Lecture 3: Wireless LAN Technologies

3.1. IEEE 802.11 Standards and Protocols
- Introduction to IEEE 802.11
- IEEE 802.11 Standards Family
- Key IEEE 802.11 Features
- Frequency Bands
- Modulation and Data Rates

3.2. Wireless LAN Architectures and Components
- Basic WLAN Architecture
- Infrastructure Mode vs. Ad Hoc Mode
- Wireless LAN Components
- Roaming and Handover

3.3. MAC Layer Protocols: CSMA/CA, RTS/CTS, and more
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
- Request to Send/Clear to Send (RTS/CTS)
- Distributed Coordination Function (DCF)
- Enhanced Distributed Channel Access (EDCA)

3.4. Wireless LAN Security Mechanisms and Vulnerabilities
- Wireless LAN Security Challenges
- Security Protocols
- Authentication Methods
- Wireless Intrusion Detection and Prevention Systems (WIDS/WIPS)
- Guest Network and VLAN Segmentation
- Security Best Practices

3.1. IEEE 802.11 Standards and Protocols

3.1.1. Introduction to IEEE 802.11

- IEEE 802.11, commonly known as Wi-Fi, revolutionized wireless communication.
- It defines standards and protocols for wireless local area networking (WLAN).
- It enables wireless communication between devices and access points, offering flexibility and mobility.

3.1.2. IEEE 802.11 Standards Family

- IEEE 802.11 encompasses various standards and amendments.
  - 802.11a: Operates in the 5 GHz band with data rates up to 54 Mbps.
  - 802.11b: Uses the 2.4 GHz band, providing 11 Mbps data rates.
  - 802.11g: Combines 2.4 GHz operation with speeds up to 54 Mbps.
  - 802.11n: Introduces MIMO technology for higher throughput.
  - 802.11ac: Operates in 5 GHz, offering Gigabit-level speeds.
  - 802.11ax (Wi-Fi 6): Enhances efficiency and capacity in high-density environments.
- These standards define protocols for communication, ensuring compatibility and functionality.
- These standards govern PHY and MAC layer specifications, ensuring compatibility and performance.

（Study idea: Create a comparison table of various standards.）

3.1.3. Key IEEE 802.11 Features

- IEEE 802.11 standards specify protocols for both the physical (PHY) and medium access control (MAC) layers.
- MAC protocols, including Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), regulate channel access.
    - Listen to determine how busy the shared channel is
    - Sends out a message telling all other nodes it is sending data
    - All other nodes “back off” from sending data for a predetermined period of time
- PHY layer specifications encompass modulation schemes, channel widths, and data rates.

3.1.4. Frequency Bands

- IEEE 802.11 operates in different frequency bands, such as 2.4 GHz and 5 GHz.
- The choice of frequency band affects signal range, data rates, and susceptibility to interference.

Rel. Year	1999	2007	2009	2013	2020	2023(?)
Freq. Band	2.4 GHz	2.4 GHz	2.4 + 5 GHz	5 GHz	2.4 + 5 + 6 GHz (6E)	2.4 + 5 + 6 GHz
Bandwidth	20 MHz	20 MHz	40 MHz	80 MHz, 160 MHz	80 MHz, 160 MHz	240 MHz, 320 MHz

3.1.5. Modulation and Data Rates

- IEEE 802.11 standards define modulation schemes like QPSK, 16-QAM, and 64-QAM.
- Higher-order modulation allows for greater data rates, but it's sensitive to signal quality.
- MIMO technology in 802.11n and later standards enhances data rates and reliability.

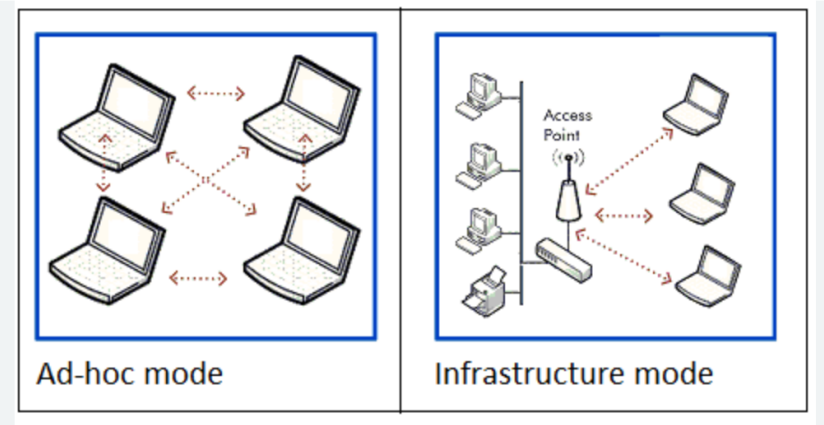
3.2. Wireless LAN Architectures and Components

3.2.1. Basic WLAN Architecture

- WLANs consist of wireless clients and access points (APs) connected to a wired network.
- APs act as bridges between wireless clients and the wired infrastructure.
- They enable wireless devices to access resources like the internet or a corporate network.

3.2.2. Infrastructure Mode vs. Ad Hoc Mode

- Infrastructure mode is the most common WLAN configuration, where devices communicate through APs.
- Ad hoc mode allows direct peer-to-peer communication among devices without APs.
- Use cases for each mode depend on requirements, with infrastructure mode being more common in enterprises.



3.2.3. Wireless LAN Components

- WLAN components include APs, wireless clients, and optional wireless LAN controllers.
- APs are responsible for radio communication and client connectivity.
- Wireless clients include laptops, smartphones, and IoT devices.
- Controllers centralize WLAN management, enhancing scalability and control.
- RADIUS servers play a vital role in user authentication in enterprise WLANs.

3.2.4. Roaming and Handover

- Roaming enables devices to maintain connectivity while moving between APs.
- Handover mechanisms ensure seamless transitions between APs.
- RSSI and roaming algorithms help devices select the best AP for handover.
- Real-world examples illustrate the importance of efficient roaming in WLANs.

3.3. MAC Layer Protocols: CSMA/CA, RTS/CTS, and more

3.3.1. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

- CSMA/CA is the fundamental MAC protocol in IEEE 802.11 WLANs.
- It operates by sensing the channel before transmitting data to avoid collisions.
- CSMA/CA includes mechanisms like backoff timers and contention windows.

3.3.2. Request to Send/Clear to Send (RTS/CTS)

- RTS/CTS is an optional mechanism used to address the "hidden node problem."
- Before transmitting, a station sends an RTS frame to request the channel.
- The AP responds with a CTS frame if the channel is clear, preventing collisions.

3.3.3. Distributed Coordination Function (DCF)

- DCF is the default contention-based access method in IEEE 802.11.
- Stations contend for the channel by waiting for a clear channel before transmitting.
- Random backoff timers introduce fairness and reduce collisions.

3.3.4. Enhanced Distributed Channel Access (EDCA)

- EDCA extends DCF with Quality of Service (QoS) support.
- Stations prioritize traffic based on Access Categories (ACs).
- Each AC has its own contention parameters, enabling differentiated access for voice, video, and data.

3.4. Wireless LAN Security Mechanisms and Vulnerabilities

3.4.1. Wireless LAN Security Challenges

- WLANs face unique security challenges, including eavesdropping, unauthorized access, and rogue devices.
- The absence of physical boundaries makes wireless networks susceptible to various threats.

3.4.2. Security Protocols

- Wired Equivalent Privacy (WEP): The first WLAN security protocol, but it has vulnerabilities.
- Wi-Fi Protected Access (WPA): Introduced stronger encryption and key management.
- WPA2/WPA3: Continual improvements with better security features and protection against attacks.

（Study idea: Create a comparison table of Wi-Fi security protocols.）

3.4.3. Authentication Methods

- Pre-Shared Key (PSK) Authentication: Simple, password-based authentication suitable for home networks.
- 802.1X/EAP (Extensible Authentication Protocol): Provides robust user and device authentication in enterprise settings.

3.4.4. Wireless Intrusion Detection and Prevention Systems (WIDS/WIPS)

- WIDS/WIPS are essential for monitoring WLAN traffic for suspicious activity.
- They can detect and respond to intrusions, unauthorized devices, and attacks.
- Deploying WIDS/WIPS helps maintain WLAN security.

3.4.5. Guest Network and VLAN Segmentation

- Isolating guest networks from internal networks enhances security.
- VLANs separate traffic logically, ensuring guest users cannot access sensitive resources.
- Network segmentation is implemented.

3.4.6. Security Best Practices

- Implementing security best practices is crucial for maintaining WLAN security.
- Regular updates, strong password policies, firmware updates, and monitoring for rogue devices are vital measures.
- Significant consequences of security breaches.