácie paketu, ktorý zachytil a opakovane odoslal. Ťažšie je pre útočníka správne spätne vypočítať kontrolnú postupnosť integrity alebo zabezpečovaciu hašovaciu funkciu, čo je spoľahlivejší test integrity správy.

Koncept integrity je niekedy rozšírený tak, aby zahŕňal aj verifikáciu, že zdroj správy je rovnaký ako oficiálny. Časové značky a čísla postupností správy môžu chrániť proti „útokom prehrávok“, ale tieto opäť nie sú považované za bezpečné, iba ak by boli chránené šifrovaním.

Bezpečnosť je vždy relatívna, nikdy nie absolútna. Pre každú obranu existuje (alebo onedlho bude) úspešný útok. Pre každý útok existuje (alebo onedlho bude) úspešná obrana. Len čas a úsilie sú reálnym problémom. Čím lepšia obrana, tým viac času a úsilia zaberie prelomenie.

Správna obrana je taká, ktorá je vyvážená a ktorá sa prispôsobuje predpokladanému rozsahu útokov. Vyváženie je dôležité z dvoch hľadísk. Prvé znamená, že aj najslabšia linka musí byť dostatočne bezpečná. Druhé, že pasívne prvky na autentifikáciu, šifrovanie a kontrolu integrity musia byť zálohované aktívnymi prvkami ako je monitorovanie a sledovanie pokusov o prielom, disciplína údržby bezpečnosti a tak ďalej. Správna obrana je taká, ktorá vyžaduje od útočníkov na prelomenie práve trochu viac času a úsilia, ako sú oni ochotní na to vynaložiť. Bezpečnostné opatrenia zvyšujú náklady a obmedzujú ochrancu. Tak ako pri každom podnikaní, rozhodnutie o týchto zmenách treba robiť s otvorenými očami.

5.2 Diskrétnosť a šifrovanie

Diskrétnosť (ochrana pred neautorizovaným prístupom k obsahu správy) sa dosahuje ochranou obsahu dát pomocou šifrovania. Šifrovanie je v sieťach WLAN voliteľné, ale bez neho akékoľvek zariadenie daného štandardu v dosahu môže čítať všetky prenášané správy.

Existujú tri staršie generácie bezpečnosti prístupov pre siete WLAN. Od konca 90-tych rokov prešli bezpečnostné algoritmy Wi-Fi niekoľkými aktualizáciami, pričom staršie algoritmy boli nahradené podstatne novelizovanými novými algoritmami. Chronologický prehľad ich zavedenia je nasledujúci:

- WEP (Wired Equivalent Privacy - drôtový ekvivalent utajenia)
- WPA (Wi-Fi Protected Access – chránený prístup Wi-Fi)
- WPA2 (Wi-Fi Protected Access, version 2 - chránený prístup Wi-Fi, verzia 2)

WEP

WEP bol ratifikovaný ako bezpečnostný štandard Wi-Fi v septembri 1999. Prvé verzie WEP neboli veľmi prísne, dokonca boli čoskoro uvoľnené, lebo obmedzenia USA na export rôznych šifrovacích technológií obmedzovali výrobcov zariadení len do 64 bitového šifrovania. Keď boli obmedzenia sprísnené, došlo k zvýšeniu na 128 bitov. Napriek zavedeniu 256 bitového šifrovania WEP, 128 bitové zostáva jednou z najbežnejších implementácií.

Napriek revidovaniu algoritmu a zväčšeniu veľkosti kľúča boli časom v štandarde WEP zistené početné bezpečnostné trhliny a ako sa zvyšoval výpočtový výkon, bolo stále ľahšie ich využívanie. Už v roku 2001 sa overoval koncept odolnosti a v roku 2005 urobila FBI verejnú demonštráciu (v snahe zvýšiť povedomie o slabinách WEP), kde získala za niekoľko minút heslá WEP pomocou voľne dostupného softvéru.

Napriek rôznym zlepšeniam, sústavnej práci a iným pokusom podporiť systém WEP zostáva veľmi zraniteľný. Systémy spoliehajúce sa na WEP by mali byť aktualizované alebo ak bezpečnosť nebola aktualizovaná, jedinou možnosťou je výmena. Aliancia Wi-Fi oficiálne stiahla WEP v roku 2004.

WPA

Podľa zistených zraniteľností vo WEP obchodná skupina Aliancie WiFi zaviedla na začiatku roku 2003 WPA. Najbežnejšou konfiguráciou WPA je WPA-PSK (Pre-Shared Key – predbežne spoločne využívaný kľúč). Kľúče používané vo WPA sú 256-bitové, čo je podstatné zvýšenie v porovnaní so 64-bitovými a 128-bitovými kľúčmi použitými v systéme WEP.

Niektoré z výrazných zmien implementovaných do WPA zahŕňa kontrolu integrity správy (na určenie toho, či útočník zachytil alebo pozmenil pakety prenášané medzi prístupovým bodom a účastníkom) a protokol integrity dočasného kľúča TKIP

(Temporal Key Integrity Protocol). TKIP využíva systém zmeny kľúča po každom pakete, čo bolo podstatne bezpečnejšie ako pevný kľúč používaný v systéme WEP. TKIP bol neskoršie nahradený štandardom zlepšeného šifrovania AES (Advanced Encryption Standard).

Napriek veľmi výraznému zlepšeniu WPA v porovnaní s WEP, strašidlo WEP prenasledovalo WPA. TKIP (základný komponent WPA) bol navrhnutý tak, aby ľahko prechádzal aktualizovaným firmvérom zariadení využívajúcich WEP. To však spôsobilo, že niektoré prvky systému WEP museli byť opätovne využívané.

WPA, tak ako jeho predchodca WEP, bol predvedený pri oboch konceptoch odolnosti a využili sa verejné demonštrácie zraniteľnosti pri vstupe do prebiehajúceho spojenia. Zaujímavé je, že proces pri ktorom je WPA obyčajne porušený, nie je priamym útokom na algoritmus WPA (hoci takýto útok bol úspešne demonštrovaný), ale pri útokoch na prídavný systém pracujúci mimo WPA-chránené nastavenie Wi-Fi - WPS (Wi-Fi Protected Setup) navrhnuté tak, aby pripojenie linkových zariadení k moderným prístupovým bodom bolo jednoduchšie.

WPA2

WPA bol v roku 2006 oficiálne nahradený systémom WPA2. Jedným z veľmi významných rozdielov medzi WPA a WPA2 bolo povinné použitie algoritmov zlepšeného štandardu šifrovania AES a zavedenie protokolu autentifikačného kódu blokovo zreťazených správ - CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) ako aj náhrady za TKIP (stále zachovávaného vo WPA2 ako havarijný systém a pre interoperabilitu s WPA).

V súčasnosti je citlivosť primárnej bezpečnosti v systéme WPA2 neznáma a vyžaduje útočníka, ktorý už má prístup k sieti Wi-Fi s cieľom získať prístup k určitým kľúčom a potom opakovať útok proti iným zariadeniam na sieti. Bezpečnostné implikácie ako také sú pri známej zraniteľnosti WPA2 skoro celkom limitované sieťami podnikovej úrovne a zasluhujú si veľmi málo praktického uvažovania vzhľadom na bezpečnosť domácich sietí.

Žiaľ, tá istá zraniteľnosť, ktorá bola najväčšou dierou v pancieri WPA, útočný vektor cez chránené nastavenie WiFi (WPS), zostáva aj v moderných prístupových bodoch s WPA2. Hoci vlámanie sa do zabezpečenej siete WPA/WPA2 s využitím jej zraniteľnosti vyžaduje 2-14 hodín trvalého úsilia s moderným počítačom, je to stále opodstatnená záležitosť bezpečnosti a WPS musí byť zablokované. Ak je to možné, firmvér prístupového bodu by mal signalizovať distribúcii, že nemôže dokonca podporovať WPS, lebo útočný vektor je celkom odlišný.

Nasleduje základný zoznam hodnotenia súčasných bezpečnostných metód WiFi, zoradených od najlepšej po najhoršiu:

1. WPA2 + AES
2. WPA + AES
3. WPA + TKIP/AES (TKIP je tu ako havarijná metóda)

4. WPA + TKIP
5. WEP
6. Otvorená sieť (bez zabezpečenia)

Ideálne má byť chránené nastavenie WiFi (WPS) zablokované a úroveň bezpečnosti nastavená na WPA2 +AES.

6 Výhody a nevýhody

Bezdrôtové siete majú rad kľúčových výhod v porovnaní s drôtovými sieťami ako mobilita, nižšie náklady a adaptabilita. Ale majú aj určité nedostatky, napríklad v bezpečnosti. Nižšie sú uvedené hlavné výhody a nevýhody bezdrôtových sietí v porovnaní s drôtovými sieťami.

Nasledujúci zoznam sumarizuje výhody bezdrôtových sietí.

Zlepšená efektívnosť

Zlepšenie dátových komunikácií vedie k rýchlejšiemu prenosu informácií v podnikaní a medzi partnermi a zákazníkmi. Napríklad predajcovia môžu diaľkovo kontrolovať hodnoty akcií a ceny namiesto volaní.

Lepšie pokrytie a mobilita

Drôty vás pripútavajú k jednému miestu. Byť bezdrôtový znamená, že môžete slobodne zmeniť svoju polohu bez straty vášho pripojenia, bez nutnosti použiť prídavné káble alebo adaptéry pre vstup do kancelárskych sietí.

Flexibilita

V prípade kancelársky založených bezdrôtových sietí pracovníci môžu byť pripojení k sieti bez toho, aby sedeli pri určených počítačoch a môžu pokračovať v produktívnej práci aj keď sú mimo kancelárie. To môže viesť ku novým štýlom práce, takým ako práca doma alebo priamemu prístupu k spoločným dátam hoci na stanovišti zákazníka.

Šetrenie nákladov

Bezdrôtové siete môžu byť ľahšie a lacnejšie na inštalovanie, špeciálne v pamiatkovo chránených budovách alebo keď vlastník nechce povoliť inštalovanie káblov. Zrieknutie sa vodičov a káblov prináša zníženie nákladov. Toto je vynikajúce pri kombinácii činiteľov relatívne nízkej ceny smerovačov, nepotrebnosti výkopov, vŕtania a ukladania vodičov vnútri stien alebo iných metód, ktoré môžu vyžadovať vytvorenie fyzických spojení. A naviac nie je potrebná údržba vedení.

Adaptabilita

Rýchla a jednoduchá integrácia zariadení do siete a flexibilita pri modifikácii inštalácie.

Nové možnosti/aplikácie

Bezdrôtové prepojenie dovoľuje ponúknuť nové produkty alebo služby. Napríklad v mnohých odletových halách letísk, železničných staniciach, hoteloch, kaviarňach a reštauráciách sú inštalované prístupové miesta k službám bezdrôtového pripojenia, umožňujúce mobilným účastníkom pripojiť ich zariadenia k ich domácej kancelári počas cestovania.

Existujú určité nevýhody súvisiace s použitím bezdrôtových sietí.

Bezpečnosť

Bezdrôtový prenos je zraniteľnejší pri útoku neoprávnených používateľov, náklady na príslušný dohľad však zaručujú bezpečnosť.

Problémy pri inštalácii

Ak v tej istej budove okrem vás používajú bezdrôtovú technológiu aj iní alebo sú tam prítomné aj iné zdroje rádiových signálov, môžete byť rušení interferenciou. Môže to spôsobiť zhoršenie spojenia alebo v extrémnych prípadoch úplné prerušenie bezdrôtovej komunikácie.

Pokrytie

V niektorých budovách môže byť zabezpečenie rovnomerného pokrytia veľmi ťažké, vedie to k vzniku nepokrytých miest, kde signál nie je k dispozícii. Napríklad pri výstavbe boli použité oceľové výstužné materiály a vy môžete len veľmi ťažko zvýšiť použitú frekvenciu.

Prenosové rýchlosti

Bezdrôtový prenos môže byť pomalší a menej efektívny ako v drôtových sieťach. V rozľahlých bezdrôtových sieťach býva chrbticová sieť obyčajne častejšie drôtová ako bezdrôtová.

7 Aplikácie

Začleňovanie bezdrôtovej komunikácie do vložených systémov stále rastie. Forrester Research, spoločnosť zameraná na zmeny technológie podnikateľských implikácií oznámila, že za niekoľko málo rokov viac ako 95% zariadení používaných na prístup do internetu budú nepočítačové zariadenia, ktoré používajú vložený (vnorený) systém.

Existuje mnoho aplikácií pre vložené zariadenia s Wi-Fi rozhraním:

- Priemyselné procesy a riadiace aplikácie, pre ktoré sú drôtové pripojenia príliš drahé alebo nevyhovujúce, napríklad nepretržite sa pohybujúce stroje.
- Tiesňové aplikácie, ktoré vyžadujú okamžité a krátkodobé nastavenie, také ako bojisko alebo havarijné situácie.
- Mobilné aplikácie, také ako sledovanie majetku.
- Dohľadové kamery (snáď nechcete aby ich ľahko zbadali, káblové prepojenie sa dá ťažko skryť).
- Vo vertikálne organizovaných štruktúrach ako sú medicína, vzdelávanie a výroba.
- Komunikácia s inými Wi-Fi zariadeniami ako sú laptopy alebo PDA.
- Aplikácie stroj-stroj M2M (Machine to Machine)

A ohľadom na tú poslednú, termín stroj-stroj (M2M) odkazuje na technológie, ktoré umožňujú bezdrôtovým aj drôtovým systémom komunikovať so zariadeniami rovnakého typu. Druhou charakteristikou komunikácie M2M je, že toto prepojenie umožňuje primárne automatickú komunikáciu medzi vzdialenými, odľahlými strojmi na jednej alebo niekoľkých úrovniach aplikácií centrálneho manažmentu. To zabezpečuje monitorovanie a riadenie v reálnom čase bez nutnosti ľudského zásahu.

Podľa ABI Research, korporácie zameranej na technologický výskum a poradenstvo, viac ako 30 biliónov zariadení má byť bezdrôtovo pripojených ku Internetu vecí (ako aj Internet of Everything - Internetu všetkého) do roku 2020.

V prostredí M2M sú dve hlavné triedy prepojenia: krátky dosah a rozľahlá oblasť. Hlavná technológia pre rozľahlé oblasti využíva vložené bunkové moduly na pripojenie vzdialených zariadení k internetu alebo aplikačným serverom. Bunkové moduly obsahujú veľa rovnakého vybavenia aké je možné nájsť aj v bunkovom telefóne, vrátane hlasovej a dátovej komunikácie a sú ideálne pre vložené aplikácie.

Aplikácie M2M môžeme nájsť vo veľkom rozsahu v priemysle a zahŕňajú: automatické čítanie meradiel AMR (automatic meter reading), predajné automaty, terminály predajných bodov POS (point of sales), doprava a logistika (manažment flotily), starostlivosť o zdravie, bezpečnostná technológia a iné aplikácie.

8 Závery

Technológie bezdrôtových sietí pripájajú bez vodičov naše vysokotechnologické zariadenia buď k vysokorýchlostnej sieti alebo iným zariadeniam. V minulosti museli byť vodiče pokladané z miestnosti do miestnosti alebo z poschodia na poschodie. Ceny za zriadenie boli vysoké a čas na zriadenie drôtovej siete bol oveľa väčší ako u bezdrôtovej siete s inými prvkami.

Dnes sa zriadenie a nastavenie bezdrôtovej siete dá urobiť reálne ľahko a je k dispozícii veľa bezdrôtových produktov, z ktorých si môžete vybrať. Okrem toho existuje mnoho dostupných zdrojov, ktoré vám môžu pomôcť pri nastavení a konfigurácii bezdrôtovej siete keď je to potrebné.

Je možné vybrať rôzne technológie, ktoré budú najlepšie vyhovovať požiadavkám aplikácie a dosah prenosu dát môže byť od niekoľko metrov do niekoľkých kilometrov. Bezdrôtové siete určite ponúknu nové možnosti pre priemyselné riešenia, ale tieto musia byť implementované so špeciálnym dôrazom na bezpečnosť.

Porovnanie typov bezdrôtových sietí

Typ siete	Názov	Štandard	Frekvenčné pásmo	Nominálny dosah	Maximálna bitová rýchlosť
WPAN	Bluetooth	IEEE 802.15.1	2,4 GHz	10 m	720 kbit/s
	IrDA	IrDA	Infračervené okno 850-900 nm vlnová dĺžka	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 a 6-8,5 GHz (Európa)	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 a 10-66 GHz	50 km	70 Mbit/s
WWAN	Bunková	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
	Družicová	DVB-S2	3-30 GHz	> 50 km	60 Mbit/s