# Challenges, Threats and Hacking Methodologies and 802.11 Basics

Shambhu Upadhyaya
Wireless Network Security
CSE 566 (Lectures 5, 6)



# Outline of the Lecture

- Overview of Challenges
- 802.11 Architecture

## Overview of Challenges

Shambhu Upadhyaya
Wireless Network Security
CSE 566 (Lecture 5)

University at Buffalo The State University of New York



## WLAN Security Goals

- There are four goals one should aim for when installing a wireless network
  - **Access control** - Only authorized users should be allowed to use the wireless network
  - **Data integrity** - The network traffic should be secure against tampering
  - **Confidentiality** - The user should be protected against a third party listening to the conversation
  - **Availability of service** - The service should be secured against Denial of Service (DoS) attacks

University at Buffalo The State University of New York

# Basic WLAN Security Mechanisms

- Service Set Identifier (SSID)
- MAC Address filtering
- Open System Authentication
- Shared Key Authentication
- Wired Equivalent Privacy (WEP) protocol

802.11 products are shipped by the vendors with all security mechanisms disabled !!

University at Buffalo The State University of New York



# SSID-Service Set Identifiers

- Limits access by identifying the service area covered by the access points
- AP periodically broadcasts SSID in beacon frames
- End station listens to these broadcasts and choose an AP to associate with based upon its SSID
- Use of SSID is a weak form of security as beacon management frames on 802.11 WLAN are always sent in the clear
- A hacker can use analysis tools (e.g., AirMagnet, Netstumbler, AiroPeek) to identify SSIDs
- Some vendors use default SSIDs which are pretty well known (e.g., CISCO uses tsunami)

University at Buffalo The State University of New York

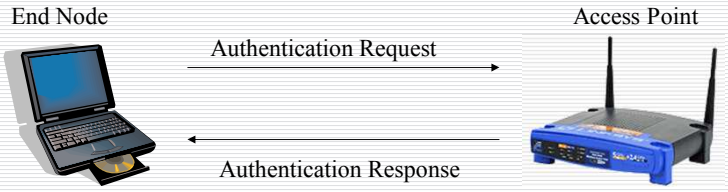
# MAC Address Filtering

- The system administrator can specify a list of MAC addresses that can communicate through an access point
- Advantage
  - Provides stronger security than SSID
- Disadvantages
  - Increases Administrative overhead
  - Reduces scalability
  - Determined hackers can still break it



# Open System Authentication

- The default authentication protocol for 802.11
- Authenticates anyone who requests authentication (null authentication)



# Shared Key Authentication

- This assumes that each station has received a secret shared key through a secure channel independent from the 802.11 network
- Stations authenticate through shared knowledge of the secret key
- Use of shared key authentication requires implementation of the 'Wired Equivalent Privacy' algorithm

End Station

Authentication Request

Authentication Challenge

Authentication Response

Authentication Result

Access Point



# Wired Equivalence Privacy (WEP)

- Designed to provide confidentiality to a wireless network similar to that of standard LANs
- WEP is essentially the RC4 symmetric key cryptographic algorithm (same key for encrypting and decrypting)
- Transmitting station concatenates 40 bit key with a 24 bit Initialization Vector (IV) to produce pseudorandom key stream
- Plaintext is XORed with the pseudorandom key stream to produce ciphertext

## Wired Equivalence Privacy (WEP)

- Ciphertext is concatenated with IV and transmitted over the Wireless Medium
- Receiving station reads the IV, concatenates it with the secret key to produce local copy of the pseudorandom key stream
- Received ciphertext is XORed with the key stream generated to get back the plaintext

University at Buffalo The State University of New York



## Wired Equivalence Privacy (WEP)

- WEP has been broken! Walker (Oct 2000), Borisov et al. (Jan 2001), Fluhrer-Mantin -Shamir (Aug 2001)
- Unsafe at any key size: Testing reveals WEP encapsulation remains insecure whether its key length is 1 bit or 1,000 or any other size

University at Buffalo The State University of New York

# Threats to Wireless Networks

- Threats in wireless networks can be configured into the following categories
  - Errors and omissions
  - Fraud and theft committed by authorized or unauthorized users of the system
  - Employee sabotage
  - Loss of physical and infrastructure support
  - Malicious hackers
  - Industrial espionage
  - Malicious code
  - Threats to personal privacy



# Vulnerabilities in Wireless Networks

- Vulnerabilities in wireless networks include
  - Existing vulnerabilities of wired networks apply to wireless networks as well
  - Sensitive information that is not encrypted (or is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices may be intercepted and disclosed
  - Denial of service (DoS) attacks may be directed at wireless connections or devices
  - Sensitive data may be corrupted during improper synchronization

## Vulnerabilities, Contd..

- Malicious entities may be able to violate the privacy of legitimate users and be able to track their actual movements
- Handheld devices are easily stolen and can reveal sensitive information
- Interlopers, from inside or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations

University at Buffalo The State University of New York



## Wi-Fi Evil Twins

- Evil twins are the latest menace to threaten the security of Internet users
- Anyone with suitable equipment can locate a hotspot and take its place, substituting their own "evil twin"
- There are no good solutions against it
- Strong authentication and encryption could be good defenses

University at Buffalo The State University of New York

# Risks in Wireless Networks

- Risks in wireless technology are considerable
- Most of current communication protocols provide inadequate security
- Many organizations still poorly manage their networks
  - Deploying equipments with "factory default" settings
  - Failing to control access points
  - Not implementing security capabilities provided
  - Not developing a suitable security architecture (e.g., Firewalls between wireless and wired systems, not using strong cryptography, etc.)



# WLAN - Security Problems

Attacks in WLANs can be classified as

- Passive Attacks

  An attack in which an unauthorized party simply gains access to an asset and does not modify its content
  - Eavesdropping
  - Traffic Analysis
- Active Attacks

  An attack whereby an unauthorized party makes modifications to a message, data stream, or file
  - Masquerading
  - Replay
  - Message Modification
  - Denial of Service (DoS)

## Passive Attacks – Eavesdropping

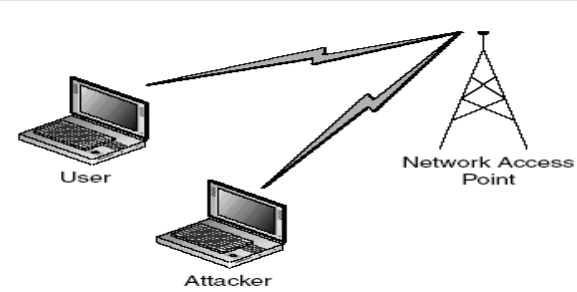
- Eavesdropping
  - Used to gather information on the network under attack
  - The intruder configures his wireless terminal to appear to have the same MAC address as an authorized access point or wireless terminal (Spoofing)
  - When spoofing an access point, the intruder's terminal appears as the authorized access point, with the intent to associate with an authorized wireless terminal and access the data on that device
  - The anonymous attacker can passively intercept radio signals and decode the data being transmitted



## Passive Attacks – Eavesdropping

- Goals of attacker are to know about
  - Users of the networks
  - Accessible resources
  - Capabilities of the equipment on the network
  - Least and most used resources
  - Coverage area of the network
- Attacker can then use this information to launch an attack on the network later

# Passive Attacks – Eavesdropping




Eavesdropping



# Passive Attacks – Eavesdropping

- With little or no modification, devices can be configured to capture all traffic on a particular network channel or frequency
- Tests have shown that an attacker can be nearly 20 miles away from a target and still receive a signal, thereby eavesdropping on wireless network communications
- Many commonly used network protocols transmit sensitive data such as username and password information in cleartext which can be captured by an attacker
- These attacks are nearly impossible to detect and even harder to prevent

# Passive Attacks – War Driving

- War Driving
  - Very prevalent problem these days
  - The process of searching for open wireless LANs by driving around a particular area
  - The name comes from the term "war dialing" which is an old attack method that involves repeatedly dialing different numbers to search for modems and other network entry points
  - War-driving software are freely available from sites like www.netstumbler.com
  - War Driving conviction is first under the recent Can-Spam act (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003)

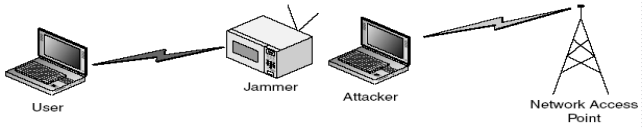


# Active Attacks - Jamming

- Interference and Jamming
  - Jamming is the deliberate introduction of interference to the signal by generating another signal at greater power and close to the transmitted frequency of the first signal
  - Interference can be best described as the effect of unwanted signals or noise on a wanted signal
  - Co-channel interference is caused by unwanted signals sharing the same frequency as the wanted signal
  - Adjacent Channel Interference is caused by signals on neighbouring channels

# Active Attacks - Jamming

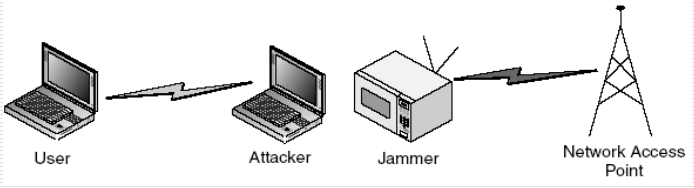
- Client Jamming
  - Provides an opportunity for a rogue client to take over or impersonate the jammed client
  - Could be used to carry out DoS against a client station so that it loses network connectivity
  - Could be used to interrupt connectivity of the client with the real base station to then reattach with a rogue station






# Active Attacks - Jamming

- Base Station Jamming
  - Jamming a base station provides an opportunity for a rogue base station to stand in for the legitimate base station

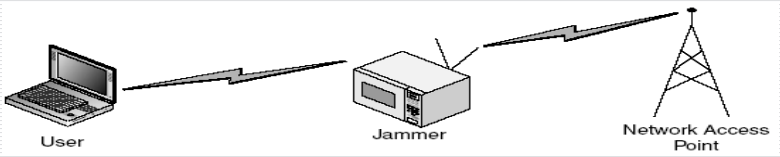


# Active Attacks - DoS

- Jamming can be used to carry out Denial of Service (DoS) attacks against the network
- DoS attacks can be carried out in the following ways
  - Brute force attack
    - Send a huge flood of packets that uses up all of the network's resources and forces it to shut down
    - Use a very strong radio signal that totally dominates the airwaves and renders access points and radio cards useless



# DoS Attack (Radio Signal Based)




- As the entire area is flooded with interference, no stations can communicate with each other
- This type of attack can require a significant amount of power if applied to a broad area
- DoS attacks on wireless networks may be difficult to prevent and stop
- Most wireless networking technologies use unlicensed frequencies and are subject to interference from a variety of different electronic devices

## DoS (Packet Based)

- The attacker uses other computers on the network to send useless packets to the server
- To initiate an attack, the intruder discovers an access point on the wireless network and then sends it a continuous stream of meaningless information
- This adds significant overhead on the network and takes away useable bandwidth from legitimate users
- Difficult to trace the attack source as it is hidden behind other users



## DDoS Using Botnets

- Botnets (collection of software modules called robots) can be used to stage DDoS (distributed DoS) attacks
- Basically, botnets are used to control and manage the zombies that are used to conduct distributed DoS attacks on a large scale
- Botnets generally run hidden like the spyware and exercise control through IRCs (Internet Relay Chat)
- There are instances where DNS attacks were carried out using botnets

# DoS (Another type)

- Wi-Fi Protected Access (WPA) is vulnerable to a type of DoS attack
- WPA uses mathematical algorithms to authenticate users to the network
- If a non-authenticated user sends more than two packets of unauthorized data within one second, WPA assumes it is under attack and shuts down
- This opens up a loophole for the hackers where all they have to do is to send data-frames periodically, causing constant shutdowns
- The hackers are difficult to find because they don't need to use much transmit power or utilization of the network



# Active Attacks – Replay Attacks

- The intruder monitors and captures transmitted packets between wireless terminals and access point
- This is achieved via a passive monitoring utilities called 'sniffers' such as AirSnort, which are readily available on the Internet as freeware
- Then these messages are replayed later so that they appear to be coming from authentic users

# Injection & Modification of Data

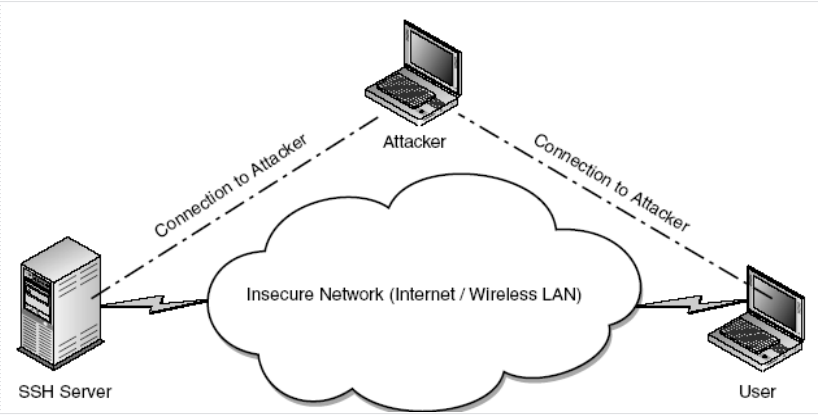
- Injection attacks occur when an attacker adds data to an existing connection to maliciously send data or commands
- An attacker can manipulate control messages and data streams by inserting packets or commands to a base station and vice versa
- Inserting control messages on a valid control channel can result in the disassociation or disconnection of users from the network
- An attacker can also flood the network access point with connect messages, tricking the network access point into exceeding a maximum limit, thereby denying authorized users access to the network



# Man in the Middle Attack

- Man in the middle attack
  - An attack that requires sophisticated software and can cause significant disruption or data loss
  - The hacker inserts themselves between an access point and a wireless terminal to capture packets in transmission
  - The wireless terminal sees the hacker as an authorized access point, while the access point sees the hacker as an authorized wireless terminal
  - Both authorized devices fail to detect the intruder and continue transmitting information
  - The intruder captures legitimate information and is also able to inject false data into the network, or initiate a DoS attack
  - Can be active or passive attack

# Man in the Middle Attack

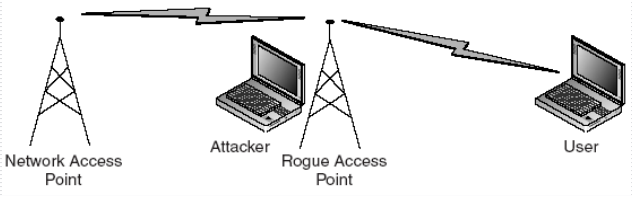



**Man in The Middle Attack**



# Rogue Access Points

- Largest percentage of WLAN security attacks
- Intercepts the traffic between access point and authorized user
- Can collect the sensitive information like authentication credentials from the user



# Infrastructure Equipment Attacks

- Incorrectly configured infrastructure equipments targeted in such attacks
- Network devices such as routers, switches, backup servers, and log servers are prime targets
- Classified mainly as follows
  - **Switch attacks**
    - Flooding the MAC or ARP table in the switch to cause it to fail open
    - Manipulating the protocol that the switches use to communicate - such as spanning tree



# Infrastructure Equipment Attacks

- **MAC attacks**
  - ARP spoofing and other physical layer attacks that can be used to fool network devices into sending the data to unintended recipients
- **Routing attacks**
  - Participating in the routing protocol, such as Open Shortest Path First (OSPF) or Enhanced Interior Gateway Routing Protocol (EIGRP), to change the flow of traffic for DoS or sniffing

# References

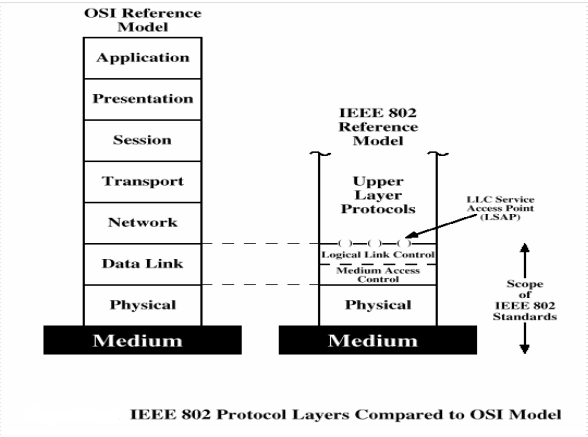

- William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan, "Your 802.11 Wireless Network has No Clothes, University of Maryland, 2001
- NIST Notes on Wireless Networks Security,
- Wireless Security, Merritt Maxim and David Pollino Copyright © 2002 by The McGraw-Hill Companies




# 802.11 Architecture

Shambhu Upadhyaya
Wireless Network Security
CSE 566 (Lecture 6)

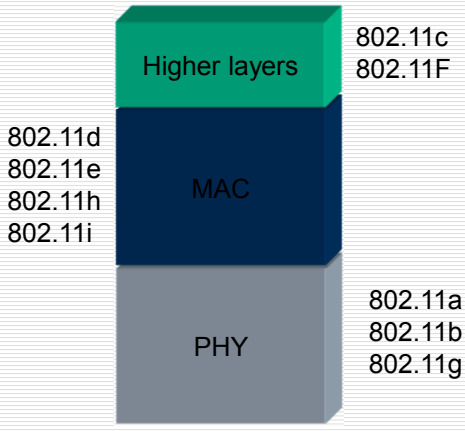
# IEEE 802 Protocol Layers




IEEE 802 Protocol Layers Compared to OSI Model

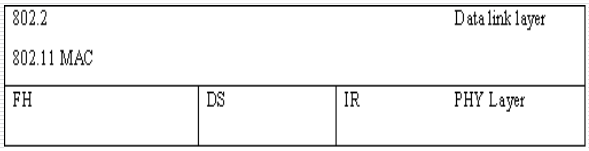


# 802.11 Sub-Layers



# 802.11 Layers Description

- 802.11 protocol covers the MAC and Physical Layer
- Current standard defines Single MAC
- Three Physical layers are supported
  - Frequency Hopping Spread Spectrum in the 2.4 GHz Band
  - Direct Sequence Spread Spectrum in the 2.4 GHz Band
  - InfraRed






# Protocol Architecture

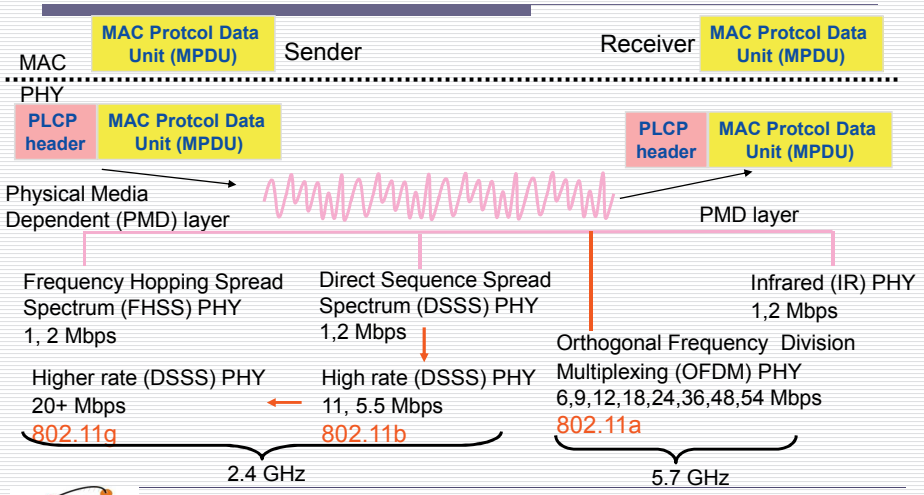
- Functions of physical layer
  - Encoding/decoding of signals
  - Preamble generation/removal (for synchronization)
  - Bit transmission/reception
  - Includes specification of the transmission medium
- Functions of Medium Access Control (MAC) layer
  - On transmission, assemble data into a frame with address and error detection fields
  - On reception, disassemble frame and perform address recognition and error detection
  - Govern access to the LAN transmission medium

# Protocol Architecture

- Functions of logical link control (LLC) Layer
  - Provide an interface to higher layers and perform flow and error control
- The logic required to manage access to a shared-access medium not found in traditional layer 2 data link control
- For the same LLC, several MAC options may be provided



# 802.11 Physical Layer



# 802.11 MAC Layer

- MAC Layer defines two different access methods
  - The Distributed Coordination Function
  - The Point Coordination Function



# Distributed Coordination Function

- This uses the CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) mechanism for access resolution
- Based on the popular CSMA protocols (eg., CSMA/CD used in Ethernet)
- CSMA Protocol works as follows
  - A station desiring to transmit senses the medium
  - If the medium is busy then the station defers its transmission to a later time
  - If the medium is sensed free then the station is allowed to transmit
- Protocol extremely effective when medium is not heavily loaded

## Distributed Coordination Function

- If stations simultaneously sense the medium as being free and transmit at the same time, it causes a collision
- Collision detected by MAC layer which causes retransmission
- (In Ethernet the collisions are sensed by the sending stations which then cause an exponential backoff)
- Similar strategy cannot be applied to Wireless networks because
  - This would require full duplex radios capable of transmitting and receiving at the same time which would be very expensive
  - In wireless domain all stations do not hear all other stations which is a requirement for this protocol



## CSMA/CA

- Thus 802.11 uses a Collision Avoidance scheme with positive acknowledgements
  - A station wanting to transmit senses the medium. If the medium is busy then it defers
  - If the medium is free for a specified time (Distributed Inter Frame Space (DIFS)), then the station is allowed to transmit
  - The receiving station checks the CRC of the received packet and sends an acknowledgment packet (ACK)
  - Receipt of the acknowledgment indicates to the transmitter that no collision occurred
  - If the sender does not receive the acknowledgment then it retransmits the fragment until it receives acknowledgment or is thrown away after a given number of retransmissions

## CSMA/CA

- To reduce the probability of collisions between transmissions from stations which cannot hear each other, Wi-Fi uses a Virtual Carrier Sense mechanism
  - If a station wants to transmit it sends a *RTS (Request to Send)* signal
  - This includes the source, destination, duration of the following transmission
  - If the medium is free the destination responds with a *CTS (Clear to Send)* signal
  - All stations receiving either the RTS and/or the CTS, set their *Virtual Carrier Sense* indicator (called *NAV, (Network Allocation Vector*)), for the given duration
  - The stations use the NAV along with physical carrier sense to sense and transmit

University at Buffalo The State University of New York



## Point Coordinated Function

- Beyond the basic Distributed Coordination Function, there is an optional Point Coordination Function
- May be used to implement time-bounded services, like voice or video transmission
- This Point Coordination Function makes use of the higher priority that the Access Point may gain by the use of a smaller Inter Frame Space (PIFS)
- By using this higher priority access, the Access Point issues polling requests to the stations for data transmission, hence controlling medium access
- In order to still enable regular stations to access the medium, there is a provision that the Access Point must leave enough time for Distributed Access in between the PCF

University at Buffalo The State University of New York

# 802.11 MAC Contd…

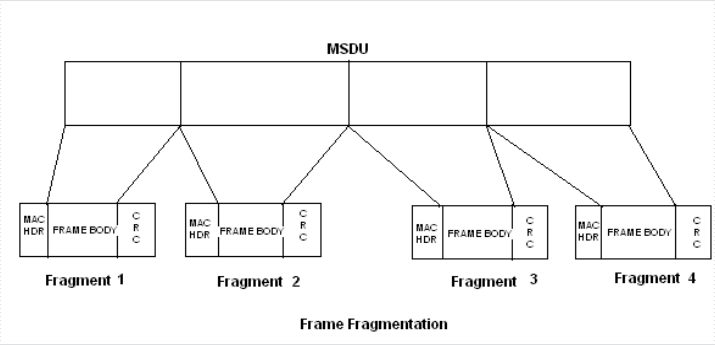
- Fragmentation and Reassembly
  - Typical Ethernet packets are long (hundreds of bytes)
  - Smaller packets preferable for wireless networks
    - Due to the higher Bit Error Rate of a radio link, probability of packet getting corrupted increases with packet size
    - In case of packet corruption (either due to collision or noise), the smaller the packet, the less overhead it causes to retransmit it
    - Due to Frequency Hopping system, the medium is interrupted periodically for hopping, so smaller packets cause less overhead



# Fragmentation & Reassembly

- To have smaller packet size for 802.11 a fragmentation/reassembly mechanism is placed at the MAC Layer
- It uses a simple Send – Wait algorithm
  - In this a large frame is fragmented and individual fragments are transmitted
  - Once a fragment is transmitted the algorithm waits till one of the following happens:
    - Receives an ACK for the said fragment, or
    - Decides that the fragment was retransmitted too many times and drops the whole frame

# Fragmentation & Reassembly




**MSDU** – MAC Service Data Unit

**CRC** – Cyclic Redundancy Check

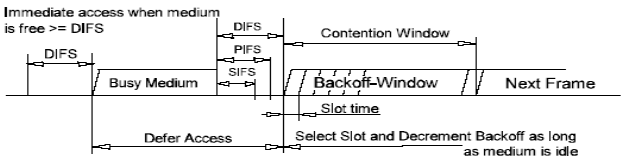


# 802.11 MAC Contd..

- MAC Defines 4 types of Inter Frame Space (IFS)
  - SIFS - Short Inter Frame Space
  - PIFS - Point Coordination IFS
  - DIFS - Distributed IFS
  - EIFS - Extended IFS

# Exponential Back-off Algorithm

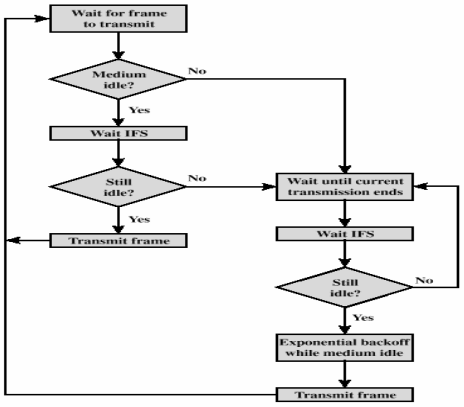
- Exponential Back-off Algorithm- Resolves Contention and is executed in the following cases
  - When the station senses the medium before the first transmission of a packet, and the medium is busy
  - After each retransmission, and
  - After a successful transmission




*Access Mechanism*



# 802.11 MAC Logic




**IEEE 802.11 Medium Access Control Logic**

# MAC Frames

- MAC frames can be classified into following 3 types
  - Data Frames
    Used for transmission of actual data on the medium
  - Control Frames
    Used for controlling access to the medium (RTS, CTS, ACK)
  - Management Frames
    Transmitted in manner similar to data frames and used to exchange management information but are not transferred to upper layers

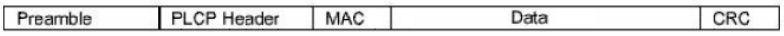


# MAC Frames

- Control Frames
  - RTS (Request To Send)
  - CTS (Clear To Send)
  - ACK (Acknowledge)
- Management Frames
  - Beacon (notify)
  - Probe (notify)
  - Authenticate (request and response)
  - Associate (request and response)
  - Reassociate (request and response)
  - Disassociate (notify)
  - Deauthenticate (notify)

# MAC Frames

Frame Format




This contains the following fields

- Preamble
- PLCP (Physical Layer Convergence Protocol) Header
- MAC Header
- User Data
- CRC (Cyclic Redundancy Check)



# MAC Frames

- Preamble
  - This is used to identify the frame format as 802.11
  - Contains special bit sequences used by clients for synchronization purpose
- PLCP Header
  - Contains the information used by the Physical Layer to decode the frames like data rate, packet length etc.
- MAC Header
  - Different for Data, Control and Management frames
  - Most important part of MAC header is the addressing information
  - The addresses are 6 bytes long and are unique for each device

# MAC Frames Contd..

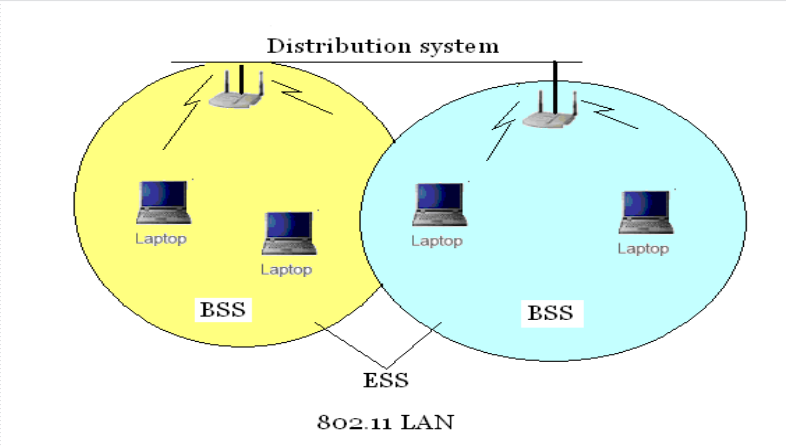
- Destination address can be of the following types:
  - Unicast Address
  - Multicast Address
  - Broadcast Address
- Frame can have two to four addresses
  - Transmitter Address (TA)
  - Receiver Address (RA)
  - Source Address (SA)
  - Destination Address (DA)
- User Data
  - This is the actual data to be transmitted
- CRC
  - Used for error detection and correction



# Beacon Frames

- Sent by Access Points to advertise themselves
- Can be used to
  - Locate access point with right SSID and suitable parameters
  - After association, lets devices know that the base station is still active
  - Helps coordinate operations such as power save mode

# 802.11 LAN Example






# 802.11 Architecture

- Architecture Components
  - 802.11 LAN is based on a cellular architecture
  - Basic Service Set (BSS)
  - Background Network- Distribution system (DS)
  - Extended Service Set (ESS)
  - Portal: Device which connects between an 802.11 and another 802 LAN
- 802.11 Supports
  - Infrastructure Mode
  - Ad hoc mode

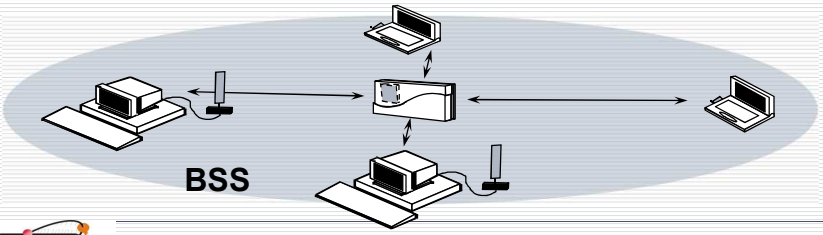
# 802.11 Architecture

- Infrastructure mode
  - An 802.11 networking framework in which devices communicate with each other by first going through an Access Point (AP)
- AD-hoc Mode
  - An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an access point (AP)



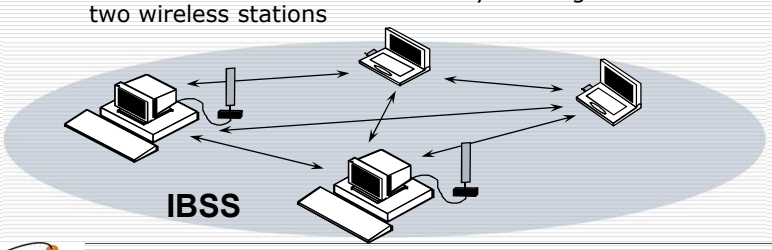
# IEEE 802.11 Terminology

- **Basic Service Set (BSS)**
  - A set of stations controlled by a single "Coordination Function" (= the logical function that determines when a station can transmit or receive)
  - Similar to a "cell" in pre IEEE terminology
  - A BSS can have an Access-Point (both in standalone networks and in building-wide configurations), or can run without an Access-Point (in standalone networks only)
  - Diameter of the cell is approx. twice the coverage-distance between two wireless stations



# IEEE 802.11 Terminology

- **IBSS- Independent Basic Service Set**
  - A Basic Service Set (BSS) which forms a self-contained network in which no access to a Distribution System is available
  - A BSS without an Access-Point
  - One of the stations in the IBSS can be configured to "initiate" the network and assume the Coordination Function
  - Diameter of the cell determined by coverage distance between two wireless stations

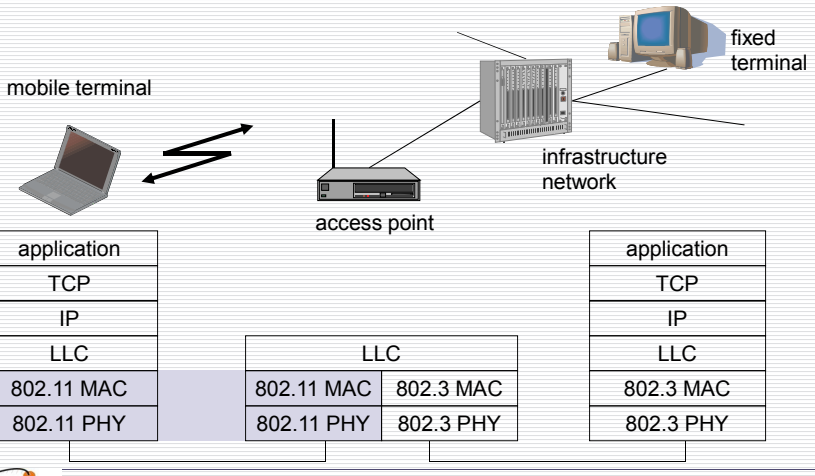





# IEEE 802.11 Terminology

- Extended Service Set (ESS)
  - A set of one or more Basic Service Sets interconnected by a Distribution System (DS)
  - Traffic always flows via Access-Point
  - Diameter of the cell is double the coverage distance between two wireless stations
- Distribution System (DS)
  - A system to interconnect a set of Basic Service Sets
    - Integrated: A single Access-Point in a standalone network
    - Wired: Using cable to interconnect the Access-Points
    - Wireless: Using wireless to interconnect the Access-Points

# Infrastructure Mode






# Operation in Infrastructure Mode

For a Station to associate with an Access Point for data transfer it goes through the following steps

- Station finds the Access Point it wants to associate with. This can be done by
  - **Passive Scanning**
    Station just waits to receive a Beacon Frame which the Access Point periodically transmits
  - **Active Scanning**
    Station tries to locate an Access Point by transmitting Probe Request Frames to the Access Point
- Station decides to join one of the available Access Points based on signal strength

# Operation in Infrastructure Mode

- After the station chooses the particular access point it wants to associate with, it goes through the Authentication process
  - This is used to control the access to infrastructure
  - Stations identify themselves to other stations (or Access-Points) prior to data traffic or association
  - 802.11 provides two types of authentication methods:
    - Open System Authentication
      - Uses null authentication algorithm
      - Default
    - Shared Key Authentication
      - Uses WEP privacy algorithm
      - Optional



# Operation in Infrastructure Mode

- Depending on the result of the Authentication phase the Access Point replies with a *Authentication Response* (accept/reject) Message
- On getting a positive Authentication Response message the station sends a *Association Request* to the Access Point
- In reply to this message the Access Point replies with a *Association Response* message
- This leads to a successful connection establishment between the station and the Access Point and now the channel is usable for data transfer

# Services in Infrastructure Mode

- Association-Related Services
  - Association
    - Establishes initial association between Station and Access Point
  - Re-Association
    - Enables transfer of association from one Access Point to another, allowing station to move from one BSS to another
  - Disassociation
    - Association termination notice from station or Access Point



# Services in Infrastructure Mode

- Access and Privacy Services
  - Authentication
    - Establishes identity of stations to each other
  - De-Authentication
    - Invoked when existing authentication is terminated
  - Privacy
    - Prevents message contents from being read by unintended recipient

## Services in Infrastructure Mode

- Transition Services Based On Mobility
  - No transition
    - Stationary or moves only within BSS
  - BSS transition
    - Station moving from one BSS to another BSS in same ESS
  - ESS transition
    - Station moving from BSS in one ESS to BSS within another ESS



## References


- Jon Edney and William Arbaugh, Real 802.11 Security, Addison-Wesley, 2004 (Chapter 5)
- IEEE 802.11 Technical Tutorial,
- http://sss-mag.com/pdf/802_11tut.pdf