

# Sicurezza dei sistemi e delle reti[1]

Mattia Monga

Dip. di Informatica
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2013/14



# Lezione XIX: Reti wireless

# Reti wireless



La prima rete wireless nasce nel 1971 fra le isole dell'arcipelago delle Hawaii (ALOHANET).
Dagli anni '90 hanno avuto una enorme diffusione:

- Trasmissione via onde radio
- Bassi costi infrastrutturali
- Flessibilità nell'utilizzo

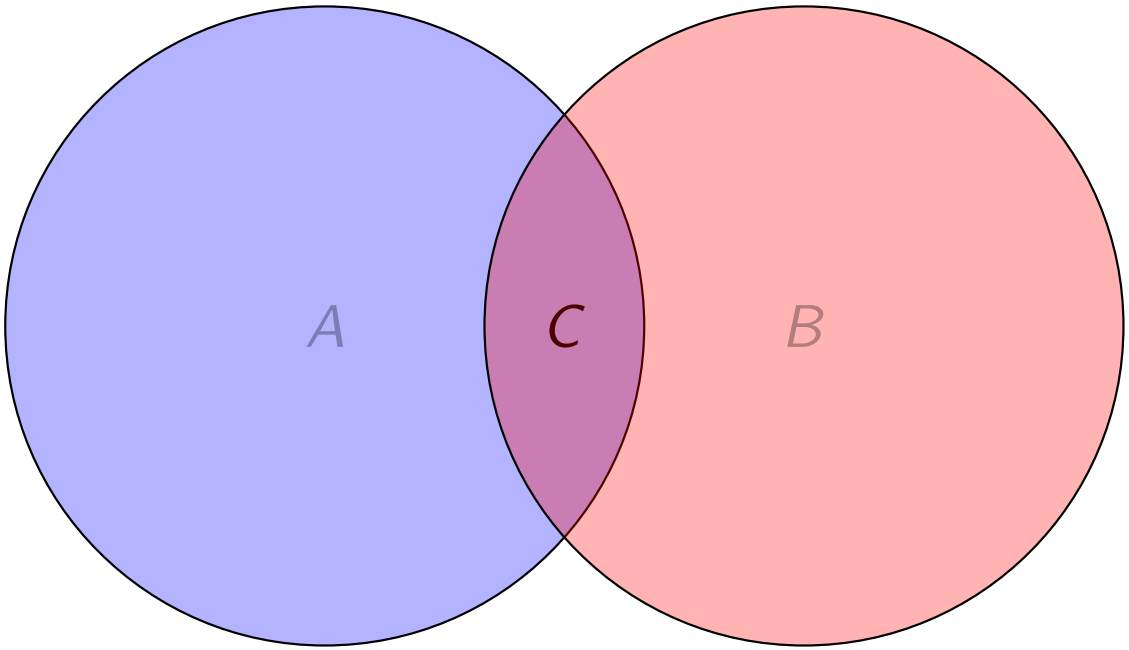
# Caratteristiche salienti




Dal punto di vista della sicurezza:

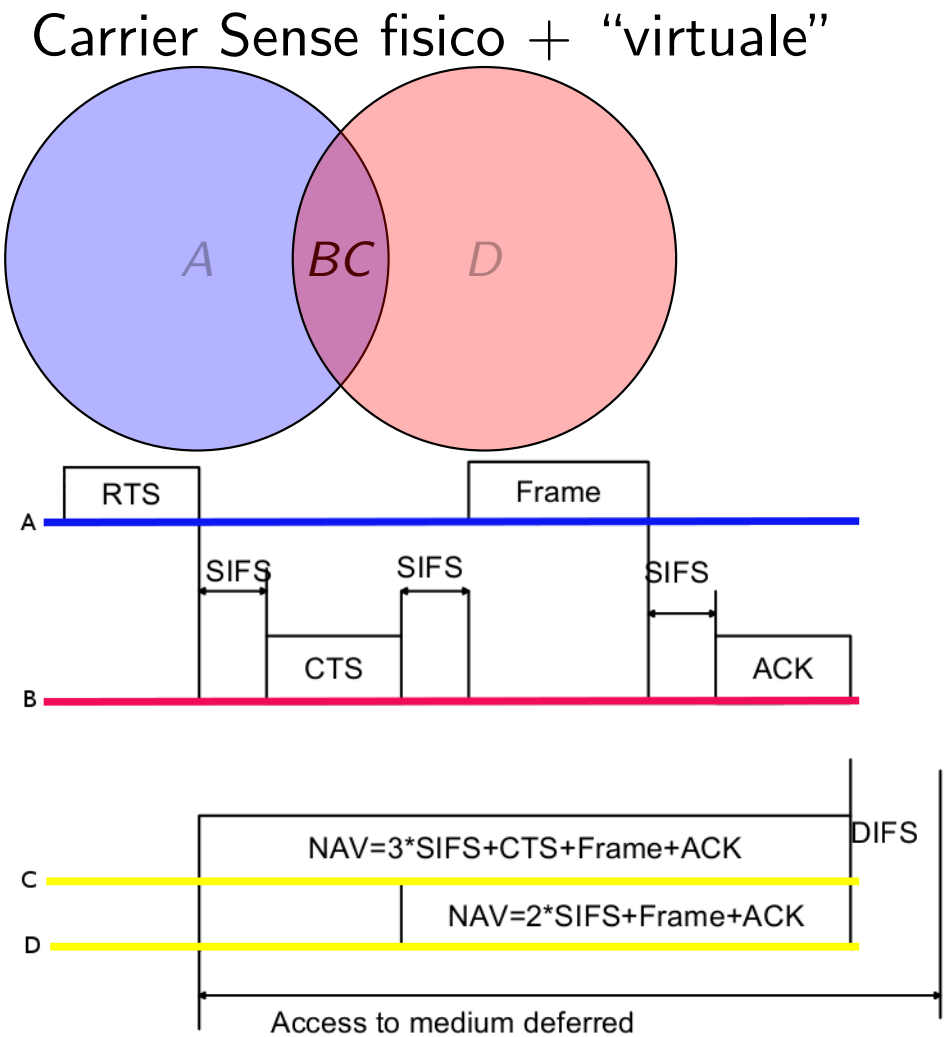
- Segnali intrinsecamente broadcast
- Anche se, a differenza delle LAN cablate, il canale non è necessariamente "condiviso" fra tutti, perché ci possono essere range di ricezione diversi
- Attenuazioni e interferenze

# Collision detection




$A$ non sente $B$, ma esiste comunque una zona di collisione dei due segnali: non si può usare il meccanismo di Ethernet.

# CSMA/CA




- $A \rightarrow B$
- Tempi standard

  SIFS<PIFS<DIFS<EIFS
- $A$, ricevuto il CTS, fa partire un timer per l'ACK
- $C$ sente RTS (e CTS), $D$ solo CTS

# 802.11 (WiFi)




Gli standard IEEE per le LAN wireless sono raccolti nella famiglia 802.11

- 802.11a 5GHz, 54Mb/s teorico, circa 20Mb/s, 12 canali
- 802.11b 2.4GHz, 11Mb/s (5.9 Mb/s TCP 7.1 Mbit/s UDP)
- 802.11g 2.4GHz, 54Mb/s teorico, circa 25Mb/s
- 802.11i (WPA2) standard di sicurezza
- 802.11n standard recente che permette bande elevate e l'uso congiunto di piú antenne

# Modalità di funzionamento



**Access point** (AP) o modalità infrastruttura: ogni nodo spedisce i pacchetti tramite un AP (che poi li gira verso una rete cablata o wireless)

**Ad hoc** un nodo scambia i frame direttamente con un altro

**Monitor** una scheda di rete riceve tutti i frame

# Caratteristiche



- Ogni nodo è contrassegnato dal suo numero MAC
- Ogni AP è contrassegnato da un Service Set IDentifier (SSID)
  - L'AP annuncia il SSID con regolarità (beaconing)
  - I nodi fanno scanning di un AP, passivo o attivo (*probe request*)
  - Il MAC dell'AP è detto BSSID

# Servizi 802.11



**Associazione** usato dai nodi per connettersi ad un AP, quando ci si trova nell'ambito della sua portata

**Autenticazione** usato dai nodi per avere il permesso di ricevere e spedire dati

# Riassumendo



Le reti wireless 802.11

- Trasmissioni broadcast, con tecniche di *carrier sense* particolari
- La modalità infrastrutturale prevede AP cui ci si deve associare

# Vulnerabilità intrinseche




- Il segnale è facile da intercettare
- Il segnale è facile da disturbare
- In alcuni casi il nodo può avere ridotte capacità di calcolo

# Attacchi frequenti



- Eavesdropping
- Denial of service
- Spoofing e message replay

L'identificazione di un nodo è spesso affidata al solo numero MAC: facilmente falsificabile (e per di piú il traffico lecito è accessibile all'attaccante!)

# WEP



Wired Equivalent Privacy (WEP) 1999, tutt'ora abbastanza diffuso.

- Shared key di 40, 104 o 232 bit (WEP key)
- Le chiavi sono identificate da un keyID di un byte, perché un nodo ne può avere piú di una
- Le chiavi devono essere trasmesse tramite un canale sicuro (offline a tempo di setup)
- Non c'è protezione fra coloro che conoscono la chiave (come in una LAN Ethernet)

# Autenticazione



Chiave condivisa $K$

1. un nodo $N$ manda una richiesta all'access point $AP$
2. $AP$: challenge $w = a_1 \dots a_{16}$ di $16 \times 8 = 128$bit
3. $N$: genera initialization vector $IV$ (24 bit), calcola $m = RC4(IV|K) \oplus w$ e manda $r = IV|m$
4. $AP$ controlla $RC4(IV|K) \oplus m = w$

# Debolezza dell'autenticazione



- Sul canale viaggiano $w$ e $r = IV|(RC4(IV|K) \oplus w)$.
- Poiché $A \oplus B \oplus B = A$, un attaccante può calcolare $RC4(IV|K)$.
- Siccome l'$IV$ lo sceglie il nodo (e può essere riutilizzato!), l'attaccante può autenticarsi con qualsiasi challenge $w'$ mandando $r = IV|(RC4(IV|K) \oplus w')$

# Debolezza del controllo d'integrità




In WEP il controllo d'integrità dei pacchetti è ottenuto con un semplice CRC del pacchetto (senza elementi segreti).

- $CRC(A \oplus B) = CRC(A) \oplus CRC(B)$
- l'attaccante può alterare un pacchetto e iniettarne di nuovi

# Tampering



Un pacchetto $p$ sul canale è $x = (p|CRC(p)) \oplus RC4(IV|K)$

- L'attaccante intercetta $x$ e manda $x' = (p'|CRC(p')) \oplus x$
- $$\begin{aligned} x' &= (p'|CRC(p')) \oplus (p|CRC(p)) \oplus RC4(IV|K) \\ &= ((p' \oplus p)|(CRC(p') \oplus CRC(p))) \oplus RC4(IV|K) \\ &= ((p' \oplus p)|(CRC(p' \oplus p))) \oplus RC4(IV|K) \end{aligned}$$
- Scegliendo opportunamente $p'$ l'attaccante manda ciò che vuole

# Injection



L'injection è ancora piú facile.

- Come visto nell'autenticazione, l'attaccante può conoscere un $RC4(IV|K)$ legittimo
- A questo punto può iniettare $IV|m|CRC(m) \oplus RC4(IV|K)$ con $m$ qualsiasi (gli $IV$ possono essere riutilizzati)

# Fragmentation attack

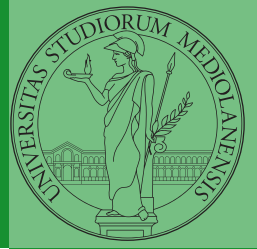


I primi 8 byte dei frame 802.11b sono fissi

| | |
|---|---|
| IP | AA AA 03 00 00 00 08 00 |
| ARP | AA AA 03 00 00 00 08 06 |

L'attaccante può quindi ottenere i primi 8 byte di $RC4(IV|K)$. È possibile frammentare un messaggio in frammenti di 4 byte + 4 byte di integrity check e utilizzare la chiave cosí trovata.

# Riassumendo






Le reti wireless rendono il canale facilmente accessibile agli attaccanti: occorre usare contromisure crittografiche.

- Wired Equivalent Privacy
- Un protocollo mal progettato con innumerevoli vulnerabilità