Module Eight

CSG1105 Applied Communications

Wireless Networking

- Wireless Networking uses the **Electromagnetic spectrum** (EM) for signalling
  - Radio frequencies: Many - Wi-Fi, WiMAX, Cellular, Bluetooth, Microwave, Satellite
  - Light: LASER, Infrared
- Wireless is used in circumstances where a cable is impractical, inconvenient or too expensive
  - Bridging physical barriers
  - Networking heritage structures
  - Enabling mobile computing
  - Ad-hoc connection

ALOHA Net

- The first wireless network began development in 1968 to connect the Hawaiian island of Oahu to other islands to allow the use of a time-sharing mainframe computer
- The ALOHA Net protocol allowed multiple stations to access a shared medium (the radio frequency) without the need for a central hub
- This protocol became the model that was used to develop CSMA/CD as used for 802.3 (Ethernet)

Wireless Technologies 1

- Wireless technologies provide the **Network Access Layer** (Datalink and Physical in the OSI model)
- The Internetwork, Transport and Application layers operate as they do for Ethernet and other physical media
- Solutions such as cellular use an existing network stack as a network access layer

Wireless Technologies 2

- Infrared (IR)
  - IR frequencies are situated between microwave and visible light
  - IR is short range, requires line-of-sight (LoS) and is blocked by physical barriers
  - Low data rates
  - Not commonly used for data networks
- LASER
  - LASER is coherent light, where a beam diverges far less than non-coherent light
  - LASERs may be used for point-to-point (p2p) connections where LoS is possible
  - Connections generally under a kilometre at useful speeds
  - LASER is mostly used to bridge networks where a physical or legal barrier prevents cabling
  - Heavily impacted by atmospheric conditions (rain, fog, smoke etc)

Wireless Technologies 3

- Satellite
  - Satellite networks are used for voice, video and data
  - Requires the launch of a satellite(s) into either low earth orbit (LEO) or geosynchronous orbit
  - Some connections relayed through multiple satellites
  - Allows distant locations with no LoS to be connected
  - Requires ground stations with appropriate antenna and transceiver
  - Expensive, high latency - used where other options impractical (eg remote mining sites)

Wireless Technologies 4

- Cellular
  - Uses the Cell Phone network (GSM, 3G, 4G, 5G) for data communications
  - Works anywhere reception of a provider is available
  - Provides mobile computing access with transceiver swapping cell towers as it moves
  - Used for Internet connection where cabled connection impractical, often used for remote monitoring (eg medical devices such as CPAP)
  - Data is expensive compared to wired Internet solutions

WiMAX

- A wireless Broadband communication standard (IEEE 802.16) using microwave frequencies
- Often used as a replacement for the 'last mile' of Internet broadband access as an alternative to VDSL or Cellular
- Requires appropriate antenna and interface equipment
- Provides access where cabled connection too slow or not available
- Requires LoS to tower point of presence (PoP)
- Usually requires installation of an external antenna
- Perth Internet provider PentaNet uses AirMAX, a similar last mile protocol

Bluetooth

- A **Personal Area Network (PAN)** protocol documented in IEEE 802.15.1
- Used for short distance ad-hoc connections between devices
- Bluetooth is low power protocol also operating in the 2.4 GHz band
- Commonly used for connecting peripherals like headphones, graphics tablets etc to computers
- May be used for local data connections (eg connecting a laptop to a cell phone to use as an Internet connection)
- May be used for file transfer between devices
- A single master device may connect and control multiple slave devices
- Bluetooth networks are **not secure**

Wi-Fi

- Wi-Fi is a set of standards for wireless networking based on IEEE 802.11
- Wi-Fi is the dominant wireless LAN protocol in use
- It is used for mobile Internet including Cell phones, Tablets, Laptops, Printers and IoT (Internet of Things) devices
- There are multiple versions (approximately 18) of the protocol, each having enhancements over previous versions

Frequencies

- The IEEE 802.11 standards specify a number of frequencies for Wi-Fi
- The two most common frequency **bands** are:
  - 2.4 GHz
  - 5 GHz
- Within the frequency bands, there are multiple **channels**
- Depending upon the Country, the exact frequencies and channels may vary

2.4 GHz

- This band has 1-14 channels depending on the country (USA has 11, Japan 14)
- The 2.4 GHz band is not exclusively for Wi-Fi, it is also used for cordless phones (not mobiles), baby monitors, garage door remotes and remote control models. This may result in interference and poor performance

Range

- The 2.4 GHz Wi-Fi has a range of up to 45m indoors and 90m outdoors
- The construction materials of a building may influence the range

Speed

- Speeds are dependant upon the version of 802.11 supported, but range from 11 Mbps to 54 Mbps

5 GHz

- This band offers at least 23 channels, with variations depending upon the country
- Unlike, 2.4GHz, the 5 GHz band does not compete with other devices

Range

- The 5GHz Wi-Fi has a range about half that of 2.4GHz
- It is more susceptible to blockage by structures

Speed

- Speeds are dependant upon the version of 802.11 supported, but range from 54 Mbps to 6933 Mbps
- There are **dual band** (2.4 and 5 GHz) standards which support higher speeds

Modes

Ad Hoc

- Also know as **peer to peer**
- Allows devices to communicate without the use of an **Access Point (AP)**
- Requires each device to maintain status information regarding the network
- Does not scale well

Infrastructure

- Most Wi-Fi networks operate in Infrastructure mode
- All devices communicate via one or more Access Points

Connecting to a Infrastructure Network

- A wireless client, the **Station (STA)** connects to an **AP**. An AP is either connected to a cabled network or wirelessly connects to an AP that does
- When a an AP is connected to a wired network and a group of wireless stations, it is know as a **Basic Service Set (BSS)**. An **Extended Service Set (ESS)** is a group of BSS's that form a single subnet
- APs broadcast a **Beacon signal** every few milliseconds which includes the **Service Set Identifier (SSID).**
- When a client wireless NIC is power on, it scans for APs and associated SSID
- A client may be configured to automatically connect to a specified SSID.
- The client NIC switches to the assigned channel of the AP and negotiates a connection. This is called an **Association**.

Security

- Radio is a **Broadcast** medium, allowing any one with a receiver to intercept a signal
- Encryption is necessary to protect the information carried on the Wi-Fi network
- The original protocol for Wi-Fi encryption was **WEP** (Wired Equivalent Privacy). WEP used a 40 bit key and was soon found to be easily broken. WEP is only supported on **some** APs for legacy support and if needed, should be isolated to a separate subnet to all other traffic
- The first replacement for WEP was **WPA** (Wireless Protected Access) which used **TKIP** (Temporal Key Integrity Protocol)
- WPA was enhanced to use **AES** (Advanced Encryption Standard) encryption resulting in **WPA2**, the currently most used wireless security protocol

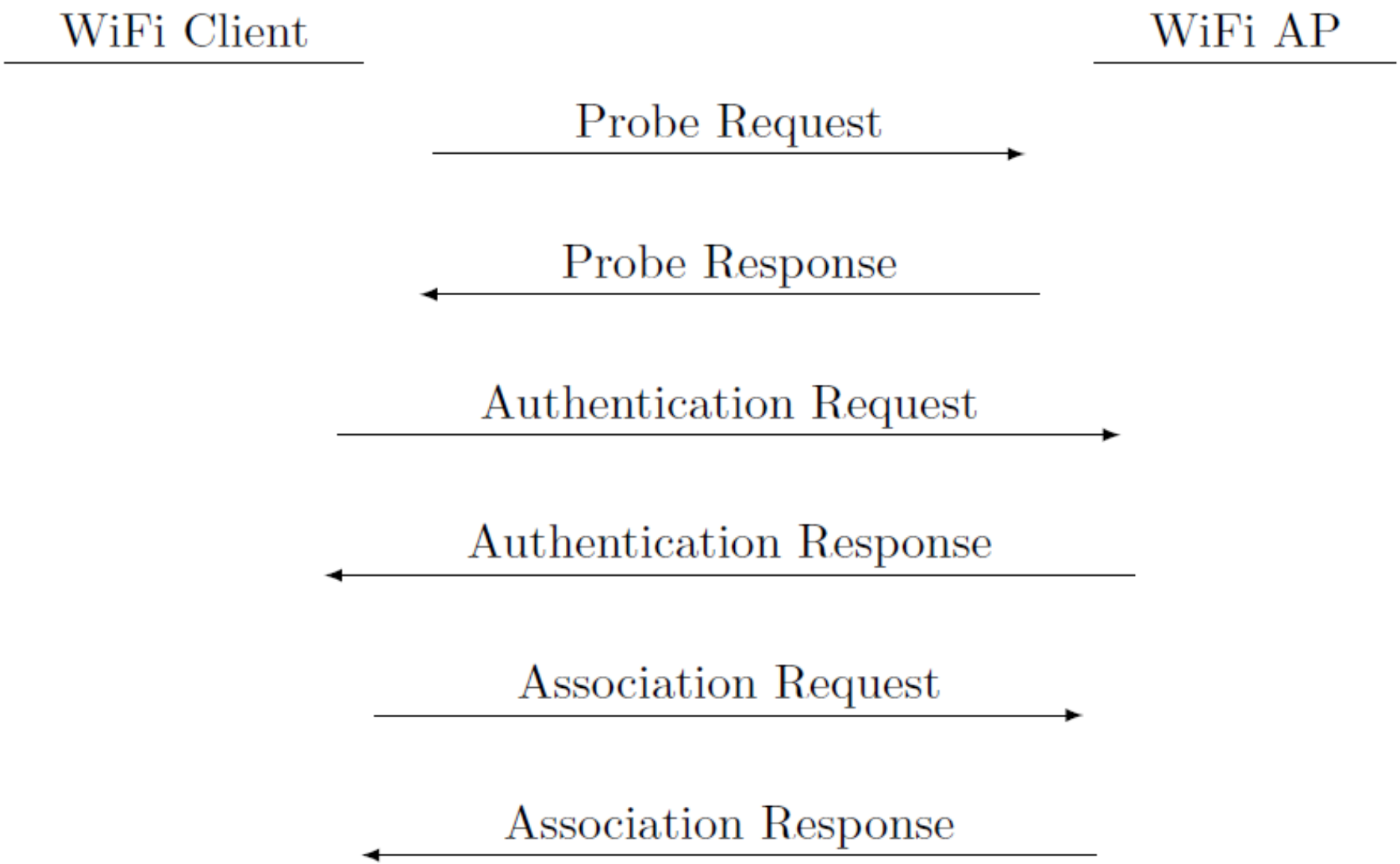
WPA3

- A new standard, **WPA3**, has been released, addressing shortcomings in WPA2.
- This will require new hardware or firmware in NICs and APs.
- WPA3 provides **forward secrecy** (disclosure of server key does not compromise session keys, prevents decryption of recorded sessions)

Authentication

- A client STA needs to be authenticated prior to an association occurring
- The authentication may be to an AP or to a remote authentication server
- **WPA Personal** - also know as **WPA-PSK** (pre-shared key). Each wireless device decrypts traffic using a calculated *pre-shared key*. The key is entered as either a 64 bit hex value or an 8-63 character ASCII string which is used to generate a 256 bit key using PBKDF2 (Password Based Key Derivation Function)
- **WPA Enterprise** - requires a **RADIUS** (Remote Authentication Dial-In User Service) authentication server. This allows a single-sign on in large organisations (Like ECU). WPA includes **EAP** (Extensible Authentication Protocol) which permits different authentication schemes.

Connection State Machine



IP Subnet Connection

- Once an association has been established, the station needs to establish an IP connection
- Generally, this is done using DHCP in the same manner as Ethernet
- Large WLANs may have multiple APs using the same SSID connected to the same IP subnet
- If a mobile device, such as a laptop or mobile moves from one AP to another AP, it will need to dissociate from the first AP and associate with the second IP.
- This may be done while maintaining TCP connections.
- Switches to which the APs are connected to need to update the switch tables. This may require the switch the second AP is connected to issue an Ethernet broadcast to update switch tables

Wi-Fi Frame Format

- The 802.11 frame is similar to a 802.3 (Ethernet) frame, but has additional fields specific for wireless communication
- 802.11 uses the same six-byte MAC addressing scheme as 802.3 (Ethernet)
- The biggest difference is that the 802.11 frame had **four** address fields
  - Receiver address - the address of the wireless station that is to receive the frame. A laptop sending a frame would use the MAC address of the AP, even if sending a broadcast frame
  - Destination address - the address of the target device. It may either be the address of a station, of a default gateway or a broadcast address
  - Transmitter address - the address device sending the frame
  - Source address - the address of the device where the frame originated

Wi-Fi MAC Protocol

- Collisions cannot be detected on a wireless medium, CSMA/CD is not an option
- Wi-Fi uses CSMA/CA (Collision Avoidance)
- It also uses **link-layer acknowledgement**
- Station listens for traffic
  - if traffic detected, wait a random period of time
  - if none waits a short period called the Distributed Inter-Frame Space (DIFS)
- Receiving station waits a short period, the Short Inter-Frame Space (SIFS), then sends an Acknowledgement (ACK)

CSMA/CA

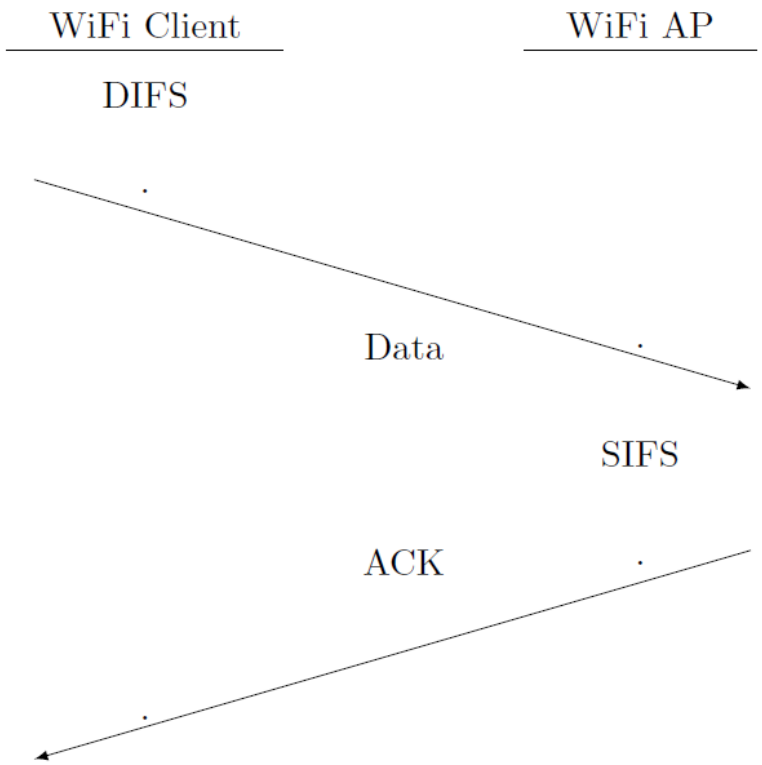
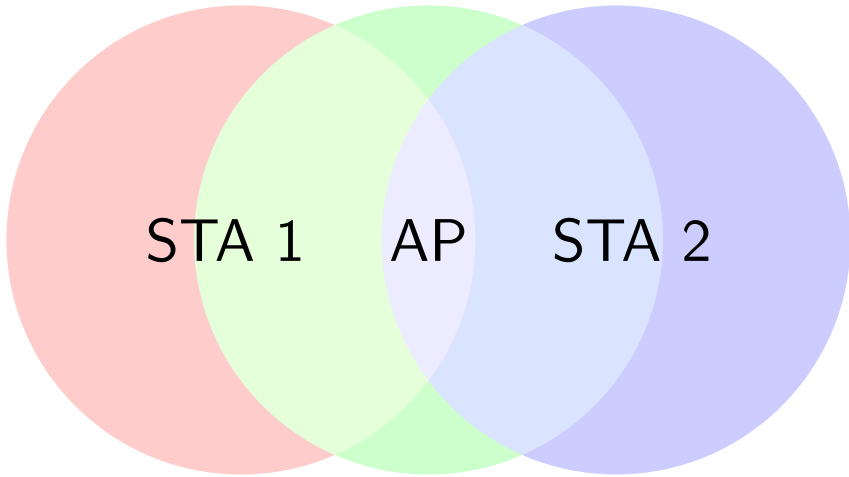


Figure 1: CSMA/CA

The hidden station problem

- Stations listen for other traffic prior to transmission
- STA 1 is in range of the AP.
- STA 2 is in range of the AP
- STA 1 is **not** in range of STA 2



RTS/CTS

- To avoid the problem of a hidden station, 802.11 includes the **RTS (Request to Send)** and **CTS (Clear to Send)** control frames
- A station sends a small RTS frame to an AP which includes the time interval required
- The AP replies with a CTS frame which:
  1. Gives the sender permission to transmit
  2. Requests all other stations not to transmit during the reservation period

Overheads

- The nature of wireless requires **Half Duplex** transmissions
- The Acknowledgement of each frame adds additional overhead
- RTS/CTS adds additional overhead and therefore only used for long transmissions
- All of the above impacts calculations of capacity of a Wi-Fi channel

Wi-Fi Selection

When not to use Wi-Fi

- Environmental
  - Near sources of strong EM interference (EMI) - motors, welding, strong RF signals
  - Multiple metal surfaces or structures - either block, refract or reflect signals
- Security
  - Range of transmission is indeterminate
  - Highly sensitive data needs special attention
- Performance
  - Multiple factors impact speed and latency
  - Applications that require deterministic delivery can be an issue