

Wireless LANs (IEEE 802.11- Wi-Fi). An overview

Wireless LAN components

802.11 focuses on Layer 1 & Layer 2 of the OSI model.

- Wireless station: A desktop, laptop or any other device capable of interfacing with a wireless NIC.
- Access point: A bridge between wireless and wired networks. Usually composed of:
 - 1) Radio
 - 2) Wired network interface (usually 802.3)
 - 3) Bridging software

Aggregates access for multiple wireless stations.

802.11 modes

Wi-Fi supports two modes of operation:

- Infrastructure mode
 - Basic Service Set (BSS): One access point
 - Extended Service Set: Two or more BSSs forming a single subnet
- Ad-hoc mode (or Peer-to-peer)
 - Independent Basic Service Set (IBSS): Set of 802.11 wireless stations that communicate directly without an access point.

802.11 Physical Layer

There are three alternative physical layers:

- Two incompatible spread-spectrum radio in 2.4GHz ISM band:
 - 1) Frequency Hopping Spread Spectrum (FHSS): 75 channels
 - 2) Direct Sequence Spread Spectrum (DSSS): 14 channels (11 in the US)
- One diffuse infrared layer

Radio speed and Range:

- 802.11 at 1Mbps or 2Mbps
- 802.11b at 5Mbps or 11Mbps (only DSSS so limited to 14 channels). Offers also dynamic rate shifting which is transparent to higher layers. Ideally 11Mbps but sifts down through 5.5Mbps, 2Mbps to 1Mbps. To support higher range and channel interference. Speed shifts back when possible/
- 802.11a at 5GHz radio spectrum with max speed of 54Mbps. Also more energy efficient.
- 802.11g more speed at 2.4GHz spectrum
- 802.11e offers better support for Multimedia and QoS
- 802.11i offers better security
- Range is typically 100 metres

802.11 DataLink Layer

Layer 2 is split to LLC and MAC. LLC provides same 48bit address as 802.3.

At the MAC layer CSMA/CD is not possible so alternative approach is used instead CSMA/CA.

CSMA/CA (Collision Avoidance)

- Sender waits for clear air, waits random time and then sends data.
- Receiver sends explicit ACK when data arrives intact.
- Also handles interference (But adds overhead)

In infrastructure mode 802.11 has the ability to handle hidden nodes.

- Sending station sends 'Request to send'
- Access point responds with "Clear to send" (all other stations hear this and delay any transmissions)
- Only used for larger pieces of data (When retransmission may waste significant time)

Joining a Basic Service Set (BSS)

Access Points (APs) send beacons. AP beacons can include SSID (Service Set ID). When client enters range of one or more APs:

- AP chosen on signal strength and observed error rates
- After AP accepts client, clients tunes in to AP channel.
- Periodically client surveys all channels to check for stronger or more reliable APs
- If found it reassociates with new AP

Reassociation with APs occurs when :

- Client moves out of range
- High error rates
- High network traffic (allows for load balancing)

Each AP has 14 overlapping channels. There are only 3 channels that have no overlap (Best for multicell coverage).

Wi-Fi Security features/vulnerabilities

- **Open System Authentication**
 - Service Set Identifier (SSID)
 - APs can broadcast their SSID
 - Station must specify SSID to Access Point when requesting association
 - Multiple APs with same SSID form Extended Service Set
 - Some 802.11b clients allow * as SSID. Associates with strongest AP regardless of SSID
- **MAC address locking**
 - APs have ACLs
 - ACLs are a list of allowed MAC addresses

BUT

- **MAC addresses are sniffable and spoofable**
 - **AP ACLs are an ineffective control**
- **Wireless LAN uses radio signal**
 - **Not limited to physical building**
 - **Signal is weakened by walls. Floors, interference**
 - **Directional antenna allows interception over long distances. Directional antenna provides focused reception. DIY plans are available (Aluminium cake tin, 11Mbps at 750 metres)**
 - **Wardriving software : Netstumbler, THC-Wardrive, Wavemon. Logging of MAC addresses, Network name, SSID, manufacturer, channel, signal strength, noise.**

Wi-Fi Issues

- **Access Point configuration (SNMP, web, serial, telnet)**
- **Evil Twin Access Points (stronger signal captures user authentication)**
- **Hub broadcasts (If AP connected to a hub all traffic in the air)**
- **Renegade Access Points (Unauthorized wireless LANs)**

802.11b Security Services

Two security services provided:

- Authentication (Shared key authentication)
- Encryption (Wired Equivalent Privacy WEP)

WEP (Authentication)

- Shared key between Stations and APs
- Extended Service Set: All APs will have same shared key
- No key management: Shared key must be entered manually into Stations, APs (scalability?)

When station requests association with AP:

- AP sends random number to station
- Station encrypts random number (RC4, 40 bit shared secret & 24 bit IV)
- Encrypted random number send to AP
- AP decrypts the received message
- If numbers match station has shared secret key

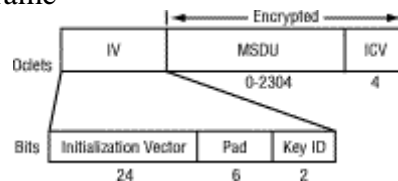
WEP (Integrity)

When a frame is send to a 802.11 device the device computes a 32 bit CRC and appends this to the plaintext frame. This is also called an Integrity Check Vector (ICV).

WEP (Confidentiality)

Figure 1 below shows a WEP encrypted data frame. The first 24 bits of the frame are known as the Initialization Vector, or the IV. The IV is to guarantee that the same plaintext data frame will never generate the same WEP encrypted data frame. How the IV changes depends on the vendor implementation. The Cisco Aironet solution changes the IV on a per packet basis.

Figure 1: WEP Encrypted Data Frame



The IV is at the center of most of the issues involving WEP. Because the IV is transmitted as plaintext and appended to the WEP-encrypted frame, anyone sniffing a WLAN can see the IV. At 24 bits long, the IV provides a range of 16,777,216 possible values. When the same IV is used with the same key on an encrypted packet (known as an IV collision), a hacker can capture the data frames and derive information about the data as well as the network.

Attacks on WEP

- Passive attack: A passive eavesdropper can intercept all wireless traffic, until an IV collision occurs. By XORing two packets that use the same IV, the attacker obtains the XOR of the two plaintext messages. The resulting XOR can be used to infer data about the contents of the two messages. IP traffic is often very predictable and includes a lot of redundancy.
- Active attack: The following attack is also a direct consequence of the problems described in the previous section. Suppose an attacker knows the exact plaintext for one encrypted message. He can use this knowledge to construct correct encrypted packets. The procedure involves constructing a new message, calculating the CRC-32, and performing bit flips on the original encrypted message to change the plaintext to the new message. The basic property is that $RC4(X) \text{ xor } X \text{ xor } Y = RC4(Y)$. This packet can now be sent to the access point or mobile station, and it will be accepted as a valid packet.
- Limited WEP keys: Some vendors allow limited WEP keys. WEP key is generated from passphrase. Passphrase creates only 21 bits of entropy in 40 bit key. Thus it reduces key strength to 21 bits. The rest of the 19 bits are predictable. 21 bit key can be bruteforced in minutes.
 - Capture ciphertext (IV is included in the message)
 - Search all possible 2^{40} possible secret keys
 - Find which key decrypts ciphertext to plaintext
 - Network traffic is highly redundant. Some known packets appear all the time.

128 bit WEP

104 bit secret key

24 bit IV

Brute force takes 10^{19} years for 104 bit key

BUT

- Certain keys leak into key stream
- If portion of the PRNG input is exposed, analysis of initial keystream allows key to be determined. IV weakness
- WEP exposes part of PRNG (IV is transmitted with message)
- Attack is practical for 40 and 128 bit keys.

Airsnort (Open Source)

802.11 Safeguards

- Security Policy & Architecture design
- Treat as untrusted LAN (Firewall between WLAN and backbone, IDS, Extra authentication)
- Discover unauthorized use (Unauthorized APs, Port scanning, Warwalking)
- Station protection (VPNs, IDS, are stations securely configured?)
- AP audits (SSID & password policy, WEP keys, Firewall and router ACL)
- AP location (Centre of buildings, avoid LOS to outside)
- Antenna design (directional antennas)

Conclusion

The recent security attacks on WLANs indicated numerous vulnerabilities in WEP and increased awareness on the need for sophisticated key management solutions. Vendors and the 802.11 standards body are working to refine and improve existing security to overcome

the recently discovered WEP shortcomings.