Network Security: WLAN Security

Mohit Sethi
Ericsson, Finland
Aalto University, Finland

WLAN Security - Outline

- Part 1:
  - WLAN Standards and Components
  - Joining Open WLAN
  - WPA2-PSK and four-way handshake
  - WPA 3: Opportunistic Wireless Encryption (Enhanced Open)
  - WPA 3: Password Authenticated Key Exchange (PAKE : Dragonfly)
  - Enterprise wireless security - EAP

WLAN Standards

- IEEE 802.11 standard defines physical and link-layer for wireless Ethernet
- Wi-Fi is an industry alliance to promote 802.11 interoperability
- Original 802.11-1997, latest 802.11-2020, many amendments
- Physical layer:
  - Uses unlicensed bands at 2.4 GHz (microwave ovens, Bluetooth) and 5 GHz
  - Up to 14 radio channels in the 2.4 GHz band, but only about 3 non-overlapping ones
- Link layer
  - Looks like Ethernet (802.3) to layers above
  - MAC protocol differs from 802.3 because one antenna cannot detect collisions while transmitting
    → explicit ACKs needed

WLAN Components

- Access point (AP) = bridge between wireless (802.11) and wired (802.3) networks
- Wireless station (STA) = PC or other device with a wireless network interface card (NIC)
  - To be precise, AP is also a STA
- Stations are identified by globally unique 48-bit MAC address
  - MAC = Medium Access Control, don't confuse with message authentication code
  - MAC address is assigned to each network interface card (NIC) by the manufacturer, which gets them from IEEE
- Infrastructure mode = wireless stations communicate only with AP
- Ad-hoc mode = no AP; wireless stations communicate directly with each other
- We will focus on infrastructure-mode WLANs

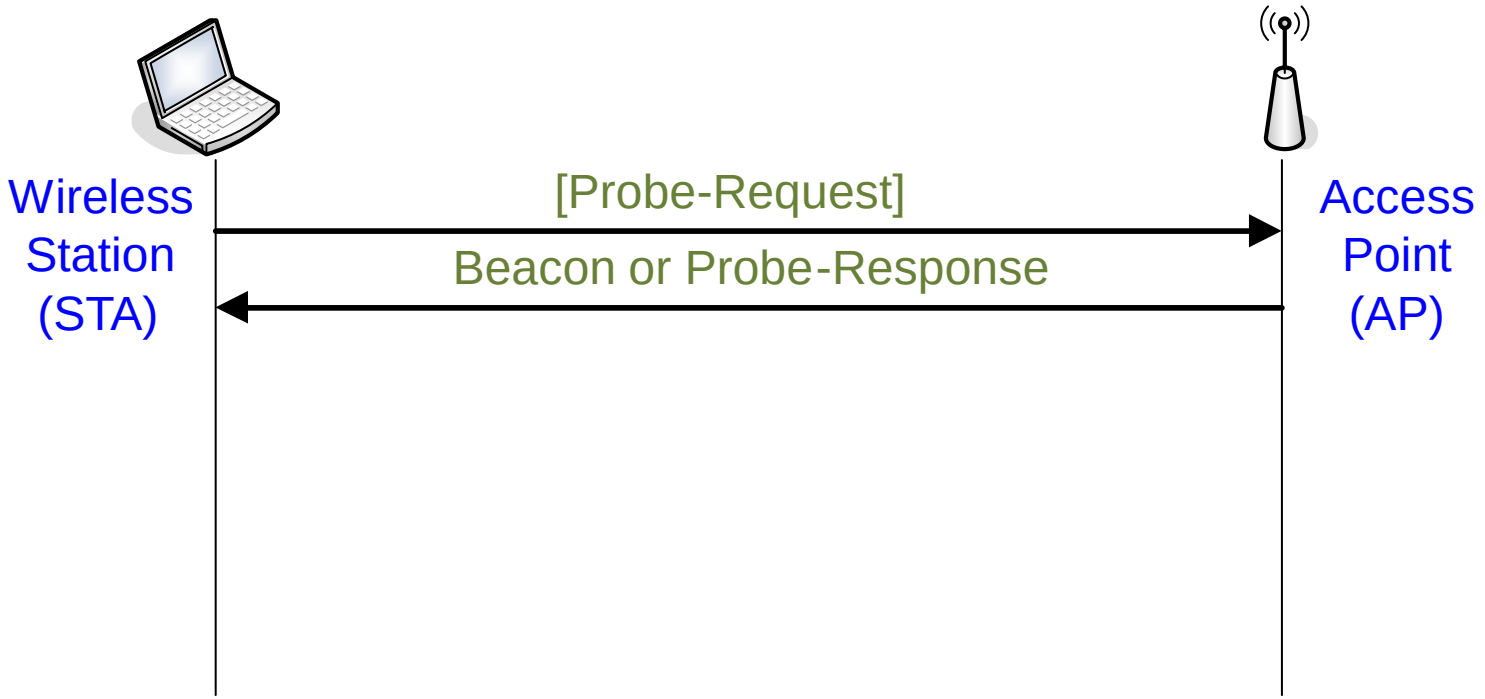
WLAN Structure

- Basic service set (BSS) = one WLAN cell (one AP + other wireless stations)
- The basic service set is identified by basic service set identifier (BSSID) = AP MAC address
- Extended service set (ESS) = multiple cells where the APs have the same service set identifier (SSID)
- The wired network is called distribution network in the standard; typically it is wired Ethernet
- APs in the same ESS can belong to the same IP network segment, or to different ones

Joining an open WLAN

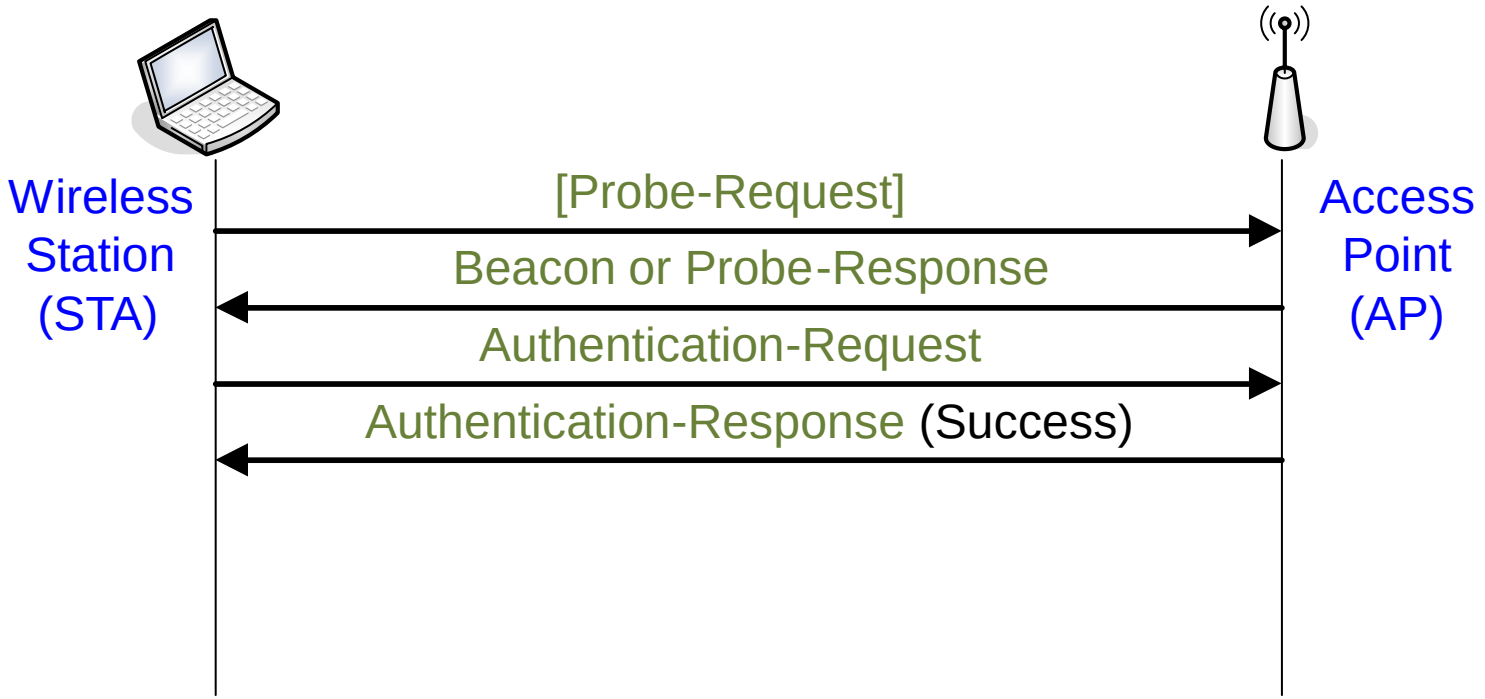
Joining an open WLAN

- AP sends beacons, usually every 50 ms
- Beacons usually include the SSID but broadcast can be turned off



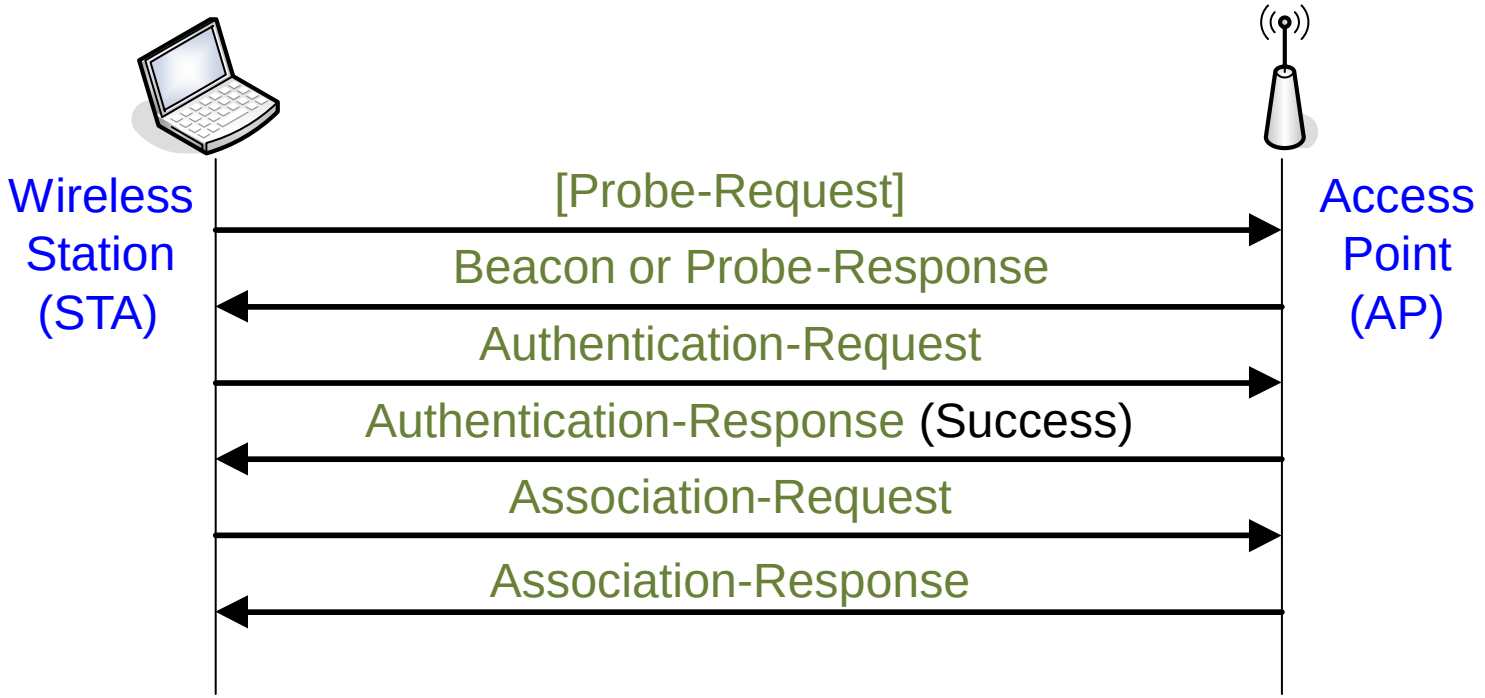
Joining an open WLAN

- AP sends beacons, usually every 50 ms
- Beacons usually include the SSID but broadcast can be turned off



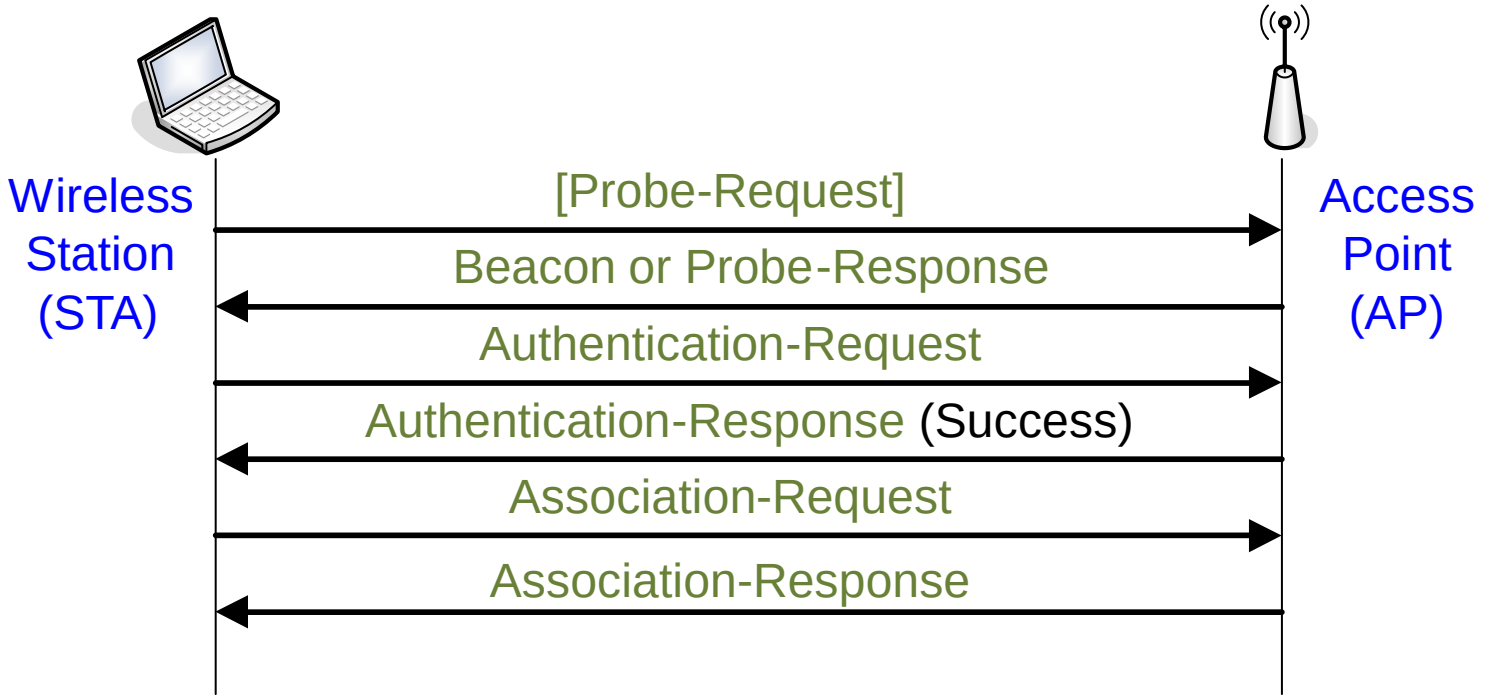
Joining an open WLAN

- AP sends beacons, usually every 50 ms
- Beacons usually include the SSID but broadcast can be turned off



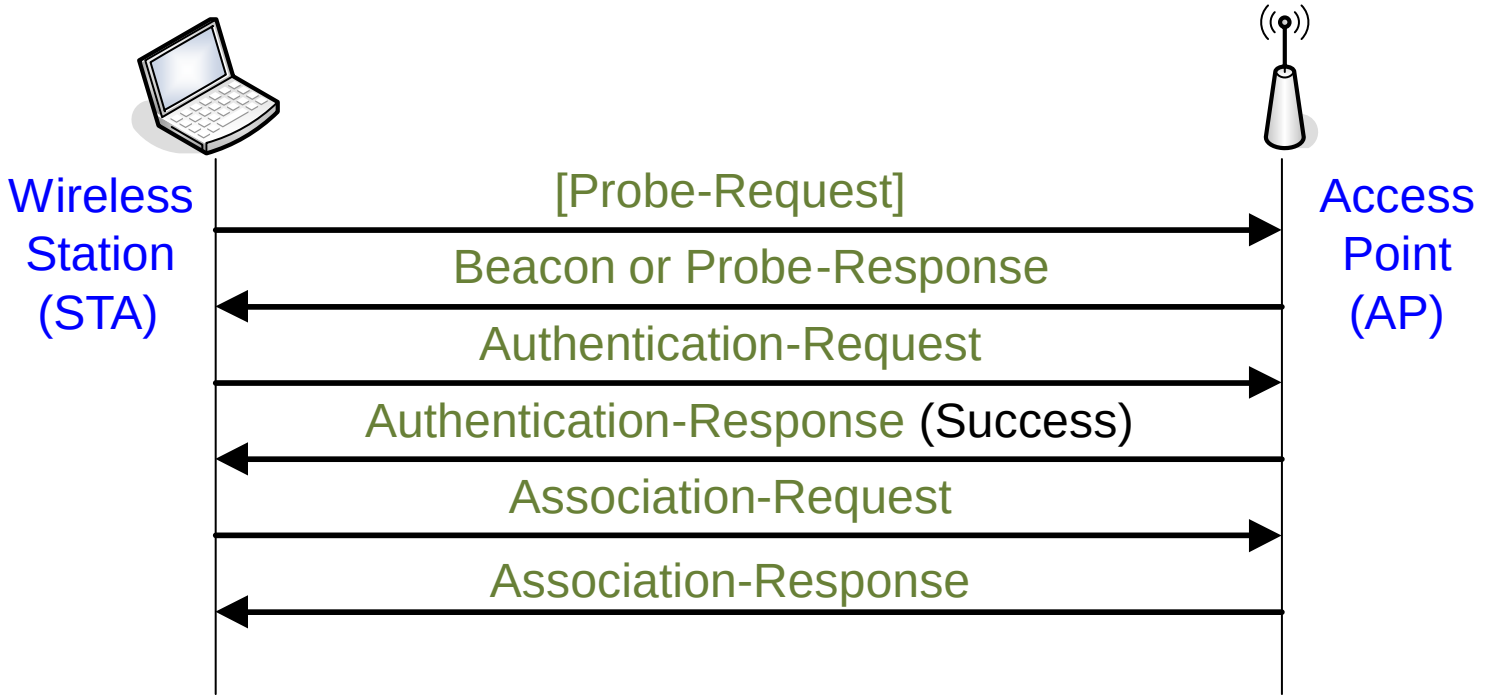
Joining an open WLAN

- AP sends beacons, usually every 50 ms
- Beacons usually include the SSID but broadcast can be turned off
- STA must specify SSID to the AP in association request



Joining an open WLAN

- AP sends beacons, usually every 50 ms
- Beacons usually include the SSID but broadcast can be turned off
- STA must specify SSID to the AP in association request



- Open system authentication = **no authentication**, empty authentication messages

Leaving a WLAN

- Both STA and AP can send a Disassociation Notification or Deauthentication Notification
- Include reason codes
  - station inactivity
  - station leaving