Bezdrátové sítě

Úvod

Bezdrátové sítě, ačkoliv je to jednoduché téma, je více komplexní, než se na první dojem může zdát. Zahrnuje nejen Wifi, ale i Bluetooth, Infrared apod. Skript obsahuje hodně standardů a věcí, které nejsou na poprvé logicky odvoditelné a je potřeba si i něco pamatovat. Na druhou stranu jsou to informace, které jsou použitelné i v reálném životě. Lochman vám dá vybrat jednu technologii, kterou pak budete popisovat. Doporučuje, aby si člověk nevybral Wifi, protože ji porota umí. Doporučuji Bluetooth.

Definice

Bezdrátová síť je typ počítačové sítě, ve které se účastníci spojení připojují pomocí bezdrátových technologií. Vše, co je zde popsáno se pohybuje v rámci první síťové vrstvy – fyzické.

Použití

Je důležité si ze začátku definovat proč bychom vůbec chtěli používat bezdrát a jaké jsou jeho výhody a nevýhody. Musíme si také uvědomit, že natažení kabelů prostě není vůbec možné z důvodu např. historických budov, využívání dočasných prostor či veřejných prostranství atd. Také je potřeba vzít v úvahu do jaké budovy chceme nebo nechceme bezdrátovou technologii dát. Z jakého materiálu je budova postavena? Má vůbec místo na kabely? Vyplatí se je nám tam dát?

Klady

1. **Bez kabeláže** – Není nutné všude nosit kabely nebo to není možné (Pohyblivé objekty)
2. **Dosah a dostupnost** – pokrytí velkého prostoru (Open-space kanceláře)
3. **Efektivní pro připojení více zařízení** – Bez rozvodu kabelů
4. **Flexibilita** – práce odkudkoliv
5. **Levnější**

Zápory

1. **Bezpečnostní riziko** – je jednoduší prolomit heslo a dostat se do sítě než magickým způsobem obejít zablokovaný port na ethernet
2. **Pomalejší rychlost** – napojení přímo je rychlejší než vzduchem
3. **Omezení regulacemi** – elektro-smog
4. **Malá šířka pásma v porovnání s metalickou**
5. **Náchylnost na počasí**

Konkluse

Největší výhoda spočívá již v samotném názvu – Bezdrátové. Nemusíme tahat hromadu drátů složitě je napojovat, konfigurovat, mít pořád otevřené porty na switchích atd. Představa, že každý náš Smartphone bude připojen kabelem do internetu asi v dnešní době není moc reálná. S tímto jde ruku v ruce i fakt, že bezdrátové sítě se nám více přizpůsobí a jsou daleko levnější než rozsáhlé rozvody kabelů.

Velká nevýhoda je bezpečnost. Kdokoliv odkudkoliv bez přístupu k drátu se nám může dostat do sítě, pokud prolomí šifrování, nebo pokud zneužije nějaké chyby na naší straně. V drátové síti je jednoduší pouze zablokovat prázdné/nepoužívané porty. Druhá největší nevýhoda je pomalá rychlost, která je daní za přístupnost.

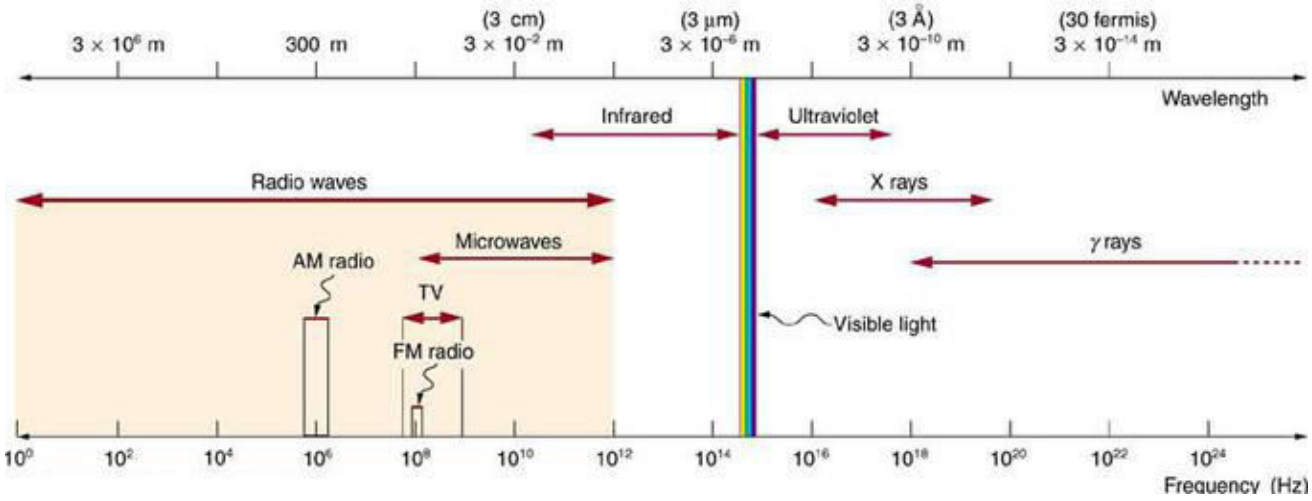
Rozdělení bezdrátových sítí

1. Podle média
   1.1. Optické
      1.1.1. IrDA
      1.1.2. Ronja
      1.1.3. Laser – podobné Ronja, zastaralé
   1.2. Radiové
      1.2.1. Bluetooth
      1.2.2. Wimax
      1.2.3. Wifi
      1.2.4. Satelit
2. Podle velikosti sítě
   2.1. WPAN – Osobní sítě (Bluetooth, Infračervené)
   2.2. WLAN – Místní sítě (Access point do internetu – Wi-Fi, point-to-point connection)
   2.3. WMAN – Metropolitní – Spojují několik WLAN dohromady
   2.4. WWAN – Worldwide – velké oblasti, města s předměstími, point-to-point
3. Podle přístupu k přenosového médiu
   3.1. CSMA/CA – (viz. CSMA/CA)
   3.2. CSMA/CD – (viz. CSMA/CD)
   3.3. Token ring
4. Podle komunikace
   4.1. Client to Client - Pear to Pear (Hruška k hrušce) – všechny uzli jsou rovnocenné a komunikují přímo (Torrenty, Bitcoin)
   4.2. Client – server - Odděluje klienta a server, nejsou rovnocenní, klient žádá službu od serveru (Email, Web)

Klíčové pojmy

Elektromagnetický smog – neionizující elektromagnetické záření – záření pomocí kterého se šíří wifi. Vytváří ho každé zařízení, ale v menším množství.

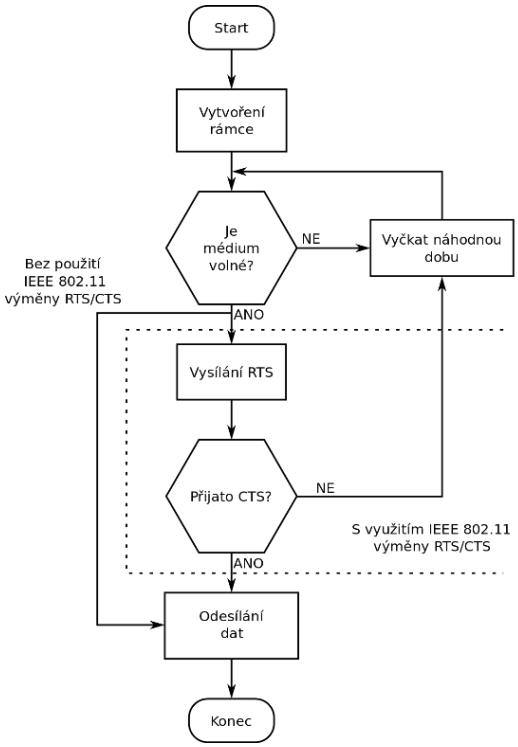
Elektromagnetické spektrum



Tento obrázek shrnuje elektromagnetické záření různých délek. Ty jsou pro nás důležité, protože právě po nich se elektromagnetické záření šíří.

Rozdělení

Rádiové vlny (Hz – 1GHz) – velký dosah, centrální kontrola přidělování a využívání (AM, FM, DAB, GSM, 3G)
Mikrovlny (1 – 300GHz) – lze soustředit do paprsku, závislé na počasí (WLAN, satelitní, některé rádiové spoje)
Infračervené (300GHz – 400 T_{era}Hz) – komunikace na krátkou vzdálenost (notebooky, tiskárny), neprojdou skrz překážky
Viditelné záření (400 – 800THz) – úzký světelný paprsek, závislost na atmosférických podmínkách



Licenční pásma

Pokud si chcete na založit rádio nebo mobilní síť, musíte si koupit nové volné pásmo, kde nikdo nevysílá. Neplatí se za vysílání, ale pouze za možnost použití daného pásma. Vysílání na pásmu si musíte zařídit sami. Jedná se o velmi kvalitní pásmo. Obecně lze říci, že čím nižší frekvence, tím je její použití vhodnější na delší skok. Současně ale platí, že čím nižší frekvence tím je vyšší poplatek za užívání. Logicky tedy za kratší skoky zaplatíte nižší poplatek. Skoro každá země má odlišné frekvence.

Bezlicenční pásmo – ISM (Industrial, Scientific and Medical)

Počet uživatelů není omezen. Je hodně rušen. Neplatí se. Taky máte mikrovlnku a neplatíte si pásmo :c

Řízení přístupu

CSMA (Maturitní otázka 12.)

Jsou protokoly, které zabraňují kolizi na síti.

CSMA/CA — Carrier Sense, Multiple Access with Collision Avoidance

Nezachytává kolizi a odvysílá rámec i presto že bude vysílání opakovat.

CSMA/CD - Carrier Sense Multiple Access with Collision Detection

Současně kontroluje přenosové médium. Pokud zjistí kolizi, zastaví vysílání a počká.

Optické

IrDA Infrared Data Association

Bezdrátová komunikace pomocí infračerveného světla. Byl vytvořen pro přenos dat pomocí mobilních zařízení. Dosah má kolem 1 m.
Vysílá infračervené světlo (875 nm) pomocí LED diody a přijímá pomocí fotodiody.
Half-duplexní komunikace – jedno zařízení určitě směr dat.

Ronja Reasonable Optical Near Joint Access

Je to optické zařízení, které umožňuje propojit 2 body na vzdálenost až 1.5 km při zachování rychlosti 10 MB/s. Lze připojit do Ethernetové karty. Bylo vyvinuto v České republice.
Ronja pracuje s červeným paprskem. Má opět usměrněnou LED čočkou a přijímací fotodiodu.

Rádiové

Je to elektromagnetického záření s vlnovými délkami od 1 milimetru až po tisíce kilometrů. Vzniká mimo jiné v obvodu střídavého proudu, k němuž je připojena anténa. Rychlost šíření rádiových vln je v prostoru přibližně rovna rychlosti světla ve vakuu. V případě jiných prostředí závisí na indexu lomu.

FWA Fixed Wireless Access

Bezdrátová síť FWA představuje tzv. řešení poslední míle, kdy poskytovatel telekomunikační služby má možnost přímého přístupu ke koncovým zákazníkům. Význam slova fixed v názvu značí a předpokládá, že přípojka koncového uživatele bude fixní (stálá). To je výrazný rozdíl od sítí typu GSM. Jedná se spíše o druh sítě než standard.

WiMAX (nic od Nintenda tho)

Podobné k Wifi a měla nahradit DSL. Maximální teoretická rychlost je 75 Mbit/s, kterou sdílí všichni uživatelé k základové stanici. Bez potřeby přímé viditelnosti má ve venkovských oblastech dosah 50 km a v husté zástavbě 3-5 km. Jedna základová stanice je schopna pojmout až 500 uživatelů ve zhruba 15km okruhu.

Satelitní spoje

Ve výšce 36 000Km, aktivní pasivní, kdykoliv, rychlost velká, armáda a věda, větší zpoždění přenosu, geostacionární družice – orbit.

Bluetooth IEEE 802.15.1

Ověřený standard pro bezdrátovou komunikaci pro spojení dvou a více zařízení. Umí zpracovat kolem 79 frekvencí, co nejblíže pásmu 2.4GHz (stejně jako mikrovlnka) díky kterým může napojit více zařízení, aniž by se rušily. Bylo vydáno několik verzí a všechny. Nejnovější je pátá, která umožňuje rychlost 2 Mbit/s. Bluetooth transmitery mají malý dosah, a proto jsou teoreticky nejbezpečnější. Existuje několik verzí, které se liší dosahem a rychlostí. Frekvenční multiplex (více zařízení najednou), Harald „Bluetooth“ Gromsson. Vyhledává samo jednotlivá zařízení. S připojenými komunikuje jako se slaves.

Proces

1. Automaticky detekuje nové zařízení (musí být v „discovery módu“)
2. Zařízení se připojí pomocí MAC adres a vymění si informace
3. Je požadováno heslo, které se na obou zařízeních musí schválit
4. Komunikace je vytvořena

Piconet network – nejednoduší síť kterou Bluetooth vytváří
Scatter-net network – více spojených piconetů

Security modes

1. First security mode – není nijak chráněn (Podpora pouze do Bluetooth 2.0 +)
2. Second security mode – centralizuje spojení a spravuje spojení s ostatními zařízeními
3. Third security mode – vytváří bezpečné spojení ještě před spojením, pro šifrování a přístup používá oddělené klíče
4. Forth security mode – nové vylepšení které umožňují lepší výměnu ověřovacích klíčů a klíčů pro přístup (je nutný)

Wi-Fi IEEE 802.11

Je technologie, která umožňuje vytvořit lokální bezdrátovou síť (WLAN). Většina dnešních zařízení dokáže komunikovat pomocí tohoto standardu (televize, počítače, notebooky, telefony...) a připojit

se na bezdrátový access point. Access point (nebo hotspot) je velký asi 20 m a mohou ho blokovat stěny apod. Normální Wi-Fi síť komunikuje na pásmu 2.4GHz, ale v dnešní době 5Ghz začíná být standard. Stejně jako mikrovlnka, takže ano, i mikrovlnka může rušit Wifi. Čím větší počet GHz tím větší je rychlost, ale je jednoduší zablokovat signál, což je problém třeba u 60GHz Wifi, která se kvůli tomuto problému skoro nepoužívá (to samé jako u všech pásem).

Zabezpečení

Jedno z nejjednodušších zabezpečení je přestat vysílat SSID (broadcast) a tím schovat wifi před běžnými uživateli nebo udělat „white-list“, kde nastavit přímo MAC adresy uživatelů, kteří se mohou připojit. Samozřejmě existuje mnoho důvodů, proč toto není žádoucí, a proto se používají hesla a další šifrování, abychom omezili přístup na naši síť.

Heslo

1. Bez hesla – To prostě nechceš.
2. Wired Equivalent Privacy (WEP) – bylo prvotní zabezpečení pro Wifi, dnes ale již není bezpečné, protože je známo pro své chyby. Jsou vytvořené programy, které jednoduše umí toto zabezpečení prolomit.
3. Wi-Fi Protected Access (WPA) – (Temporal Key Integrity Protocol - IEEE 802.11i) používal 64-bit, nebo 128-bit encryption key, který musel být manuálně zadán. Měl hodně problémů a jeho implementace nebyla snadná. Dnes kvůli vadám je stejně (ne)bezpečný jako WEP.
4. Wi-Fi Protected Access II (WPA2) – Vylepšuje WPA a přidává nový standard AES, který je označen jako zcela bezpečný. Je povinný pro všechna nová zařízení.
5. Wi-Fi Protected Access 3 (WPA3) “IEEE 802.11-2016” – náhrada za WPA2. Dokáže používat až 192bit šifrování a bude používat jiný standard pro výměnu klíče. Stále ve vývoji.

Bezpečnostní služby

- Autentizace - hesla
- Řízení přístupu
- Zajištění utajení a důvěrnosti dat - šifrování
- Zabezpečení integrity dat
- Ochrana proti odmítnutí původu zprávy – při nedostatku informací o zdroji
- Šifrování
    - Symetrické – stejný klíč pro šifrování a dešifrování
    - Asymetrické – soukromý a veřejný klíč (BTC hype)

Útoky

- Falšování integrity zdroje
- Man-in-the-middle
- Útoky na hesla
- Odposlech – Sniffing, Spoofing
- DDOS attack

Zdroje

1. https://cs.wikipedia.org/wiki/Bezdr%C3%A1tov%C3%A1_s%C3%AD%C5%A5
2. https://en.wikipedia.org/wiki/Wireless_network
3. http://www.ped.muni.cz/wtech/03_studium/teps/teps-07.pdf
4. https://www.fi.muni.cz/usr/brandejs/PV005/Bezdratove_site_patka.pdf
5. https://cs.wikipedia.org/wiki/Bezdr%C3%A1tov%C3%A1_komunikace
6. https://cs.wikipedia.org/wiki/Bezdr%C3%A1tov%C3%A1_s%C3%AD%C5%A5
7. https://en.wikipedia.org/wiki/Wireless_network
8. https://cs.wikipedia.org/wiki/CSMA/CA
9. https://en.wikipedia.org/wiki/Wireless_network
10. https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=15812
11. https://slideplayer.cz/slide/1956681/
12. http://www.ped.muni.cz/wtech/03_studium/teps/teps-07.pdf
13. https://www.fi.muni.cz/usr/brandejs/PV005/Bezdratove_site_patka.pdf
14. https://managementmania.com/cs/bezdratova-sit
15. https://www.starnet.cz/novinky/vase-domaci-bezdratova-sit
16. https://www.google.com/search?client=firefox-b-d&q=pros+and+cons+wireless+technology
17. https://www.nibusinessinfo.co.uk/content/pros-and-cons-wireless-networking
18. https://en.wikipedia.org/wiki/Electromagnetic_spectrum
19. https://cs.wikipedia.org/wiki/Elektromagnetick%C3%A9_spektrum
20. https://cs.wikipedia.org/wiki/CSMA/CD
21. https://www.google.com/search?client=firefox-b-d&q=MAN
22. https://www.wifi-shop.cz/ptp-spoje-licencovana-pasma-38-ghz_c13172574.html
23. https://en.wikipedia.org/wiki/Infrared_Data_Association
24. https://cs.wikipedia.org/wiki/Peer-to-peer
25. https://cs.wikipedia.org/wiki/Klient-server
26. https://cs.wikipedia.org/wiki/Laser
27. https://cs.wikipedia.org/wiki/Ronja
28. https://www.electronics-notes.com/articles/connectivity/bluetooth/network-pairing-connection.php
29. https://duo.com/decipher/understanding-bluetooth-security