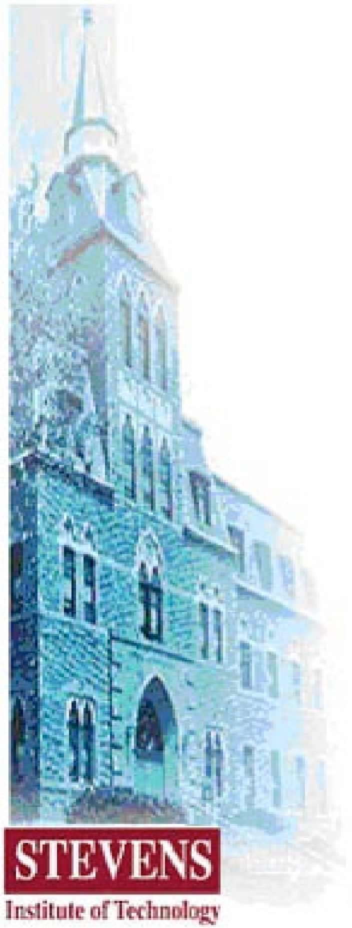


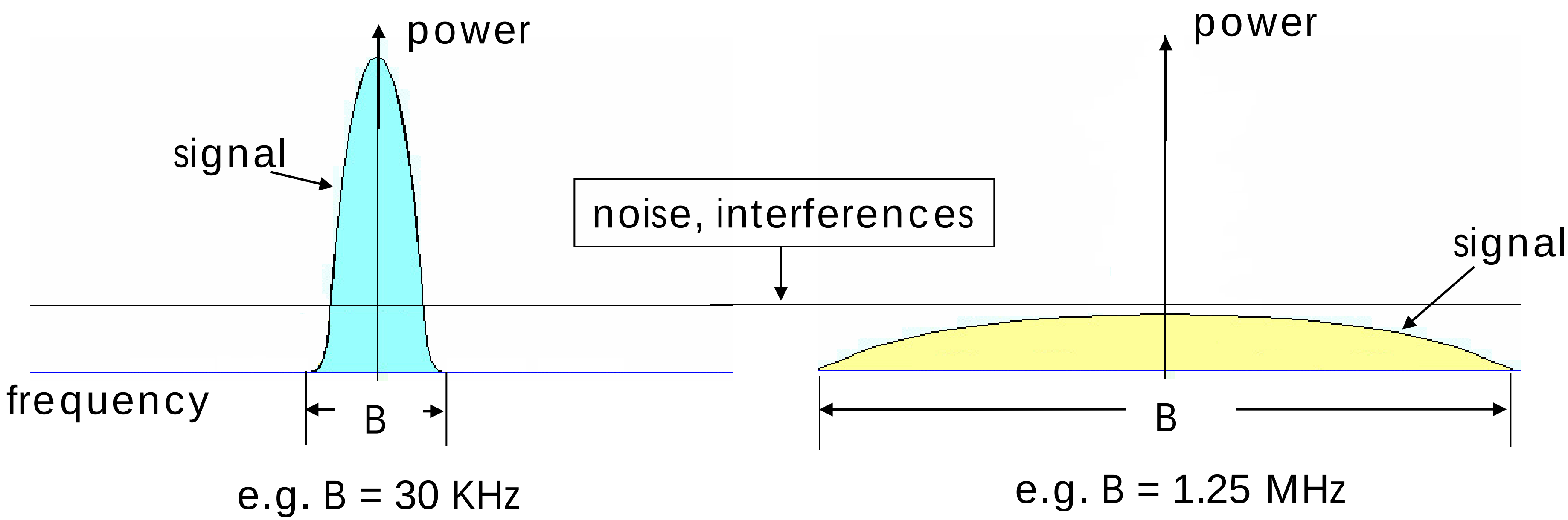
Wireless Communication Security

802.11 PHY Technologies

- Two kinds of radios based on
  - "Spread Spectrum"
  - "Diffused Infrared"
- Spread Spectrum radios based on
  - Frequency hopping (FH)
  - Direct sequence (DS)
- Radio works in 2.4GHz ISM band --- license-free by FCC (USA), ETSI (Europe), and MKK (Japan)
  - 1 Mbps and 2Mbps operation using FH
  - 1, 2, 5.5, and 11Mbps operation using DSSS (FCC)

Why Spread Spectrum ?

- C = B*log2(1+S/N) . . . [Shannon]
- To achieve the same channel capacity C
  - Large S/N, small B
  - Small S/N, large B
  - Increase S/N is inefficient due to the logarithmic relationship

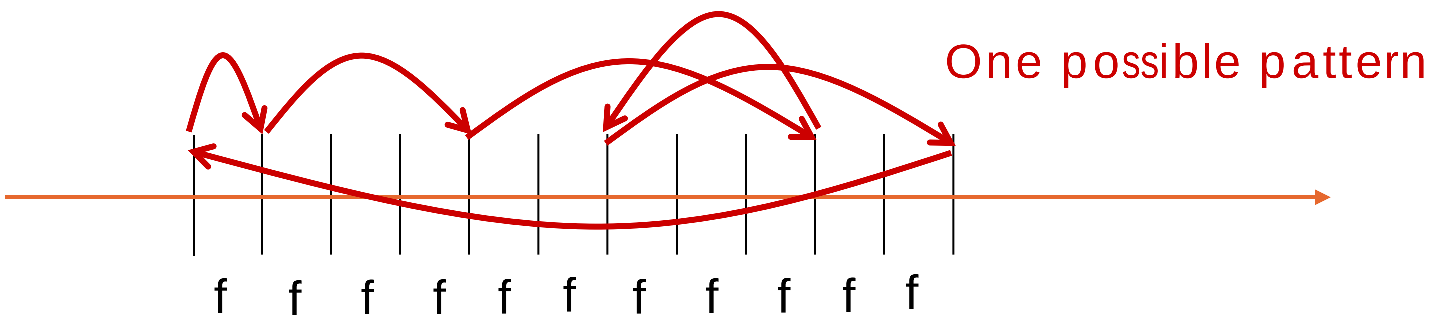


Spread Spectrum

- Methods for spreading the bandwidth of the transmitted signal over a frequency band (spectrum) which is wider than the minimum bandwidth required to transmit the signal.
- Reduce effect of jamming
  - Military scenarios
- Reduce effect of other interferences
- More “secure”
  - Signal “merged” in noise and interference

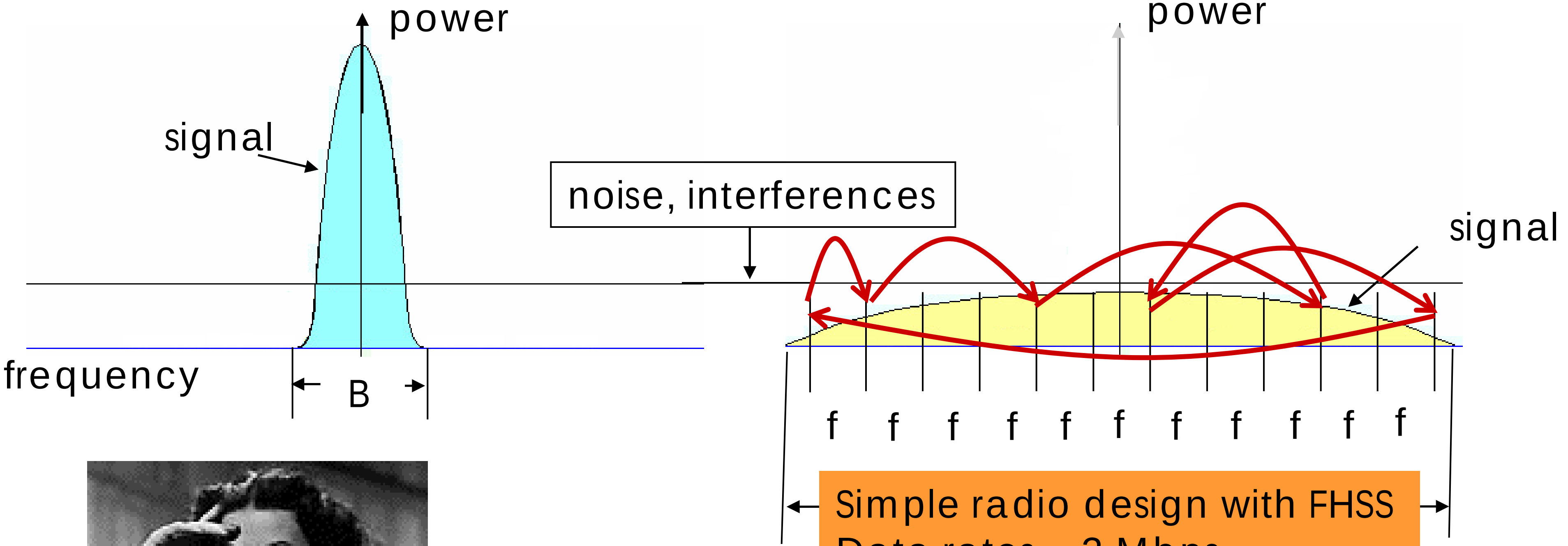
Frequency Hopping SS (FHSS)

- 2.4GHz band divided into 75 1MHz subchannels
- Sender and receive agree on a hopping pattern (pseudo random series). 22 hopping patterns defined



- Different hopping sequences enable co-existence of multiple BSSs
- Robust against narrow-band interferences

FHSS due to [Lamarr1940]



Simple radio design with FHSS
Data rates ~ 2 Mbps

Invented by Hedy Lamarr (Hollywood film star) in 1940, at age of 27, with musician George Antheil

Direct Sequence SS

- Direct sequence (DS): most prevalent
  - Signal is spread by a wide bandwidth pseudorandom sequence (code sequence)
  - Signals appear as wideband noise to unintended receivers

- Not for intra-cell multiple access
  - Nodes in the same cell use same code sequence

IEEE 802.11b DSSS

- ISM unlicensed frequency band (2.4GHz)
- Channel bandwidth: fhigh – flow = 22 MHz
- 1MHz guard band
- Direct sequence spread spectrum in each channel
- 3 non-overlapping channels

Channel	f_{low}	f_{high}
1	2.401	2.423
2	2.404	2.428
3	2.411	2.433
4	2.416	2.438
5	2.421	2.443
6	2.426	2.448
7	2.431	2.453
8	2.436	2.458
9	2.441	2.463
10	2.446	2.468
11	2.451	2.473

Diffused Infrared

- Wavelength range from 850 – 950 nm
- For indoor use only
- Line-of-sight and reflected transmission
- 1 – 2 Mbps

What is Different About Wireless Networks?

- Low bandwidth
  - minimize message sizes, number of messages
- Increased risk of eavesdropping
  - use link-level encryption ("wired equivalency")
- Also wireless networks typically imply **user/device mobility**
  - Security issues related to mobility
    - authentication
    - charging
    - privacy
  - Focus of this presentation

Traditional Security

- Wireless security can be broken into two parts: Authentication and encryption.
- Authentication mechanisms can be used to identify a wireless client to an access point and vice-versa.
- Encryption mechanisms ensure that it is not possible to intercept and decode data.
- For many years, MAC access control lists have been used for authentication, and 802.11 WEP has been used for encryption.

WLAN Security - Going Forward

- 802.11i appears to be a significant improvement over 802.11b from a security standpoint
- Vendors are nervous about implementing 802.11i protocols due to how quickly WEP was compromised after its release
- Only time will tell how effective 802.11i actually will be
- Wireless networks will not be completely secure until the standards that specify them are designed from the beginning with security in mind

802.11b: Built in Security Features

- Service Set Identifier (SSID)
- Differentiates one access point from another
- SSID is cast in ‘beacon frames’ every few seconds.
- Beacon frames are in plain text!

Associating with the AP

- Access points have two ways of initiating communication with a client
- Shared Key or Open Key authentication
- Open key: need to supply the correct SSID
  - Allow anyone to start a conversation with the AP
- Shared Key is supposed to add an extra layer of security by requiring authentication info as soon as one associates

How Shared Key Auth. works

- Client begins by sending an association request to the AP
- AP responds with a challenge text (unencrypted)
- Client, using the proper WEP key, encrypts text and sends it back to the AP
- If properly encrypted, AP allows communication with the client

Wired Equivalent Privacy (WEP):

- Authentication as in protocol ap4.0
  - host requests authentication from access point
  - access point sends 128 bit nonce
  - host encrypts nonce using shared symmetric key
  - access point decrypts nonce, authenticates host
- No key distribution mechanism
- Authentication: knowing the shared key is enough

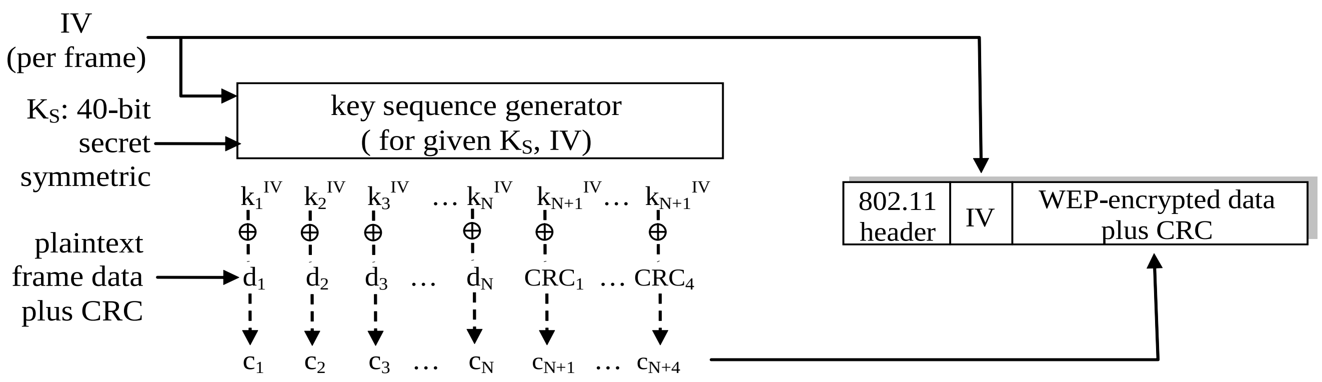
WEP data encryption

- Host/AP share 40 bit symmetric key (semi-permanent)
- Host appends 24-bit initialization vector (IV) to create 64-bit key
- 64 bit key used to generate stream of keys, k_i^{IV}
- k_i^{IV} used to encrypt ith byte, d_i, in frame:

$$c_i = d_i \text{ XOR } k_i^{IV}$$

- IV and encrypted bytes, c_i sent in frame

802.11 WEP encryption



Sender-side WEP encryption

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 …
  - 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} …
  - Next time IV is used, Trudy can decrypt!

Case study of a non-trivial attack

- Target Network: a large, very active university based WLAN
- Tools used against network:
  - Laptop running Red Hat Linux v.7.3,
  - Orinoco chipset based 802.11b NIC card
  - Patched Orinoco drivers
  - Netstumbler
    - Netstumbler can not only monitor all active networks in the area, but it also integrates with a GPS to map AP's
  - Airsnort
    - Passively listen to the traffic
- NIC drivers MUST be patched to allow Monitor mode (listen to raw 802.11b packets)

Assessing the Network

- Using Netstumbler, the attacker locates a strong signal on the target WLAN
- WLAN has no broadcasted SSID
- Multiple access points
- Many active users
- Open authentication method
- WLAN is encrypted with 40bit WEP

Cracking the WEP key

- Attacker sets NIC drivers to Monitor Mode
- Begins capturing packets with Airsnort
- Airsnort quickly determines the SSID
- Sessions can be saved in Airsnort, and continued at a later date so you don’t have to stay in one place for hours
- A few 1.5 hour sessions yield the encryption key
- Once the WEP key is cracked and his NIC is configured appropriately, the attacker is assigned an IP, and can access the WLAN

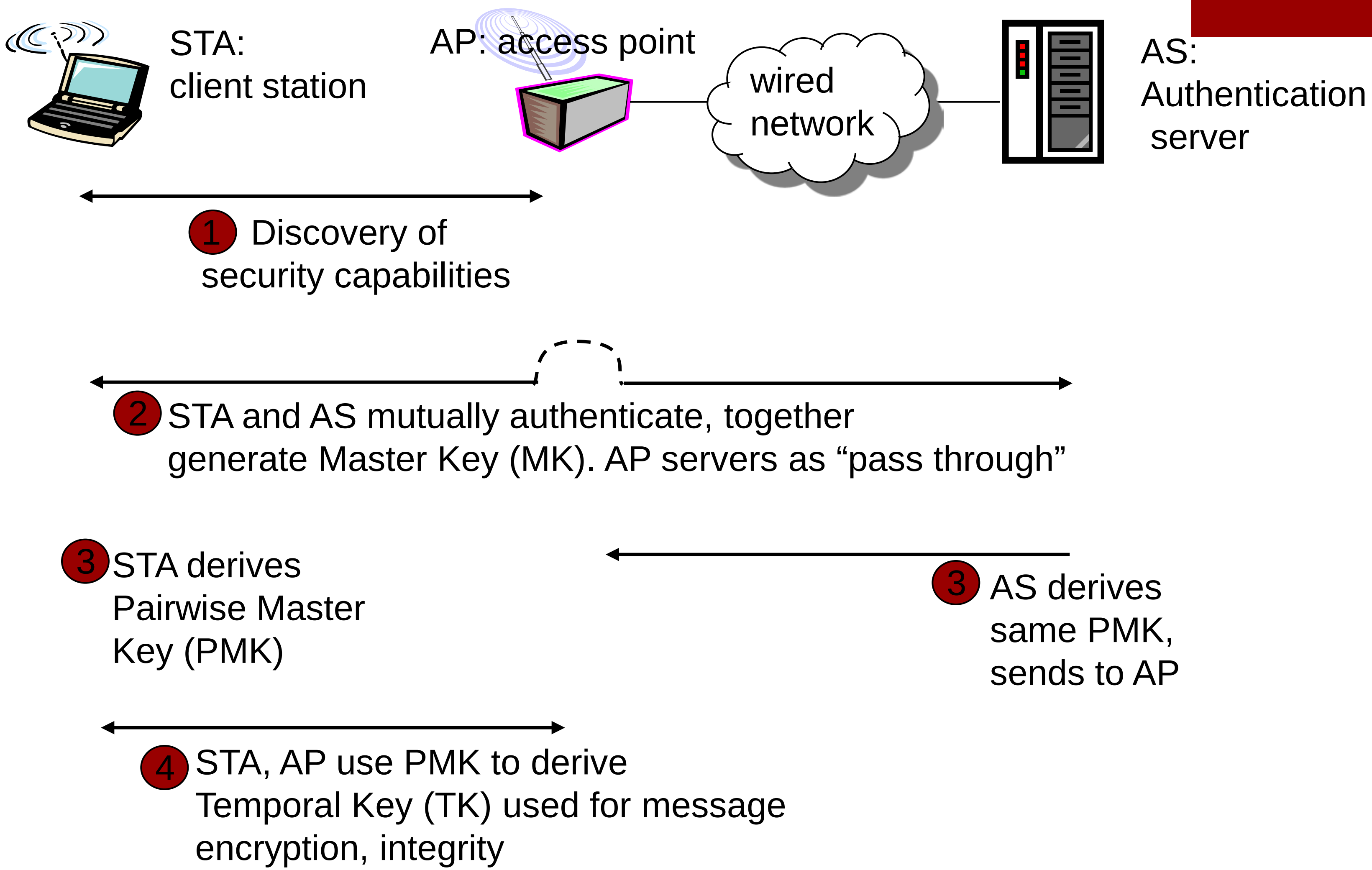
More Attacks in Wireless Networks

- Rogue Access Point
  - Solution: Monitor the air space for unexpected AP
- Radio Frequency (RF) Interference
- AP Impersonation
  - Rogue AP spoofs its MAC address to the identity of an authorized AP
  - Man-in-the-middle attack
  - Denial of service attack

802.11i: improved security

- numerous (stronger) forms of encryption possible
- provides key distribution
- uses authentication server separate from access point

802.11i: Four Phases of Operation



EAP: extensible authentication protocol

- EAP: end-end client (mobile) to authentication server protocol
- EAP sent over separate “links”
  - mobile-to-AP (EAP over LAN)
  - AP to authentication server (RADIUS over UDP)