臺灣大學 National Taiwan University



Wireless LAN Security

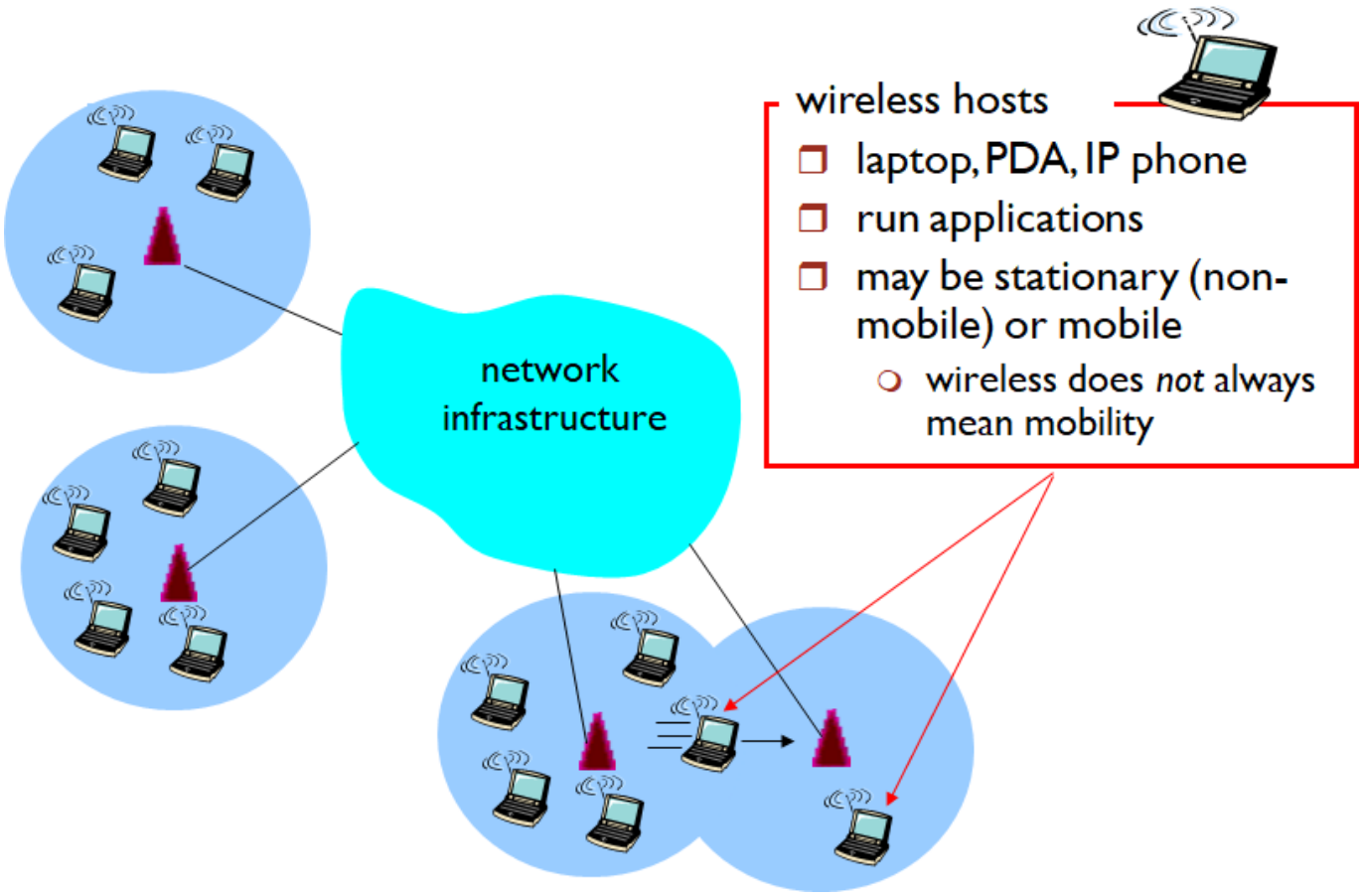
Prof. Ai-Chun Pang
National Taiwan University
Email: acpang@csie.ntu.edu.tw



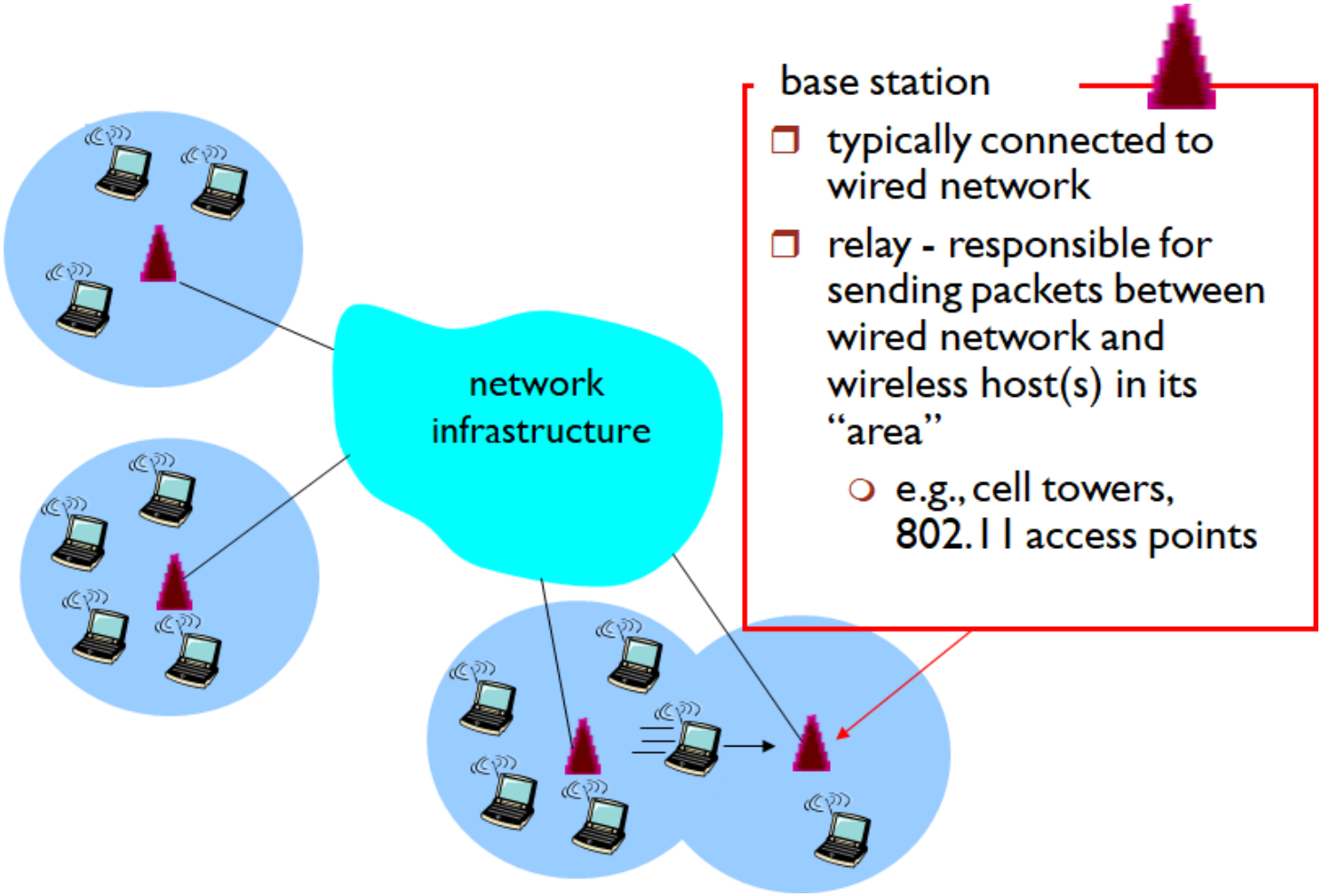
Outline

- Introduction to Wireless Network
- Securing wireless LANs
  - Authentication
  - Authorization

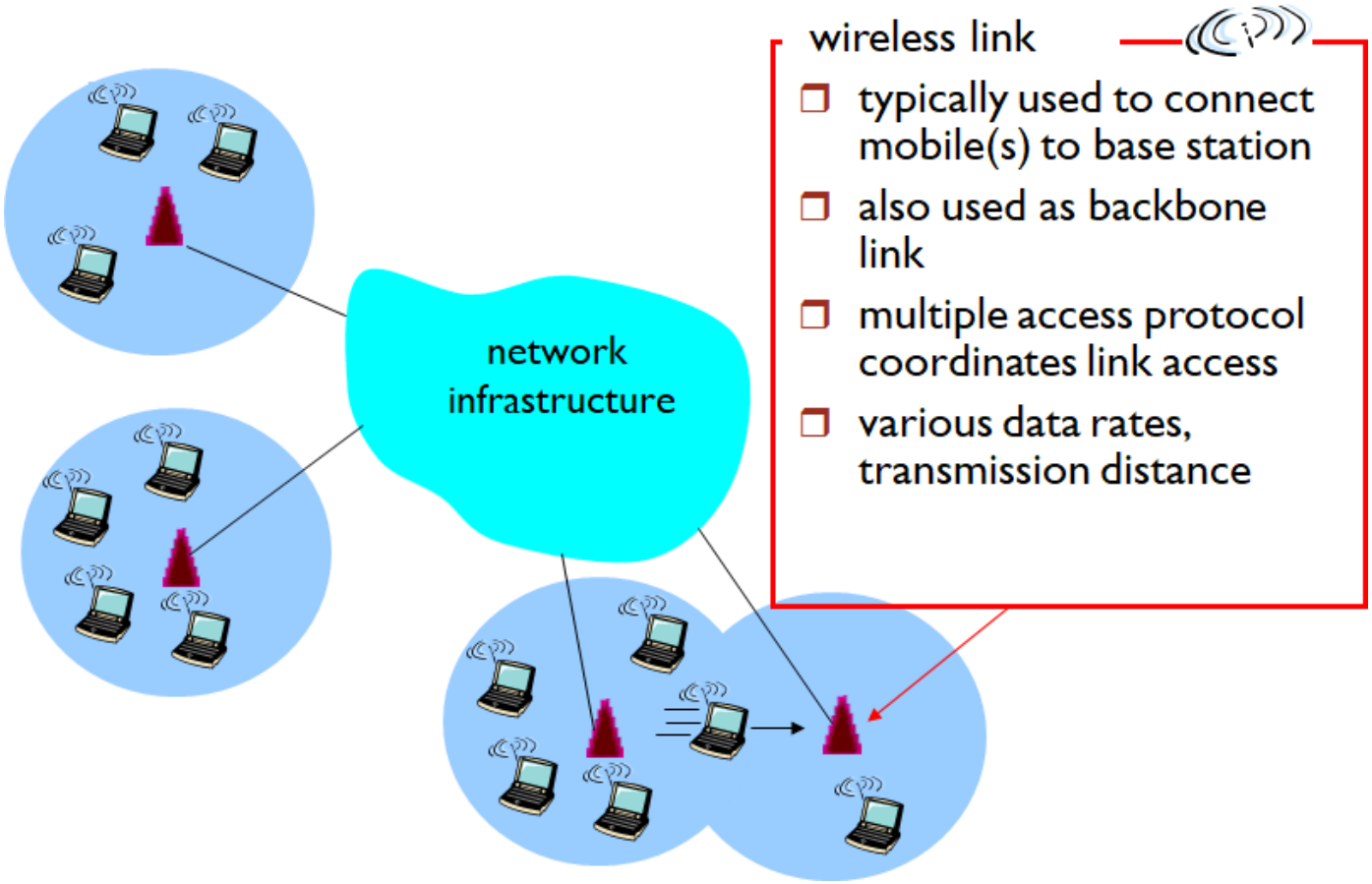
Elements of wireless network



Elements of wireless network

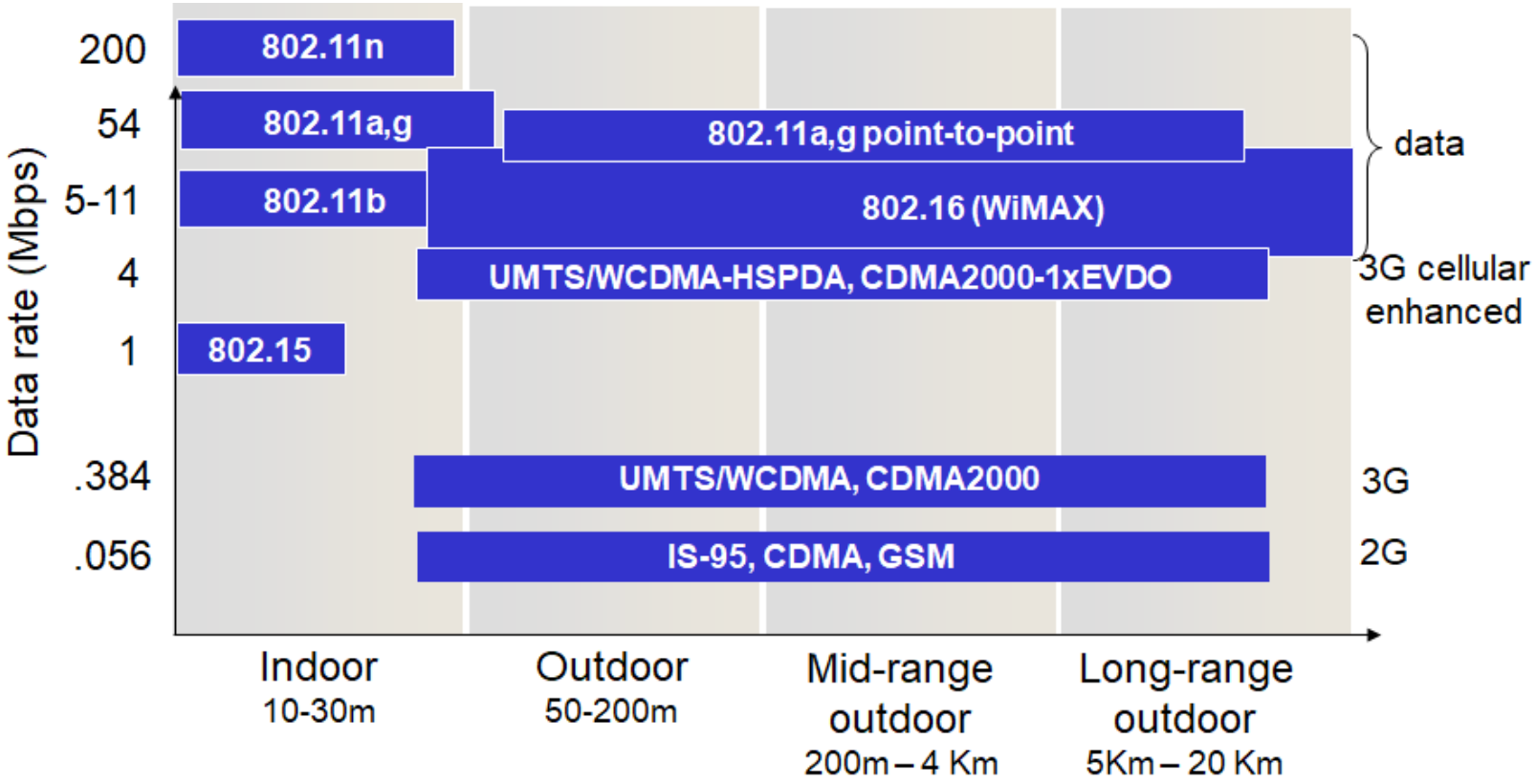


Elements of wireless network

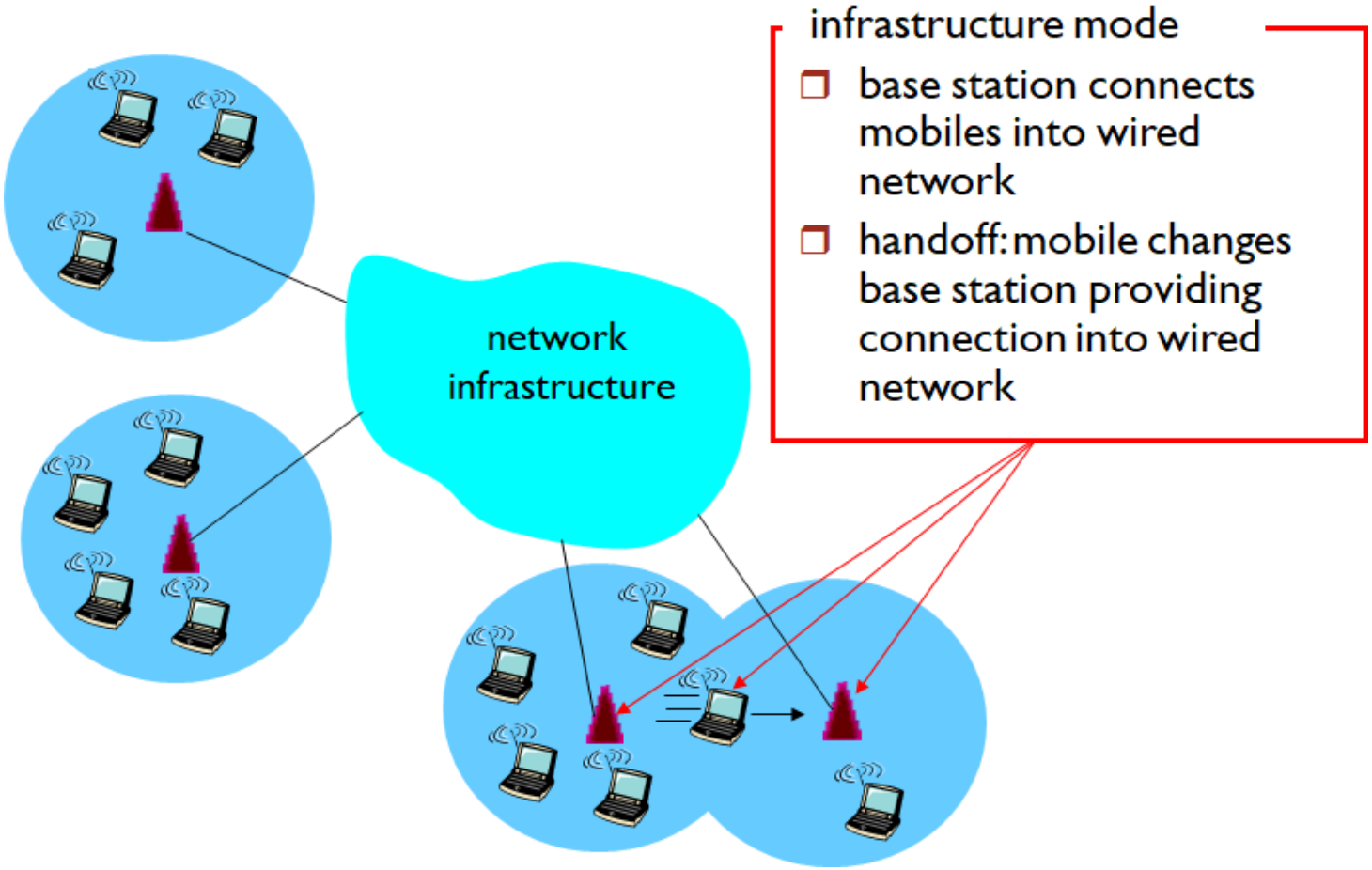




Characteristics of selected wireless network standards

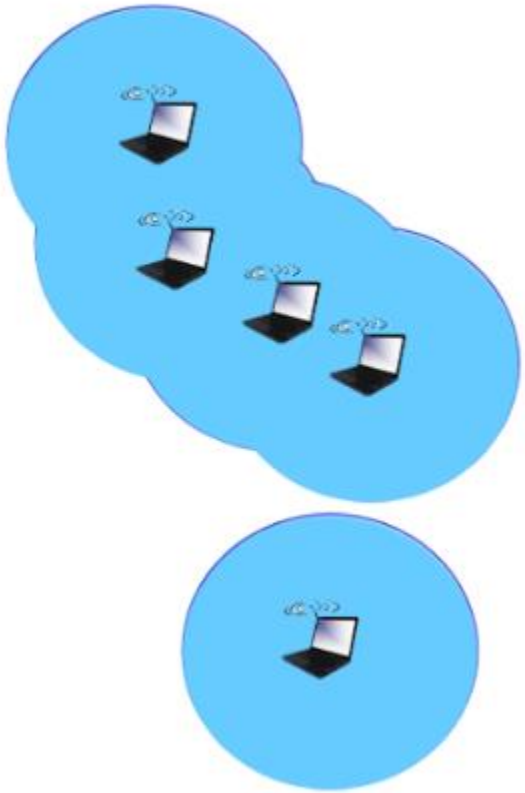


Elements of wireless network





Elements of wireless network



ad hoc mode

- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves



Wireless Network Taxonomy

	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: *mesh net*
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach a given wireless node (MANET, VANET)



Outline

- Introduction to Wireless Network
- Securing wireless LANs
  - Authentication
  - Authorization



What can a "bad guy" do?

A lot!

- eavesdrop: intercept messages
- actively insert messages into connection
- impersonation: can fake (spoof) source address in packet (or any field in packet)
- hijacking: “take over” ongoing connection by removing sender or receiver, inserting himself in place.
- denial of service: prevent service from being used by others (e.g., by overloading resources)



IEEE 802.11 security

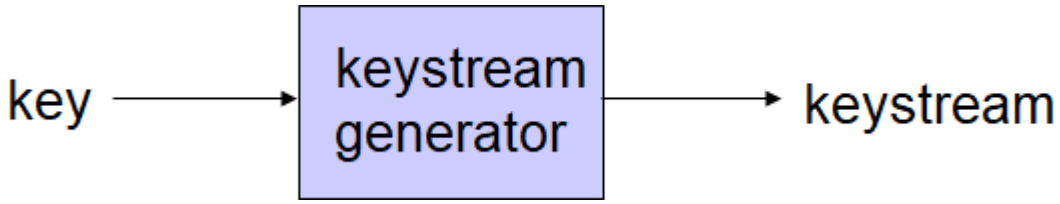
- *war-driving:* drive around Bay area, see what 802.11 networks available?
  - More than 9000 accessible from public roadways
  - 85% use no encryption/authentication
  - packet-sniffing and various attacks easy!
- securing 802.11
  - encryption, authentication
  - first attempt at 802.11 security: Wired Equivalent Privacy (WEP): a failure
  - current attempt: 802.11i



WEP design goals

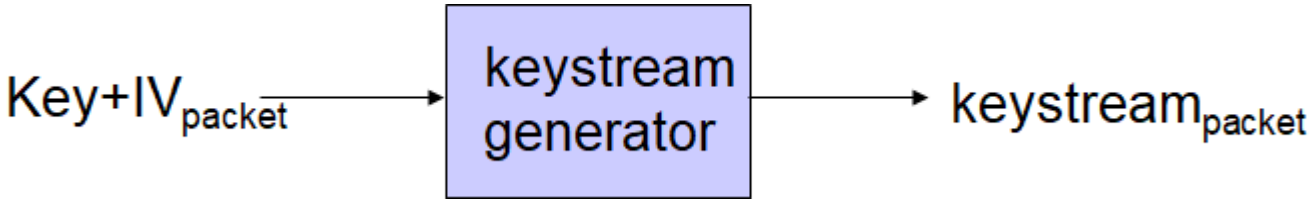
- **Symmetric key crypto**
  - Confidentiality
  - Station authorization
  - Data integrity
- **Self synchronizing: each packet separately encrypted**
  - Given an encrypted packet and key, the packet can be decrypted even if its preceding packet was lost (unlike Cipher Block Chaining (CBC) in block cipher)
- **Efficient**
  - Can be implemented in hardware or software

Review: symmetric stream ciphers



- *combine each byte of keystream with byte of plaintext to get ciphertext:*
  - m(i) = ith unit of message
  - ks(i) = ith unit of keystream
  - c(i) = ith unit of ciphertext
  - c(i) = ks(i) ⊕ m(i) (⊕ = exclusive or)
  - m(i) = ks(i) ⊕ c(i)
- WEP uses RC4

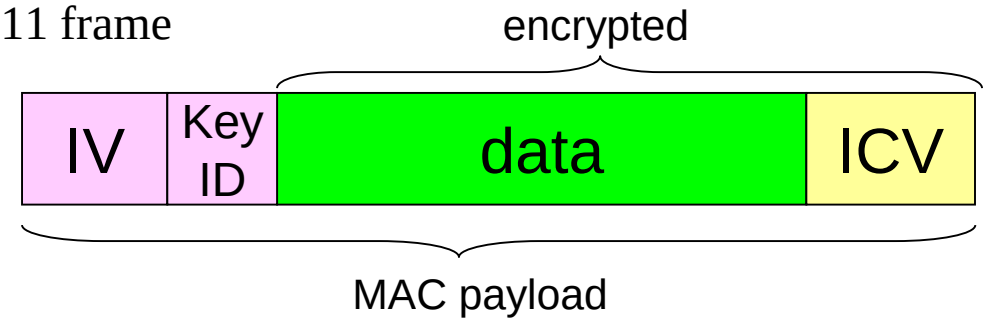
Stream cipher & packet independence



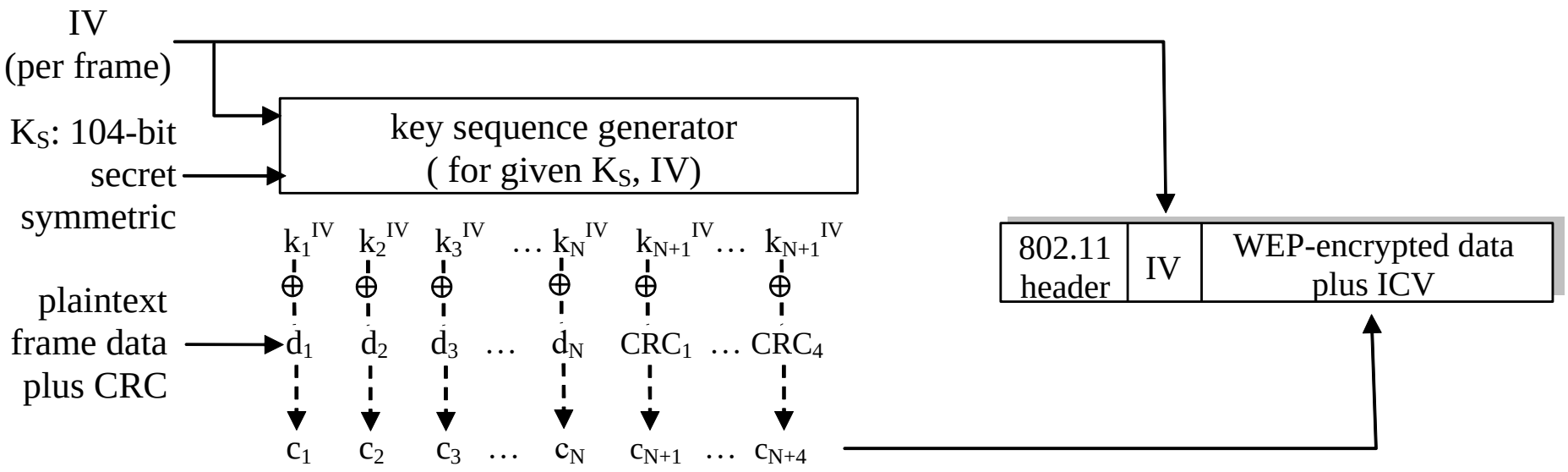
- recall design goal: each packet separately encrypted
- if for frame n+1, use keystream from where we left off for frame n, then each frame is not separately encrypted
  - need to know where we left off for packet n
- WEP approach: initialize keystream with key + new IV for each packet:

WEP encryption (1)

- sender calculates Integrity Check Value (ICV, four-byte hash/CRC over data
- each side has 104-bit shared key
- sender creates 24-bit initialization vector (IV), appends to key: gives 128-bit key
- sender also appends keyID (in 8-bit field)
- 128-bit key inputted into pseudo random number generator to get keystream
- data in frame + ICV is encrypted with RC4:
  - bytes of keystream are XORed with bytes of data & ICV
  - IV & keyID are appended to encrypted data to create payload
  - payload inserted into 802.11 frame

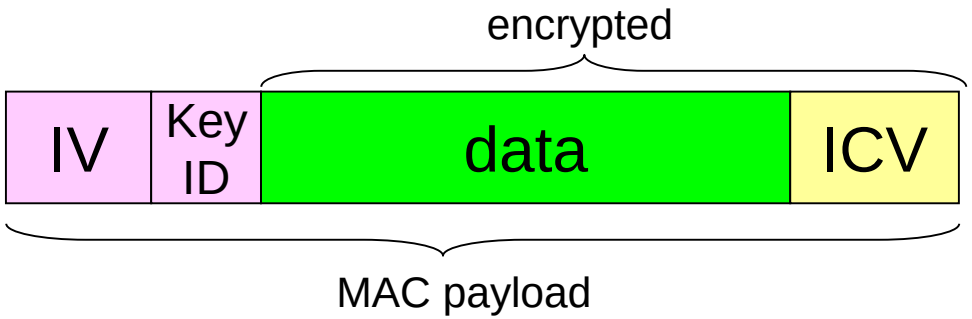


WEP encryption (2)



new IV for each frame

WEP decryption overview

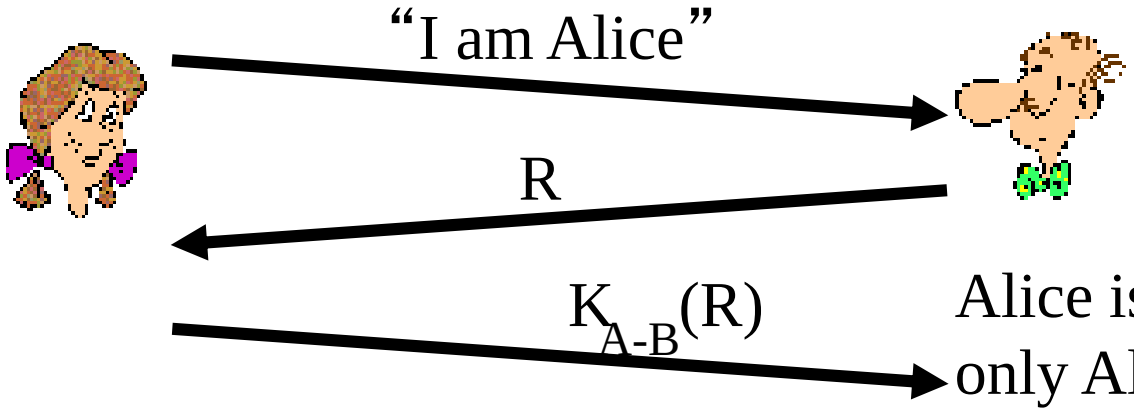


- receiver extracts IV
- inputs IV, shared secret key into pseudo random generator, gets keystream
- XORs keystream with encrypted data to decrypt data + ICV
- verifies integrity of data with ICV

End-point authentication w/ nonce

Nonce: number (R) used only *once –in-a-lifetime*

How to prove Alice "live": Bob sends Alice *nonce*, R. Alice must return R, encrypted with shared secret key



WEP authentication

authentication request

nonce (128 bytes)

nonce encrypted shared key

success if decrypted value equals nonce

Notes:

- not all APs do it, even if WEP is being used
- AP indicates if authentication is necessary in beacon frame
- done before association



Breaking 802.11 WEP encryption

security hole:

- 24-bit IV, one IV per frame, -> IV' s eventually reused
- IV transmitted in plaintext -> IV reuse detected

attack:

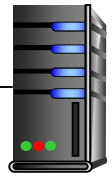
- Trudy causes Alice to encrypt known plaintext $d_1\ d_2\ d_3\ d_4\ \ldots$
- Trudy sees: $c_i = d_i$ XOR k_i^{IV}
- Trudy knows $c_i\ d_i$, so can compute k_i^{IV}
- Trudy knows encrypting key sequence $k_1^{IV}\ k_2^{IV}\ k_3^{IV}\ \ldots$
- Next time IV is used, Trudy can decrypt!

802.11i: four phases of operation

STA: client station

AP: access point

wired network



AS: Authentication server

1 Discovery of security capabilities

2 STA and AS mutually authenticate, together generate Master Key (MK). *AP serves as "pass through"*

3 STA derives Pairwise Master Key (PMK)

3 AS derives same PMK, sends to AP

4 STA, AP use PMK to derive Temporal Key (TK) used for message encryption, integrity