WLAN přístupová metoda CSMA/CA a zabezpečení

Tato prezentace představuje princip bezdrátové přístupové metody CSMA/CA, kterou využívají sítě WLAN (Wi-Fi). Vysvětlíme rozdíl mezi CSMA/CD a CSMA/CA, proč je „vyhýbání se kolizím“ v bezdrátovém prostředí nezbytné, a jak se realizuje v praxi. Dále se zaměříme na zabezpečení Wi-Fi sítí a představíme základní mechanismy šifrování (WEP, WPA, WPA2, WPA3), včetně jejich silných a slabých stránek.

Úvod do WLAN a přístupových metod

WLAN (Wireless LAN) a standardy

- Bezdrátové lokální sítě obvykle založené na IEEE 802.11.
- Základní vrstvy a frekvenční pásma: 2,4 GHz, 5 GHz, 6 GHz (Wi-Fi 6E).

Proč není CSMA/CD vhodné pro bezdrát

- V bezdrátovém prostředí se hůře detekují kolize (problém se signálem a odrazy).
- Stanice nemohou vysílat a zároveň přijímat se stejnou anténou, aby ověřily kolizi.

Řešení → CSMA/CA (Collision Avoidance)

- Metoda „vícenásobného přístupu s detekcí nosné a vyhýbáním se kolizím“.
- Používá se k minimalizaci výskytu kolizí v bezdrátovém prostředí.

Princip CSMA/CA

Carrier Sense

- Stanice nejprve kontroluje (sensing) stav přenosového média (čte energii v kanálu).
- Pokud je médium volné, stanice může vysílat.

Collision Avoidance

- Před odesláním delšího rámce může stanice poslat RTS (Request To Send).
- Přístupový bod (AP) odpoví CTS (Clear To Send), pokud je médium volné.
- Během doby CTS „rezervace“ ostatní stanice čekají.

ACK a backoff

- Při úspěšném příjmu rámce stanice či AP odesílá potvrzení ACK.
- Pokud se ACK neobjeví, předpokládá se kolize a nastupuje „backoff“ – náhodná čekací doba.

RTS/CTS Mechanismus

RTS (Request To Send)

- Rámec, kterým stanice oznámí, že chce vysílat delší data.
- Obsahuje informace o délce požadovaného vysílání.

CTS (Clear To Send)

- Odezva od příjemce (typicky AP), která umožní exkluzivní přístup k médiu na danou dobu.
- Ostatní stanice, které příjem CTS zaznamenají, se zdrží vysílání.

Využití

- Zvláště užitečné v situaci skrytých uzlů (hidden node problem), kdy se dvě stanice „nevidí“, ale obě jsou v dosahu AP.

Porovnání CSMA/CD a CSMA/CA

Metoda	CSMA/CD (Ethernet)	CSMA/CA (Wi-Fi)
Detekce kolize	Probíhá během vysílání dat	Obvykle nemožné, proto prevence
Prostředí	Drátové sítě (Ethernet)	Bezdrátové sítě (WLAN, 802.11)
Způsob řešení kolize	Okamžité zastavení vysílání + backoff	RTS/CTS, backoff, ACK, vyhýbání se kolizím
Výhody	Jednodušší implementace v kabelech	Nutné pro bezdrát, řeší hidden node
Nevýhody	Vyžaduje možnost poslouchat během vysílání	Vyšší režie (kontrolní rámce, backoff)

Zabezpečení WLAN – Historický vývoj

WEP (Wired Equivalent Privacy)

- Původní mechanismus zabezpečení (RC4 šifra), slabá inicializační vektor (IV).
- Snadno prolomitelný, považován za zastaralý.

WPA (Wi-Fi Protected Access)

- Reakce na slabiny WEP, přidává TKIP (Temporal Key Integrity Protocol).
- Stále však může obsahovat slabší ochranu (např. když se používá starší RC4).

WPA2 (IEEE 802.11i)

- Standardizovaná silnější ochrana, využívá AES (CCMP).
- Dlouhá léta považovaná za bezpečnou volbu pro domácí i podnikové sítě.

WPA3

- Moderní varianta, zavádí SAE (Simultaneous Authentication of Equals), lepší ochranu proti offline útokům.
- Některá zařízení mohou mít problém s kompatibilitou, postupné rozšiřování.

Autentizace a režimy zabezpečení

PSK (Pre-Shared Key)

- Nejčastější v domácích sítích (WPA2-PSK).
- Sdílené heslo (fráze), nutná dostatečná délka a složitost pro zvýšení odolnosti.

Enterprise (802.1X/EAP)

- V podnikových sítích, používá RADIUS server pro ověření uživatelů.
- Vyžaduje infrastrukturní prvky (např. FreeRADIUS, Windows Server NPS).

Open (nezabezpečené)

- Žádné šifrování (např. kavárny, hotely).
- Lze doplnit captive portál, ale data stále nejsou šifrována.

Bezpečnostní rizika a doporučení

Slabá hesla

- Krátké nebo jednoduché heslo lze prolomit slovníkovým útokem.

WEP a WPA s TKIP

- V dnešní době nedostatečné, náchylné k průnikům.

Doporučení

- Používat WPA2 či WPA3 s AES (CCMP).
- V domácnosti volit složité heslo (12+ znaků).
- V enterprise prostředí nasadit RADIUS a 802.1X pro lepší správu a ověřování.

Další bezpečnostní prvky WLAN

MAC filtr

- Omezení přístupu dle MAC adres, snadno zfalšovatelné, není bezpečné samo o sobě.

Skrývání SSID

- Nezobrazení názvu sítě, avšak lze snadno odhalit zachycením management rámců.

Captive portál

- Webová stránka pro přihlášení (např. v kavárnách), ale data nejsou šifrována, pokud není současně použita zabezpečená vrstva (WPA2, HTTPS).

Intrusion Detection/Prevention

- Pokročilé AP a kontroléry dokáží detekovat neoprávněné AP (Rogue AP), DoS útoky apod.

Shrnutí

- **CSMA/CA** je nezbytná metoda řízení přístupu v bezdrátových sítích (Wi-Fi), protože **kolize není snadné detekovat**. Mechanismy jako *RTS/CTS* pomáhají předcházet konfliktům, zvláště v prostředí se skrytými uzly.
- **Zabezpečení WLAN** prošlo dlouhým vývojem. Dnes je standardem **WPA2 (AES-CCMP)**, popř. **WPA3**. Starší WEP nebo WPA s TKIP jsou **zranitelné**.
- Pro **domácí uživatele** je vhodná volba **WPA2-PSK/WPA3-PSK** se silným heslem, **enterprise sítě** preferují **WPA2/WPA3 Enterprise** s autentizací 802.1X/RADIUS.
- Dodatečná opatření (MAC filtr, skryté SSID) nejsou samy o sobě bezpečnostním řešením, lze je však použít jako drobné doplňky.

Kontrolní otázky

1. Vysvětlete, proč se v bezdrátovém prostředí nedá prakticky použít CSMA/CD a je nutné CSMA/CA.
2. Jak funguje RTS/CTS mechanismus a k čemu slouží?
3. Proč je WEP považován za velmi slabý a nedoporučuje se?
4. Jaké výhody přináší WPA2 (AES-CCMP) oproti dřívějším standardům zabezpečení?
5. V čem spočívá rozdíl mezi režimem WPA2-PSK a WPA2 Enterprise (802.1X)?
6. Proč je důležité používat dostatečně silné heslo v domácí Wi-Fi síti?

Doporučená literatura

1. **Tanenbaum, A. S., Wetherall, D.**: *Počítačové sítě*, 5. vydání (v češtině) – Kapitoly o bezdrátových sítích a zabezpečení.
2. **Kurose, J. F., Ross, K. W.**: *Computer Networking: A Top-Down Approach* – Části věnované Wi-Fi (IEEE 802.11) a protokolům CSMA/CA.
3. **Cisco Networking Academy**: *CCNA Wireless* (či obdobné materiály) – Podrobný rozbor architektury WLAN a zabezpečení.
4. **Oficiální dokumenty IEEE 802.11** – Standard popisující fyzickou i MAC vrstvu Wi-Fi, včetně zabezpečení 802.11i.
5. **Wi-Fi Alliance** – Informace o certifikacích WPA2, WPA3 a nejnovějších trendech ve Wi-Fi technologiích.