Wireless Networks
Lecture 17: Wireless LANs
802.11 Management

Peter Steenkiste
CS and ECE, Carnegie Mellon University

Peking University, Summer 2016

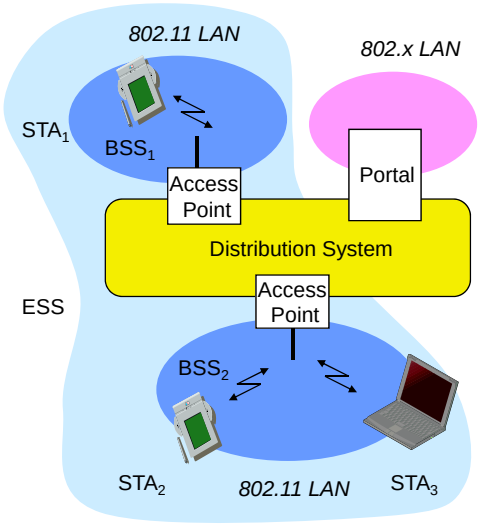
Outline

- Brief history
- 802 protocol overview
- Wireless LANs – 802.11 – overview
- 802.11 MAC, frame format, operations
- 802.11 management
- 802.11 security
- 802.11 power control
- 802.11*
- 802.11 QoS

Management and Control Services

- Association management
- Handoff
- Security: authentication and privacy
- Power management
- QoS

802.11: Infrastructure Reminder



- **Station (STA)**
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- **Access Point**
  - station integrated into the wireless LAN and the distribution system
- **Basic Service Set (BSS)**
  - group of stations using the same AP
- **Portal**
  - bridge to other (wired) networks
- **Distribution System**
  - interconnection network to form one logical network (ESS: Extended Service Set) based on several BSS

Service Set Identifier - SSID

- Mechanism used to segment wireless networks
  - » Multiple independent wireless networks can coexist in the same location
  - » Effectively the name of the wireless network
- Each AP is programmed with a SSID that corresponds to its network
- Client computer presents correct SSID to access AP
- Security Compromises
  - » AP can be configured to “broadcast” its SSID
  - » Broadcasting can be disabled to improve security
  - » SSID may be shared among users of the wireless segment

Association Management

- Stations must associate with an AP before they can use the wireless network
  - » AP must know about them so it can forward packets
  - » Often also must authenticate
- Association is initiated by the wireless host – involves multiple steps:
  1. Scanning: finding out what access points are available
  2. Selection: deciding what AP (or ESS) to use
  3. Association: protocol to “sign up” with AP – involves exchange of parameters
  4. Authentication: needed to gain access to secure APs – manyoptions possible
- Disassociation: station or AP can terminate association

Association Management: Scanning

- Stations can detect AP based by scanning
- Passive Scanning: station simply listens for Beacon and gets info of the BSS
  - Beacons are sent roughly 10 times per second
  - Power is saved
- Active Scanning: station transmits Probe Request; elicits Probe Response from AP
  - Saves time + is more thorough
  - Wait for 10-20 msec for response
- Scanning all available channels can become very time consuming!
  - Especially with passive scanning
  - Cannot transmit and receive frames during most of that time – not a big problem during initial association

Association Management: Selecting an AP and Joining

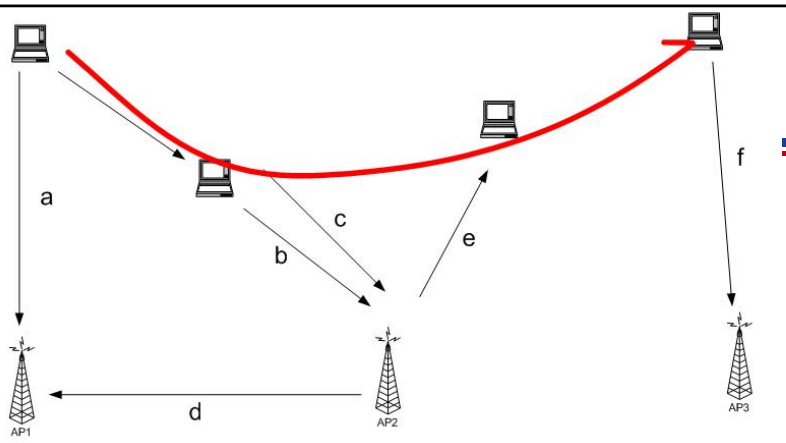
- Selecting a BSS or ESS typically must involve the user
  - What networks do you trust? Are you willing to pay?
  - Can be done automatically based on stated user preferences (e.g. the "automatic" list in Windows)
- The wireless host selects the AP it will use in an ESS based on vendor-specific algorithm
  - Uses the information from the scan
  - Typically simply joins the AP with the strongest signal
- Associating with an AP
  - Synchronization in Timestamp Field and frequency
  - Adopt PHY parameters
  - Other parameters: BSSID, WEP, Beacon Period, etc.

Association Management: Roaming

- Reassociation: association is transferred from active AP to a new target AP
  - Supports mobility in the same ESS – layer 2 roaming
- Reassociation is initiated by wireless host based on vendor specific algorithms
  - Implemented using an Association Request Frame that is sent to the new AP
  - New AP accepts or rejects the request using an Association Response Frame
- Coordination between APs is defined in 802.11f
  - Allows forwarding of frames in multi-vendor networks
  - Inter-AP authentication and discovery typically coordinated using a RADIUS server
  - "Fast roaming" support (802.11r) also streamlines authentication and QoS, e.g. for VoIP

Association Management: Reassociation Algorithms

- Failure driven: only try to reassociate after connection to current AP is lost
  - Typically efficient for stationary clients since it not common that the best AP changes during a session
  - Mostly useful for nomadic clients
  - Can be very disruptive for mobile devices
- Proactive reassociation: periodically try to find an AP with a stronger signal
  - Tricky part: cannot communicate while scanning other channels
  - Trick: user power save mode to "hold" messages
  - Throughput during scanning is still affected though
    - Mostly affects latency sensitive applications



(a) ---- The station finds AP1, it will authenticate and associate.

(b) ---- As the station moves, it may pre-authenticate with AP2.

(c) ---- When the association with AP1 is no longer desirable, it may reassociate with AP2.

(d) ---- AP2 notify AP1 of the new location of the station, terminates the previous association with AP1.

(e) ---- At some point, AP2 may be taken out of service. AP2 would disassociate the associated stations.

(f) ---- The station find another access point and authenticate and associate.

Outline

- **Brief history**
- **802 protocol overview**
- **Wireless LANs – 802.11 – overview**
- **802.11 MAC, frame format, operations**
- **802.11 management**
- **802.11 security**
- **802.11 power control**
- **802.11***
- **802.11 QoS**

WLAN Security Requirements

- Authentication: only allow authorized stations to associate with and use the AP
- Confidentiality: hide the contents of traffic from unauthorized parties
- Integrity: make sure traffic contents is not modified while in transit

WLAN Security Exploits

- Insertion attacks: unauthorized Clients or AP
  - » Client: reuse MAC or IP address –free service on "secured" APs
  - » AP: impersonate an AP, e.g., use well known name
- Interception and unauthorized monitoring
  - » Packet Analysis by "sniffing" – listening to all traffic
- Brute Force Attacks Against AP Passwords
  - » Dictionary Attacks Against SSID
- Encryption Attacks
  - » Exploit known weaknesses of WEP
- Misconfigurations, e.g., use default password
- Jamming – denial of service
  - » Cordless phones, baby monitors, leaky microwave oven, etc.

Security in 802.11b

- WEP: Wired Equivalent Privacy
  - » Achieve privacy similar to that on LAN through encryption
  - » Intended to provide both privacy and integrity
  - » RC4 and CRC32
  - » Has known vulnerabilities
- WPA: Wi-Fi Protected Access
  - » Larger, dynamically changed keys
- 802.1x: port-based authentication for LANs
  - » Port-based authentication for LANs
- 802.11i (WPA2)
  - » Builds on WPA
  - » Uses AES for encryption

MAC Filtering

- Each client is identified by its 802.11 Mac Address
- Each AP can be programmed with the set of MAC addresses it accepts ("white list")
- Combine this filtering with the AP's SSID
- Very simple solution
  - » Some overhead to maintain list of MAC addresses
- But it is possible to forge MAC addresses …
  - » Unauthorized client can "borrow" the MAC address of an authenticated client
  - » Built in firewall will discard unexpected packets

Wired Equivalent Privacy WEP

- Original standard for WiFi security
- Very weak standard: key could be cracked with a couple of hours of computing (much faster today)
  - » Too much information is transmitted in the clear
  - » No protocol for encryption key distribution
  - » Clever optimizations can reduce time to minutes
- All data then becomes vulnerable to interception
  - » WEP typically uses a single shared key for all stations
- The CRC32 check is also vulnerable so that the data could be altered as well
  - » Can makes changes without even decrypting!
- 128-bit WEP encryption is recommended

Port-based Authentication

- 802.1x is the IEEE standard for port-based authentication
- Users get a username/password to access the access point
- Was originally defined for switches but extended to APs
- Can be used to bootstrap other security mechanisms
  - » Effectively creating a session

Wi-Fi Protected Access WPA

- Introduced by Wi-Fi Alliance as an interim solution after WEP flaws were published
  - Uses a different Message Integrity Check
  - Encryption still based on RC4, but uses 176 bit key (48bit IV) and keys are changed periodically
  - Also frame counter in MIC to prevent replay attacks.
- Can be used with 802.1x authentication (optional)
  - It generates a long WPA key that is randomly generated, uniquely assigned and frequently changed.
  - Attacks are still possible since people sometimes use short, poorly random WPA keys that can be cracked
- 802.11i is a "permanent" security fix
  - Builds on the interim WPA standard (i.e. WPA2)
  - Replaces RC4 by the more secure Advanced Encryption Standard (AES) block encryption
  - Better key management and data integrity
  - Uses 802.1x for authentication.

Authentication in WLAN Hotspots

- Upon association with the AP, only authentication traffic can pass through, as defined by IEEE 802.1x

- The protocol used to transport authentication traffic is the Extensible Authentication Protocol (EAP - RFC3748)

Dual SSID Approach