Bezdrátové sítě

Lukáš Patka, 12.12.2007

Dnešní přednáška

- motivace
- bezdrátové přenosy
- licenční, bezlicenční pásmo
- WLAN (wireless local area network): 802.11
  - standardy
  - techniky rozprostřené spektra
  - bezpečnost bezdrátových sítí
  - hw, antény
- WPAN (wireless personal area network): Bluetooth
- bezdrátové sítě na FI MU

Předměty na FI MU

- PA151 - **Soudobé počítačové sítě**
  - DAB, DVB, satelitní komunikace, mobilní sítě, WLAN
- PV169 - **Základy přenosu dat**
  - spojová a fyzická vrstva ISO OSI
- PV183 - **Technologie počítačových sítí**
  - WLAN, WPAN

Proč bezdrátové sítě?

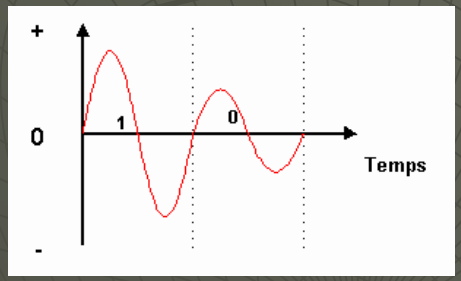
- natažení kabelů není všude možné
  - veřejné prostranství, historické budovy
- kabelové připojení může být nákladné
- poslední míle
- využívání dočasných prostor
- mobilita klientů

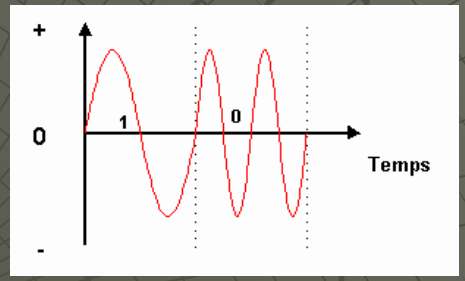
Nevýhody bezdrátových sítí

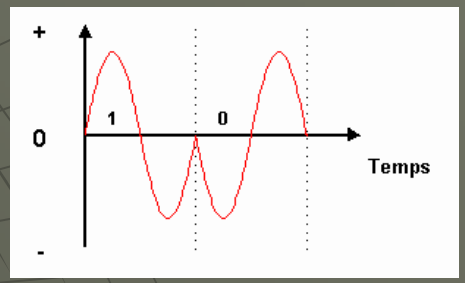
- malá šířka pásma v porovnání s metalickými sítěmi
- omezení stanovená národními regulačními úřady

Bezdrátové přenosy

- data přenášena šířením změn elektromagnetických vlastností prostředí
- bezdrátová média šíří pouze analogové signály
- kódování digitálních dat do analogového signálu: amplitude, frequency, phase-shift keying



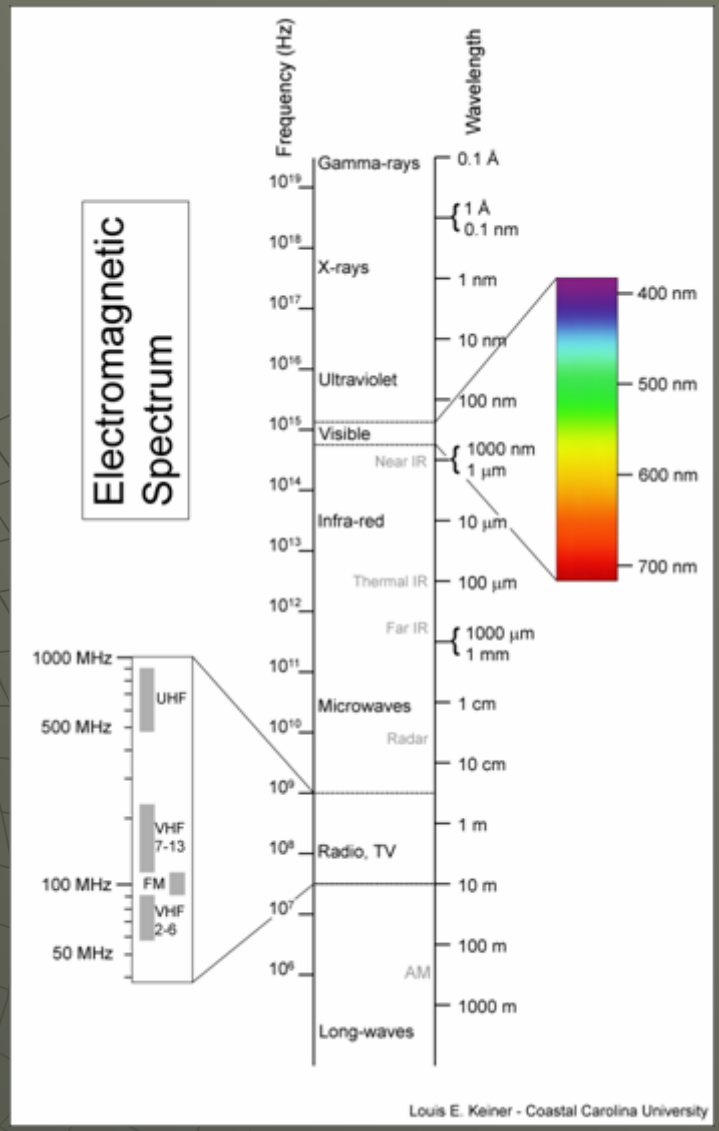




- rychlost přenosu dat je úměrná šířce přenosového pásma
  - Shannonova věta: max. dosažitelná rychlost při dané šířce pásma a daném poměru SNR
    - $C = B \log2(1 + S/N)$
    - $SNRdB = 10\log(S/N)$
  - Nyquistova věta: max. rychlost přenosu dat víceúrovnovým signálem při dané šířce pásma
    - $C = 2B \log2 M$

Elektromagnetické spektrum

- **rádiové vlny**
  - Hz - 1GHz
  - AM, FM rádio, DAB, DVB, DECT, GSM, 3G
  - relativně velký dosah si vynucuje centrální kontrolu přidělování a využívání frekvencí
- **mikrovlny**
  - 1 – 300 GHz
  - WLAN, satelitní spojení, orientované radiové spoje
  - lze soustředit do úzkého svazku
  - závislé na počasí- pohlcovány deštěm
- **infračervené záření**
  - 300GHz - 400 THz
  - komunikace na krátkou vzdálenost (notebooky, tiskárny,..)
  - neprostupují skrz překážky
- **viditelné záření**
  - 400 - 800 THz
  - laserová pojítka
  - úzký světelný paprsek
  - relativně velká závislost na atmosférických podmínkách- déšť, mlha



Regulátoři kmitočtových pásem

- mezinárodní: **ITU** (International Telecommunication Union)
  - Radio Regulations: mezinárodní dohody regulující využití frekvenčních pásem, oběžných drah satelitů
    - http://www.itu.int/publ/R-REG-RR/en
  - World Radiocommunication Conferences
    - kontrola/úprava Radio Regulations, každé 2 roky, 22.10.-16.11. 2007
- Evropa:
  - **CEPT** (European Conference of Postal and Telecommunications Administrations)
    - dohody mají pouze formu doporučení
      - European Common Allocation Online Database: http://apps.ero.dk/ECA/
    - 48 členů, včetně ČR, SR
  - **ETSI** (European Telecommunications Standards Institute)
  - **ECC** (Electronic Communications Committee)
    - sloučení **ERC** (European Radiocommunications Committee), **ECTRA** (European Committee for Regulatory Telecommunications Affairs)
- EU:
  - The European Commission
    - **RSC** (Radio Spectrum Committee)
    - **RSPG** (Radio Spectrum Policy Group)
- ČR:
  - **ČTÚ** (Český telekomunikační úřad)
    - plán přidělení kmitočtových pásem
      - http://www.ctu.cz/1/download/plan-prideleni-kmitoctovych-pasem_1114099610.pdf

Licenční pásmo

- placené, ale garantované
- pásma pro datové sítě – 3,5 GHz, 26 a 28 GHz
- mobilní sítě GSM - 900 a 1800 MHz
- televizní a radiové vysílání
- profesionální datové sítě FWA
- radiové sítě Tetra

Bezlicenční pásmo

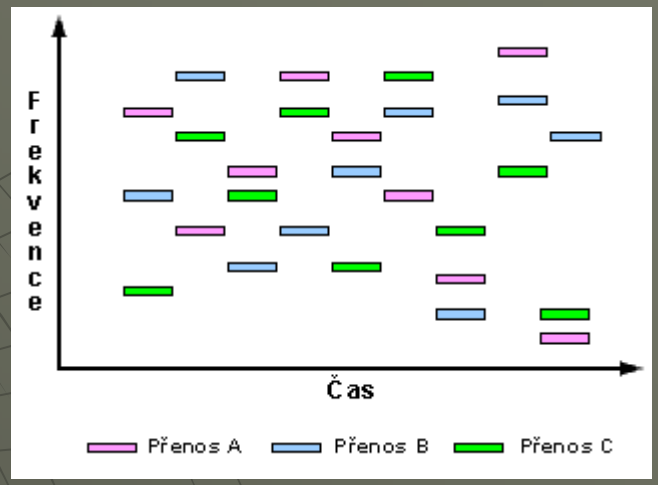
- pásmo ISM (Industrial, Scientific and Medical)
- počet uživatelů není omezen
  - problém rušení
- majitel mikrovlnky nemusí žádat o licenci ☺
- ECA definuje následující frekvenční rozsahy jako ISM:
  - 9-14kHz, 24-24.05GHz, 24.05-24.25GHz, 40.66-40.7MHz, 59.3-62GHz, 433.05-434.79MHz, **2400-2450 MHz**, **2450-2483 .5MHz**, 2483.5-2500MHz, 5725-5830 MHz, 5830-5850 MHz, 5850-5925 MHz, 6765-7000 kHz, 13410-13570kHz, 26175-27500kHz

Rozprostřené spektrum

- tradiční technologie vměstnávají co největší počet signálů do relativně úzkého pásma
- rozprostřené spektrum naopak pomocí matematických funkcí rozptýlí sílu signálu do širokého frekvenčního bloku
- přijímač opačnou operací převede zpět do úzkopásmového signálu
- eliminace interferencí (rušení) úzkopásmových zdrojů
- znesnadnění odposlechu signálu
- zavedení redundance
  - vysílaná zpráva je přenášena pomocí signálů modulovaných na více frekvencích. Tyto signály mohou sloužit (v případě výskytu chyby, rušení) k obnovení původní zprávy

Techniky rozprostřeného spektra

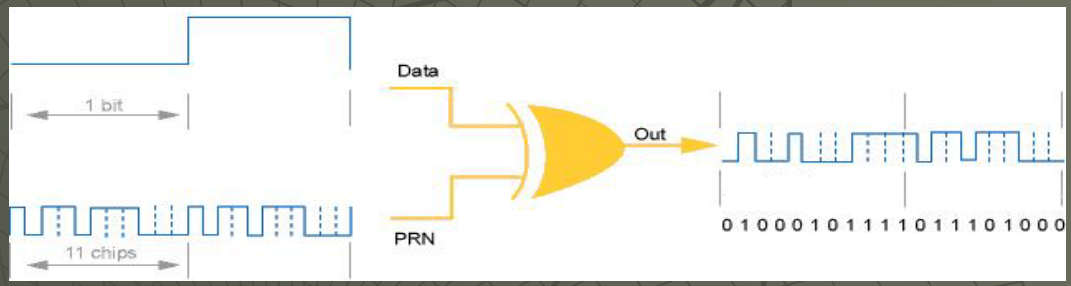
- **FHSS** - *Frequency Hopping Spread Spectrum*
  - nosný signál vysílán po krátkou dobu (max 400 milisekund)
  - přeskočí a pokračuje na jiné frekvenci, to se neustále opakuje
  - posloupnost přeskoků je dána pseudonáhodným generátorem čísel

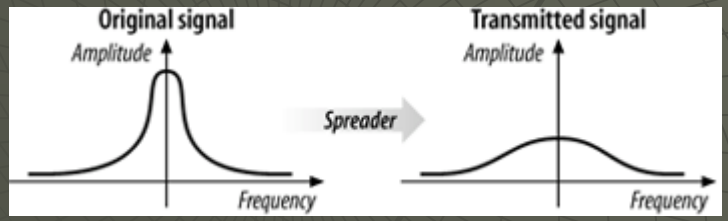


  - frekvenčních pásem 79, šířka 1 MHz
  - teoreticky až 26 paralelně pracujících přístupových bodů, prakticky kolem 15-ti
  - rychlosti 2 Mb/s, modulace Frequency-Shift Keying
  - nejlevnější na výrobu

Techniky rozprostřeného spektra II

- **DSSS** - *Direct Sequence Spread Spectrum*
  - každý bit je transformován do n-bitové sekvence
    - bit XOR pseudonáhodná sekvence

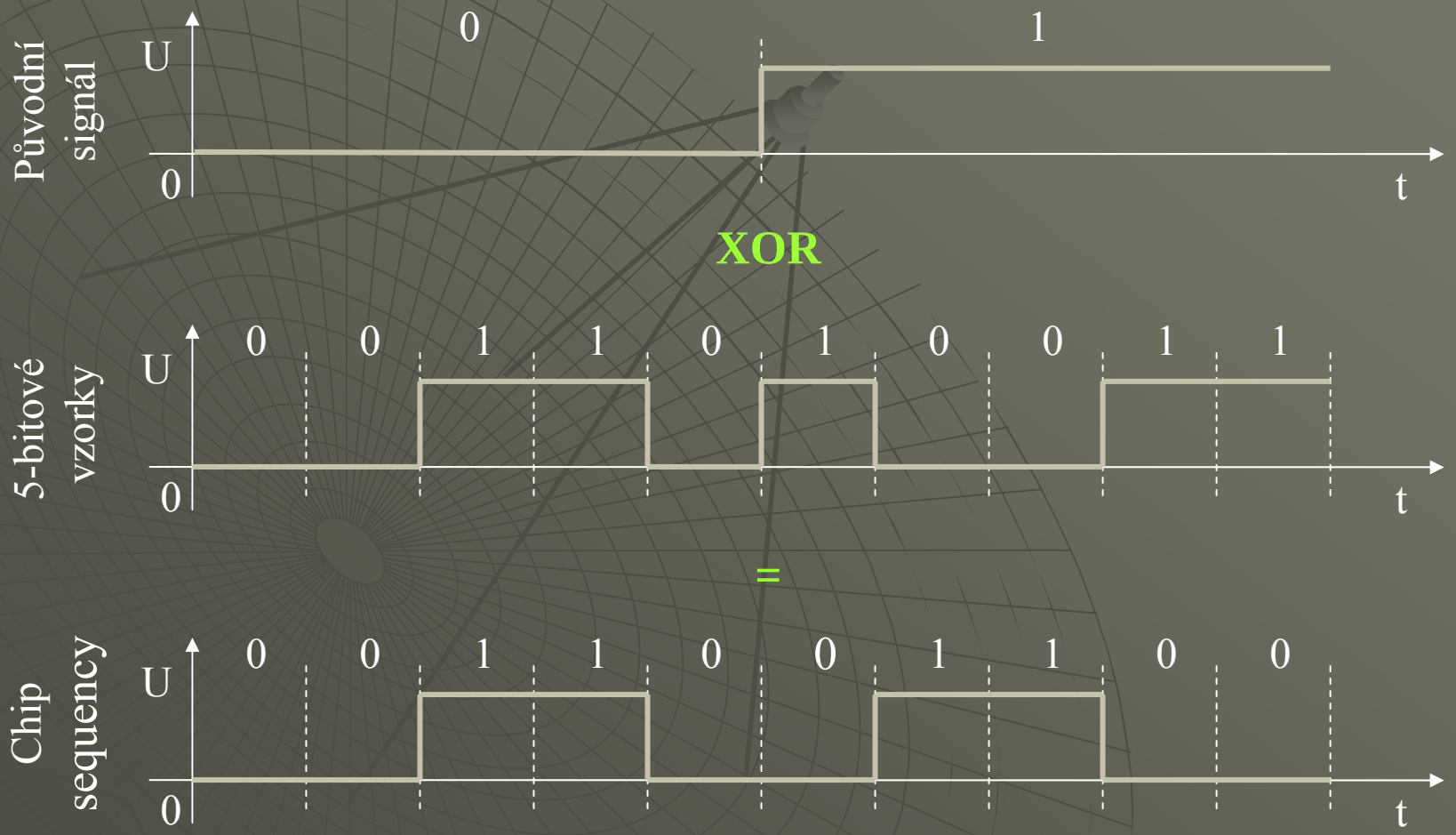




  - základní rychlosti 2 a 1 Mb/s, modulace DPSK (Differential Phase Shift Keying)
  - pro rychlosti 11 a 5,5 Mb/s se používá modulace CCK (Complimentary Code Keying)
  - 802.11, 802.11b

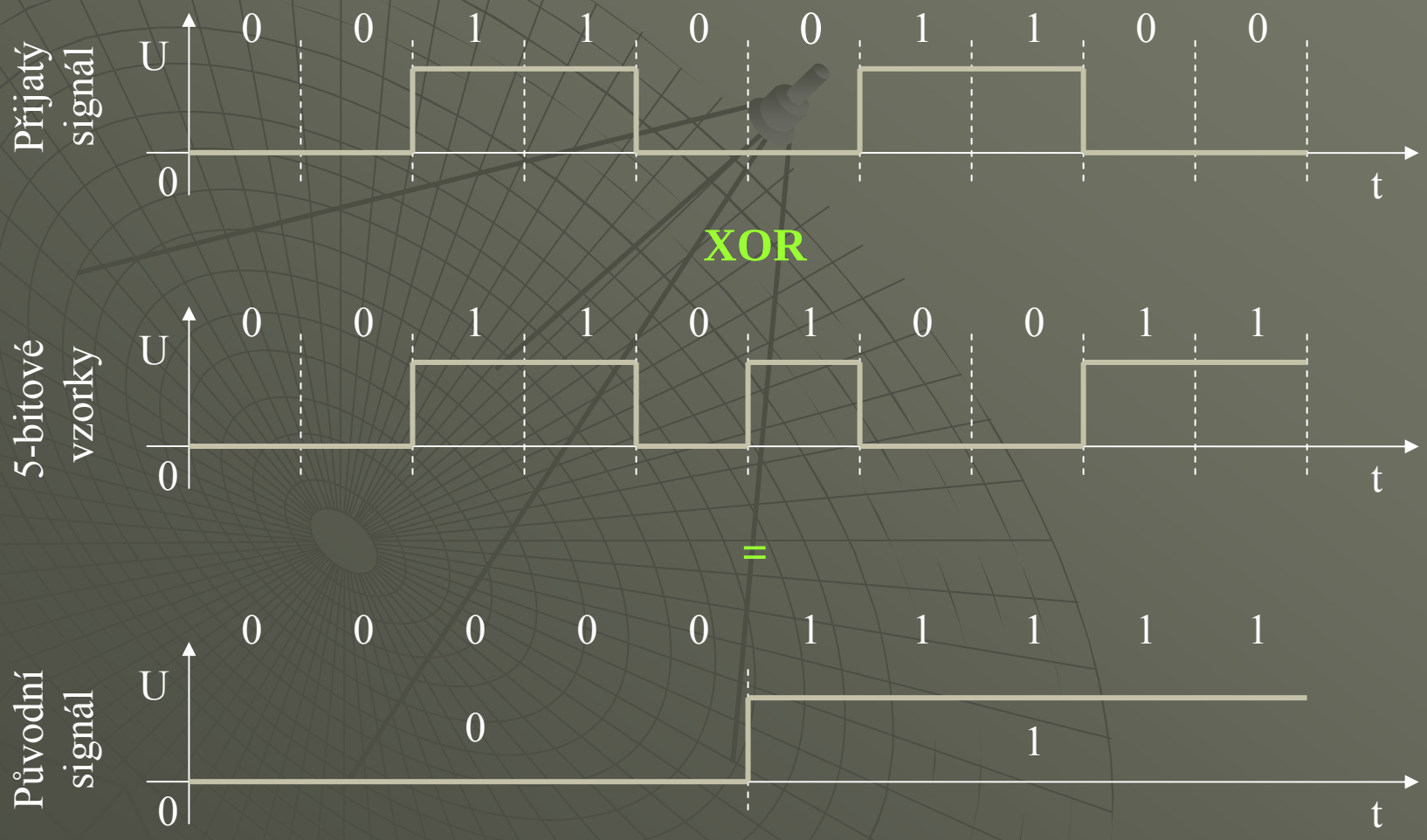
DSSS

- strana vysílače:



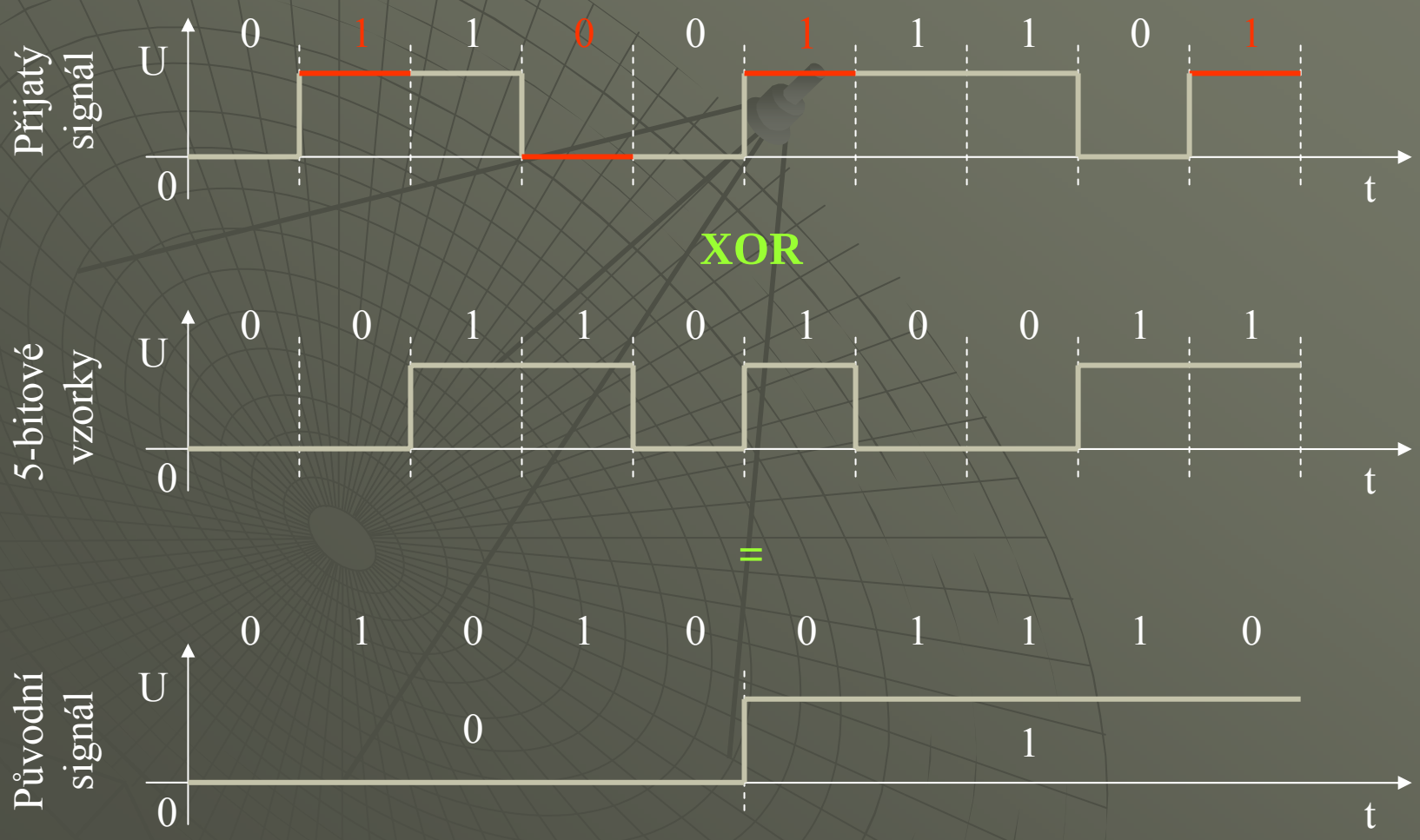
DSSS

- strana přijímače – bezchybný přenos:



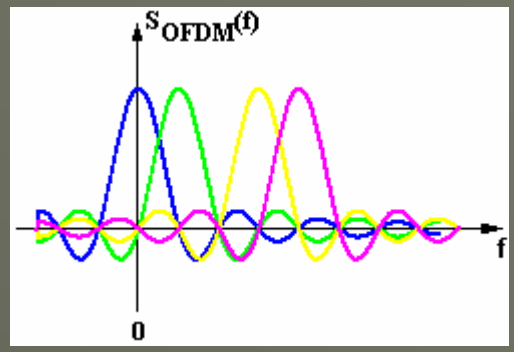
DSSS

- strana přijímače (rušení) - přenos s chybami:



Techniky rozprostřeného spektra III

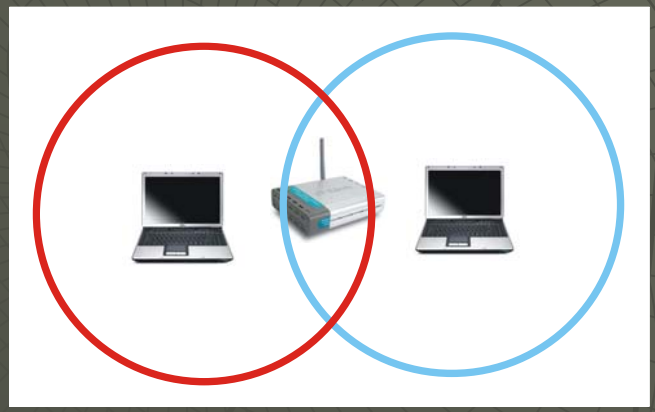
- **OFDM –** *Orthogonal Frequency Division Multiplex*
  - přenosové pásmo se rozdělí na velké množství úzkých kanálů
  - data se v kanálech přenáší relativně pomalu a signál je tak robustnější
  - nosné frekvence jednotlivých kanálů jsou voleny tak, aby modulované datové proudy byly vzájemně ortogonální- eliminuje rušení sousedících kanálů



  - v členitém terénu horší výsledky
  - max. přenosová rychlost, daná součtem všech kanálů, je 54 Mb/s
  - 802.11a, 802.11g

Řízení přístupu

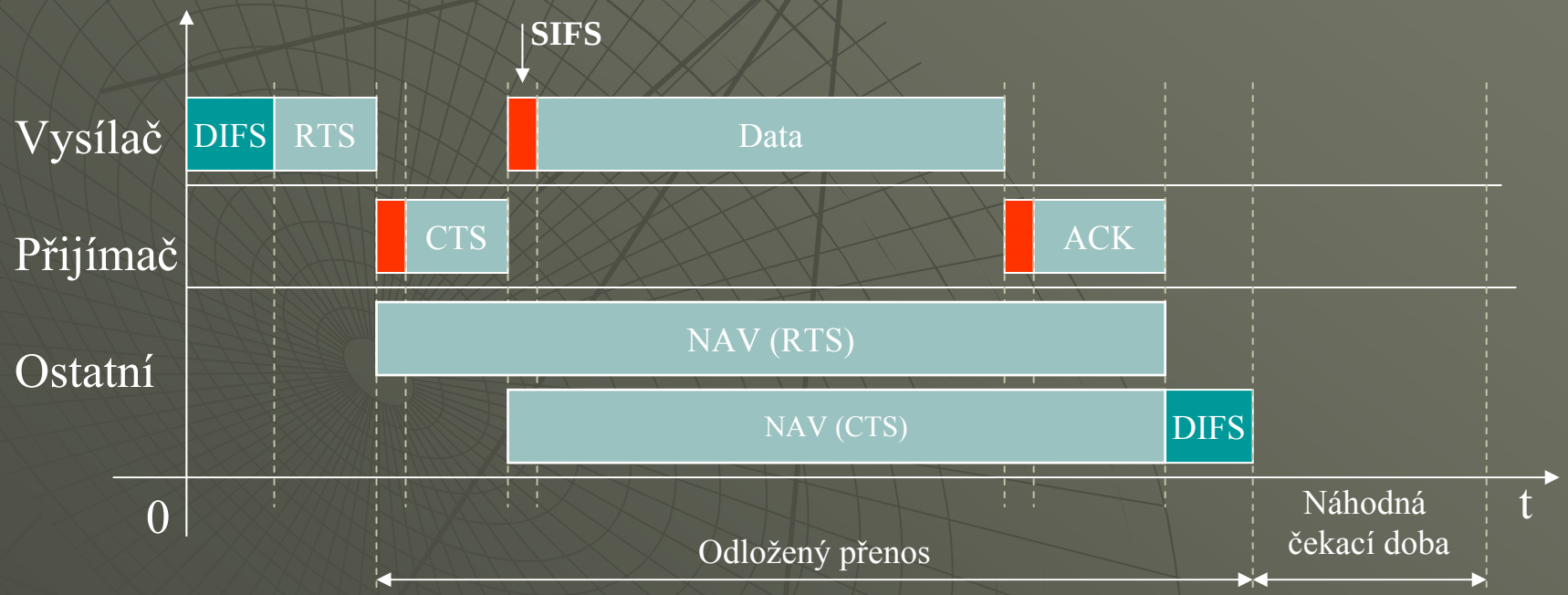
- **CSMA/CA** – *Carrier Sense, Multiple Access with Collision Avoidance*
- Přístupovou metodu CSMA/CD není možné použít, protože:
  - stanice by musely být schopny zároveň vysílat i přijímat signál (nárůst cenových nákladů)
  - **problém skrytého uzlu**:
    - dvě stanice jsou v dosahu přístupového bodu, ale nenacházejí se ve vzájemném dosahu



CSMA/CA

- používá se systém pozitivního potvrzování
  - stanice, která chce vysílat si ověří, zda-li je síť po určitou dobu (**DIFS** – Distributed Inter Frame Space) volná
  - jestliže síť je (stane se) v průběhu DIFS obsazená, tak se přenos dat odloží
  - v opačném případě je vyslán krátký packet **RTS** – Request To Send, který mimo jiné obsahuje infor-maci o době, kterou bude následující přenos trvat
  - cílová stanice odpovídá (po krátkém okamžiku - SIFS) packetem **CTS** – Clear To Send, který opět mimo jiné obsahuje dobu, po kterou bude následující přenos trvat
  - všechny stanice, které slyší RTS nebo CTS si nastaví vlastní indikátor **NAV** – Network Allocation Vector na dobu přenášenou v těchto packetech a nebudou se v jejím průběhu snažit přistupovat k síti
  - celá transakce je (v případě úspěšného přenosu dat) ukončena zasláním packetu **ACK** – Acknowledge
  - jestliže přenos není potvrzen packetem ACK, pak je situace vyhodnocena jako kolize a přenos se opakuje

CSMA/CA


SIFS
Vysílač
DIFS
RTS
Data
Přijímač
CTS
ACK
Ostatní
NAV (RTS)
NAV (CTS)
DIFS
0
t
Náhodná
čekací doba
Odložený přenos

Standardy

- **802.11a** - v pásmu 5 GHz s rychlostí až 54 Mb/s, povolen jen uvnitř budov, používá OFDM
- **802.11b** - v pásmu 2,4 GHz s rychlostí až 11 Mb/s, nejrozšířenější, WiFi
- **802.11c** – definice procedur v rámci MAC podvrstvy pro síťové mosty, 1998
- **802.11d** - mezinárodní harmonizace kmitočtového spektra, 2001
- **802.11e** – rozšíření MAC pro QoS, kvalita služeb
- **802.11f** - *Inter Access Point Protocol* (IAPP), spolupráce přístupových bodů od různých výrobců

Standardy II

- **802.11g** - zvýšení rychlosti v pásmu 2,4 GHz na 54 Mb/s se zpětnou kompatibilitou s 802.11b
- **802.11h** – změny v řízení přístupu k spektru 5 GHz na 54 Mb/s
- **802.11i** - zlepšení bezpečnosti v 802.11 bezdrátových sítích vylepšením autentizačního a šifrovacího algoritmu.
- **802.11j** – pouze Japonsko
- **802.1x** - standard zabezpečení jak drátových, tak bezdrátových sítí.

802.11b

- **kmitočtové pásmo:** 2 400 - 2483,5 Mhz (v ČR)
- **použitá modulace:** HR/DSSS (*High Rate DSSS* - přímá sekvence o vysoké rychlosti)
- **dosahované rychlosti:** 1; 2; 5,5; 11 Mb/s, záleží na podmínkách
- **efektivní rychlost** je až o 40% nižší kvůli režii
- **vysílací výkon:** je stanoven na maximální ekvivalentní izotropicky vyzářený výkon 100 mW
- **dosah:** maximálně lze v příhodných podmínkách dosáhnout spoje na vzdálenost několika kilometrů

802.11g

- **kmitočtové pásmo:** 2 400 – 2 483,5 Mhz (v ČR)
- **použitá modulace:** OFDM
- **dosahované rychlosti:** 1; 2; 5,5; 6; 9; 11; 12; 18; 24; 36; 48; 54 Mb/s
- **vysílací výkon:** vzhledem k práci ve stejném pásmu je upraven stejnou generální licencí ČTU jako pro IEEE 802.11b
- **dosah:** je mírně větší nebo stejný jako u 802.11b
- zpětně kompatibilní s 802.11b

802.11n

- minimálně 100 Mb/s (na fyzické vrstvě je cílem pro výrobce dokonce 600 Mb/s)
- MIMO (multiple input multiple output)
- aktuálně draft 2.0
- výrobci zaručují výměnu zařízení v případě nekompatibility s finální verzí standartu

Použití kanálů

Země	Kanál	Frekvence
USA a Kanada	1-11	2,412-2,462
Evropa	1-13	2,412-2,472
Francie	10-13	2,457-2,472
Španělsko	10-11	2,457-2,462
Japonsko	14	2,484

Kanály

- 13 kanálů není mnoho
- odstup mezi kanály pouze 5MHz
- překryv se sousedními 4 kanály
  - při použití DSSS s délkou posloupnosti 11 bitů je nutné použít pásmo o šířce 22 MHz – 25 MHz
  - je možné používat maximálně **3** nezávislé systémy pracující s DSSS, které se nebudou vzájemně rušit

802.11a

- frekvence 5150–5250 MHz, 5250–5350 MHz, 5470–5725 MHz
- přenosová rychlost 54 Mb/s
- rozprostření spektra pomocí OFDM
- ČTÚ nepovoluje, v pásmu 5GHz vyžaduje:
  - DFS: dynamická volba kanálu
  - TPC: automatická regulace výkonu
  - obě funkce specifikuje až standard 802.11h

WECA

- *Wireless Ethernet Compatibility Aliance* - založena 1999
- ověřuje kompatibilitu produktů
- začala používat označení WiFi (*Wireless Fidelity*) a nálepku WiFi certified
- následně mluvíme o WiFi sítích, tzn. splňuje požadavky organizace WECA
- uděluje certifikaci WiFi Zone providerům, kteří poskytují bezdrátový přístup na veřejných místech
- používalo se také označení WiFi5 pro 802.11a, ale bylo to matoucí

Typy bezdrátových sítí

- **Ad-hoc**
  - stanice komunikují přímo
  - není přístupový bod
  - vhodné pro dočasné sítě (LAN párty)
- **Infrastrukturní**
  - základní jednotkou access point – veškerá komunikace přes něj
  - nelze připojit stanici na více AP
  - AP může asociovat více stanic
  - transformuje bezdrátovou komunikaci na páteřní síť

Bezpečnost

- nelze dostatečně omezit prostor, kde je signál k zachycení
- **šifrování**
  - zabezpečení dat před odposlechnutím
  - WEP (*Wired Equivalent Privacy*) - používá symetrickou proudovou šifru RC4
    - klíče 64, 128, 256 bitů, ale 24 bitů je inicializační vektor
    - 2001 - program pro rekonstrukci WEP klíčů AirSnort
      - několik hodin trvá prolomit
    - častá obměna klíčů
    - distribuce klíčů uživatelům

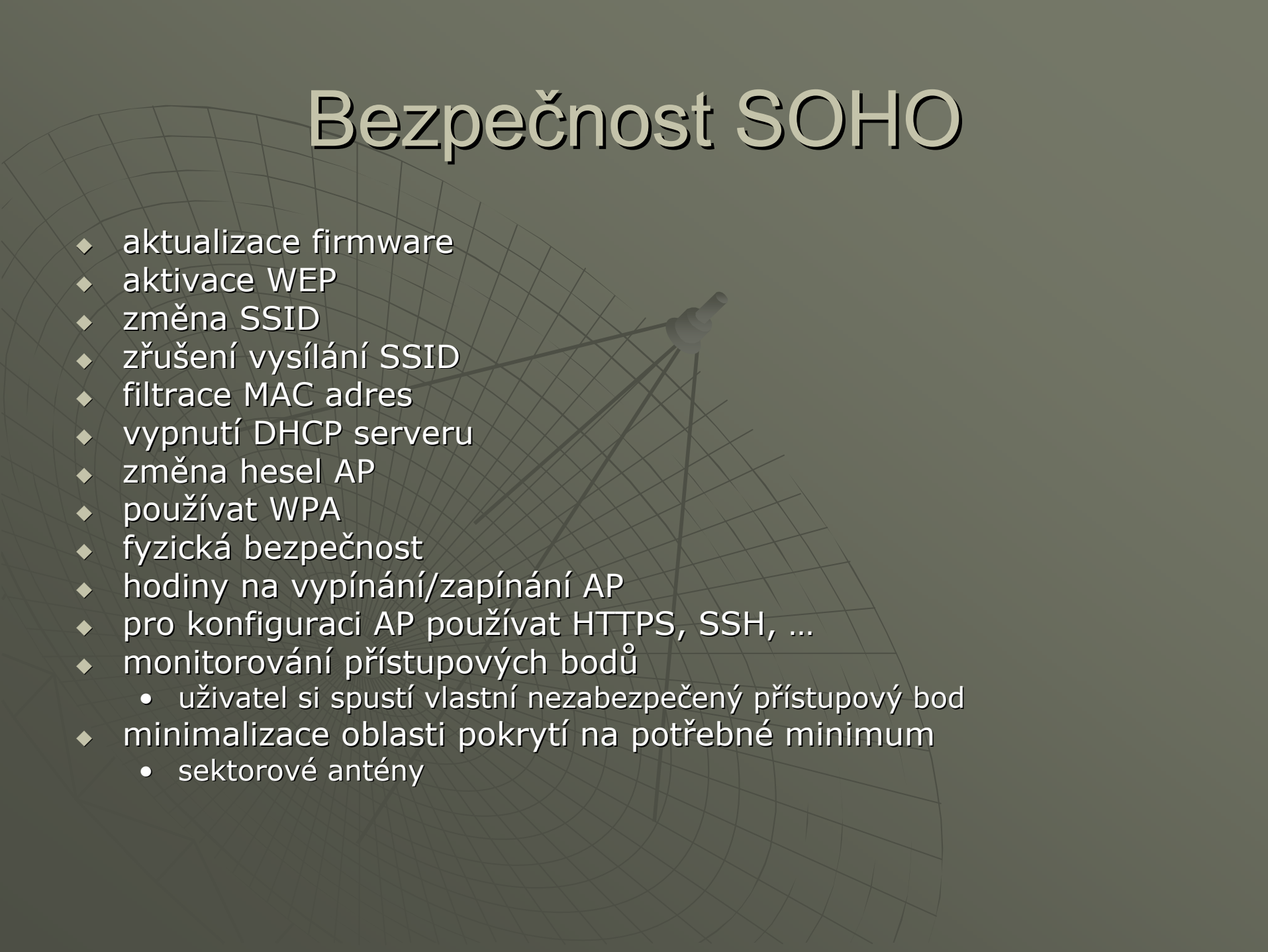
Bezpečnost II

- **autentizace**
  - řízení přístupu oprávněných uživatelů
  - u drátových stačí dobrý vrátný
  - jednosměrný proces
  - možnost útoku man-in-the-midlle
  - **open system**
    - klient posílá SSID (Service Set Identificator), přístupový bod jej ale může vysílat a stanice jej může přijmout a použít pro přístup
    - lze AP konfigurovat jako uzavřený, zkušený uživatel však dokáže SSID vytáhnout z odposlechnutých paketů
  - **shared-key**
    - ověření správnosti sdíleného klíče pomocí WEP

Bezpečnost III

- **filtrování adres**: nedefinuje 802.11
  - seznam MAC adres klientů, kteří se mohou k AP připojit
  - lze však odposlouchávat komunikaci a následně si svoji MAC přenastavit
  - problém s údržbou seznamu
  - omezení šířky pásma
  - časové omezení
- **WPA** (*WiFi Protected Access*) – 2003
  - používá šifrování dynamickým klíčem TKIP
  - 128 bitový klíč
  - mění dočasný klíč každých 10 000 paketů
  - integrita zpráv kontrolována pomoci algoritmu MIC
- **802.1x** – obecný bezpečnostní rámec pro všechny typy LAN
  - zajišťuje autentizaci uživatelů, integritu zpráv (šifrováním), distribuci klíčů
  - založen na protokolu EAP (Extensible Authentication Protocol)
  - není neprůstřelné
- **802.11i** – založen na šifrování pomocí AES
  - klíč 128, 192, 256 bitů
  - k protokolu TKIP přidán ještě CCMP
  - dostatečný šifrovací algoritmus i pro vládní účely
- některé přístupové body jsou absolutně nechráněny!
- pouze 44% přístupových bodů používají šifrovanou komunikaci
- 10% přístupových bodů používá zcela standardní nechráněné nastavení

Bezpečnost SOHO



- aktualizace firmware
- aktivace WEP
- změna SSID
- zřušení vysílání SSID
- filtrace MAC adres
- vypnutí DHCP serveru
- změna hesel AP
- používat WPA
- fyzická bezpečnost
- hodiny na vypínání/zapínání AP
- pro konfiguraci AP používat HTTPS, SSH, …
- monitorování přístupových bodů
  - uživatel si spustí vlastní nezabezpečený přístupový bod
- minimalizace oblasti pokrytí na potřebné minimum
  - sektorové antény

HW pro WiFi sítě

- spousta výrobců (Asie, Cisco, Nokia,…) ale je i hodně „no-name“ výrobců
- rozlišujeme hlavně podle podpory OS a ceny
- AP liší se ve způsobu prvnotního nastavení (telnet, SNMP, webové rozhraní)
- někdo dodává tovární nastavení – nutné změnit!
- dnes i HiFi , DVD s podporou WiFi

AP

- výkon – množství najednou připojených uživatelů - 30 až 254
- možnost připojení externích antén
- vhodné rozhraní do kabelové sítě
- napájení – po síti, vyhnu se problémům s eletroinstalací
- možnost roamingu
- zabezpečení
- DHCP

Antény

- **všesměrové** - pokrývají úhel 360°
  - nejběžnější typ
  - používány na FI
- **sektorové** - pokrývají určitý sektor prostředí
  - úhly např. 45°, 90°, ...
  - vhodné na zeď budovy
- **směrové** - vyzařují jedním směrem v úzkém pruhu
  - signál soustředí do jednoho bodu
  - vhodné pro delší vzdálenosti
- **zisk antény** – nejdůležitější parametr
  - čím větší, tím vzdálenější signál lze zachytit
  - udává se v dbi (decibel na isotrop)
- **vyzařovací úhel** – horizontální, vertikální
- **vzhled** - na barvě nezáleží ☺, váha a rozměry, ochrana proti větru, případně vlhku
- lze vyrobit vlastní
- vhodný kabel, konektory

WPAN - Bluetooth

- radiová technologie o nízkém vysílacím výkonu (1mW) vyvinutá za cílem nahrazení pevného propojení elektronických zařízení (PC, tiskárny, mobilní telefony, PDA atd.)
- pracuje v pásmu 2,4 GHz
- datová rychlost 720 kb/s do vzdálenosti 10 metrů
- použita technika FHSS
- přímá viditelnost mezi vysílačem a přijímačem není potřeba
- jednoduchost, miniaturizace a nízká spotřeba

Přenos infračerveným zářením

- DFIR – *Diffused Infrared*
- povinně rychlostí 1 Mb/s, volitelně 2 Mb/s
- omezeno na jednu kancelář, nebo jiný souvislý prostor
- neprochází pevným materiálem
- dražší než rádiové sítě

Bezdrátová síť na MU

- přístup přes virtuální privátní sít Masarykovy univerzity https://vpn.muni.cz
- Pptp server Masarykovy univerzity umožňuje strojům, které nejsou registrovány pod doménou muni.cz přistupovat do sítě Masarykovy univerzity a využívat zdrojů a služeb, které jsou v rámci této sítě poskytovány
- FSS, CPS, ESF, FF, PřF, LF, FI
- http://studovna.muni.cz/info/accesspointy.shtml
- EDUROAM

Bezdrátová síť na FI MU

- http://www.fi.muni.cz/tech/wireless/
- založené na standardu 802.11b
- ORiNOCO AP-1000, AP-2000, AP-2500 a ORiNOCO Outdoor Router
- AP-2000 a 2500 zvládají i 802.11g
- každé AP má jednu kartu ORiNOCO PC Card Silver
- AP jsou napojeny na externí antény se ziskem 6 dBi, venkovní AP má anténu 10 decibelovou
- celkem je po budově 21 AP – pokryty všechny prostory

Bezdrátová síť na FI MU II

- vyhrazena podsíť 147.251.51
- klient obdrží od DHCP serveru dynamickou IP adresu a je mu povolen pouze přístup na fakultní administrativu, kde svou kartu přihlásí k používání

  https://fadmin.fi.muni.cz/auth/sit/wireless/login.mpl
- následně je povolen přístup do sítě na základě MAC adresy
- síť je za firewallem a je pro ni speciální provoz
- stejný přístup jako ke strojům mimo FI
  - nelze např. sdílet disky přes NFS a SMB
- pokud klient 2x po pěti minutách neodpoví, zruší se jeho povolení na firewallu

Bezdrátová síť na FI MU III

- Uživatelé musí vzít na vědomí, že veškerá komunikace mezi jejich počítačem a a bezdrátovým přístupovým bodem je odposlechnutelná, dokonce případný útočník má možnost za určitých okolností převzít jejich adresu a takto "unést" existující spojení. Doporučuje se proto používat k přihlašování i k přenosu dat zabezpečené šifrované protokoly (například HTTPS, IMAPS, POP3S a SSH)

Bluetooth bezdrátová síť FI

- http://www.fi.muni.cz/tech/wireless/bt.xhtml
- experimentálně zprovozněn 1 bezdrátový access point
- výhoda spočívá v menší náchylnosti na ruchy
- nevýhodou je nízká přenosová rychlost (teoreticky max. 1Mb/s) a malé množství klientů, které může být k přístupovému bodu připojeno
- na FI jsou zařízení splňující výkonovou třídu 1, proto při komunikaci s klientem stejné třídy může být vzdálenost mezi nimi v otevřeném prostoru až 100 m
- PDA s vestavěným Bluetooth rozhraním většinou odpovídají pouze třídě 2, která umožňuje komunikaci se zařízením do vzdálenosti 10 m od AP
- Tento připojení **nesmí** být využit pro objemné datové přenosy. Je vhodný především pro čtení pošty a jinou nenáročnou šíťovou komunikaci.
- autentizační PIN byl zvolen 0000

Hotspot

- veřejné přípojné body na exponovaných místech
- hotely, letiště, kavárny, benzínky, parky, dokonce i na severním pólu
- zpoplatnění za přenesená data, nebo za čas strávený na síti
- v zahraničí mnohem více bezplatných
- celkem okolo 100 tisíc
- www.wifi.lupa.cz
- www.marigold.cz/hotspoty
- www.telecom.cz/wifi
- www.wifijet.cz
- www.widenet.cz