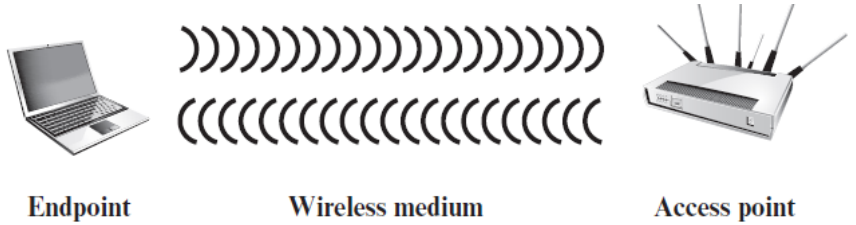
Wireless Network Security

An Introduction

Kamalika Bhattacharjee

Wireless Security



- Wireless networks, and the wireless devices that use them, introduce a host of security problems over and above those found in wired networks.
- Some of the key factors contribute to the higher security risk of wireless networks compared to wired networks
- **Channel**
  - Wireless networking typically involves broadcast communications, which is far more susceptible to eavesdropping and jamming than wired networks.
  - Wireless networks are also more vulnerable to active attacks that exploit vulnerabilities in communications protocols.
- **Mobility**
  - Wireless devices are, in principal and usually in practice, far more portable and mobile than wired devices. This mobility results in a number of risks.

Wireless Security

- **Resources**
  - Some wireless devices, such as smartphones and tablets, have sophisticated operating systems but limited memory and processing resources with which to counter threats, including denial of service and malware.
- **Accessibility**
  - Some wireless devices, such as sensors and robots, may be left unattended in remote and/or hostile locations. This greatly increases their vulnerability to physical attacks.
- Wireless environment consists of three components that provide point of attack
- The **wireless client** can be a cell phone, a Wi-Fi–enabled laptop or tablet, a wireless sensor, a Bluetooth device, and so on.
- The **wireless access point** provides a connection to the network or service. Example: cell towers, Wi-Fi hotspots, and wireless access points to wired local or wide area networks.
- The **transmission medium**, which carries the radio waves for data transfer, is also a source of vulnerability.

Wireless Network Threats

- **Accidental association:**
  - Company wireless LANs or wireless access points to wired LANs in close proximity (e.g., in the same or neighboring buildings) may create overlapping transmission ranges.
  - A user intending to connect to one LAN may unintentionally lock on to a wireless access point from a neighboring network.
  - Although the security breach is accidental, it nevertheless exposes resources of one LAN to the accidental user.
- **Malicious association:**
  - In this situation, a wireless device is configured to appear to be a legitimate access point, enabling the operator to steal passwords from legitimate users and then penetrate a wired network through a legitimate wireless access point.
- **Ad hoc networks:**
  - These are peer-to-peer networks between wireless computers with no access point between them. Such networks can pose a security threat due to a lack of a central point of control.

Wireless Network Threats

- **Nontraditional networks:**
  - Nontraditional networks and links, such as personal network Bluetooth devices, barcode readers, and handheld PDAs, pose a security risk in terms of both eavesdropping and spoofing.
- **Identity theft (MAC spoofing):**
  - This occurs when an attacker is able to eavesdrop on network traffic and identify the MAC address of a computer with network privileges.
- **Man-in-the middle attacks:**
  - This attack involves persuading a user and an access point to believe that they are talking to each other when in fact the communication is going through an intermediate attacking device. Wireless networks are particularly vulnerable to such attacks.

Wireless Network Threats

- **Denial of service (DoS):**
  - Here, a DoS attack occurs when an attacker continually bombards a wireless access point or some other accessible wireless port with various protocol messages designed to consume system resources.
  - The wireless environment lends itself to this type of attack, because it is so easy for the attacker to direct multiple wireless messages at the target.
- **Network injection:**
  - A network injection attack targets wireless access points that are exposed to nonfiltered network traffic, such as routing protocol messages or network management messages.
  - An example of such an attack is one in which bogus reconfiguration commands are used to affect routers and switches to degrade network performance.

Wireless Security Measures

SECURING WIRELESS TRANSMISSIONS

- The principal threats to wireless transmission are eavesdropping, altering or inserting messages, and disruption. To deal with eavesdropping, two types of countermeasures are appropriate:
- **Signal-hiding techniques:**
  - Organizations can take a number of measures to make it more difficult for an attacker to locate their wireless access points
  - This includes turning off service set identifier (SSID) broadcasting by wireless access points; assigning cryptic names to SSIDs; reducing signal strength to the lowest level that still provides requisite coverage; and locating wireless access points in the interior of the building, away from windows and exterior walls.
  - Greater security can be achieved by the use of directional antennas and of signal-shielding techniques.

Wireless Security Measures

SECURING WIRELESS TRANSMISSIONS

- The principal threats to wireless transmission are eavesdropping, altering or inserting messages, and disruption. To deal with eavesdropping, two types of countermeasures are appropriate:
- **Encryption:**
  - Encryption of all wireless transmission is effective against eavesdropping to the extent that the encryption keys are secured.
  - The use of encryption and authentication protocols is the standard method of countering attempts to alter or insert transmissions.
  - Organizations can also reduce the risk of unintentional DoS attacks.
  - Site surveys can detect the existence of other devices using the same frequency range, to help determine where to locate wireless access points.
  - Signal strengths can be adjusted and shielding used in an attempt to isolate a wireless environment from competing nearby transmissions.

Wireless Security Measures

SECURING WIRELESS ACCESS POINTS

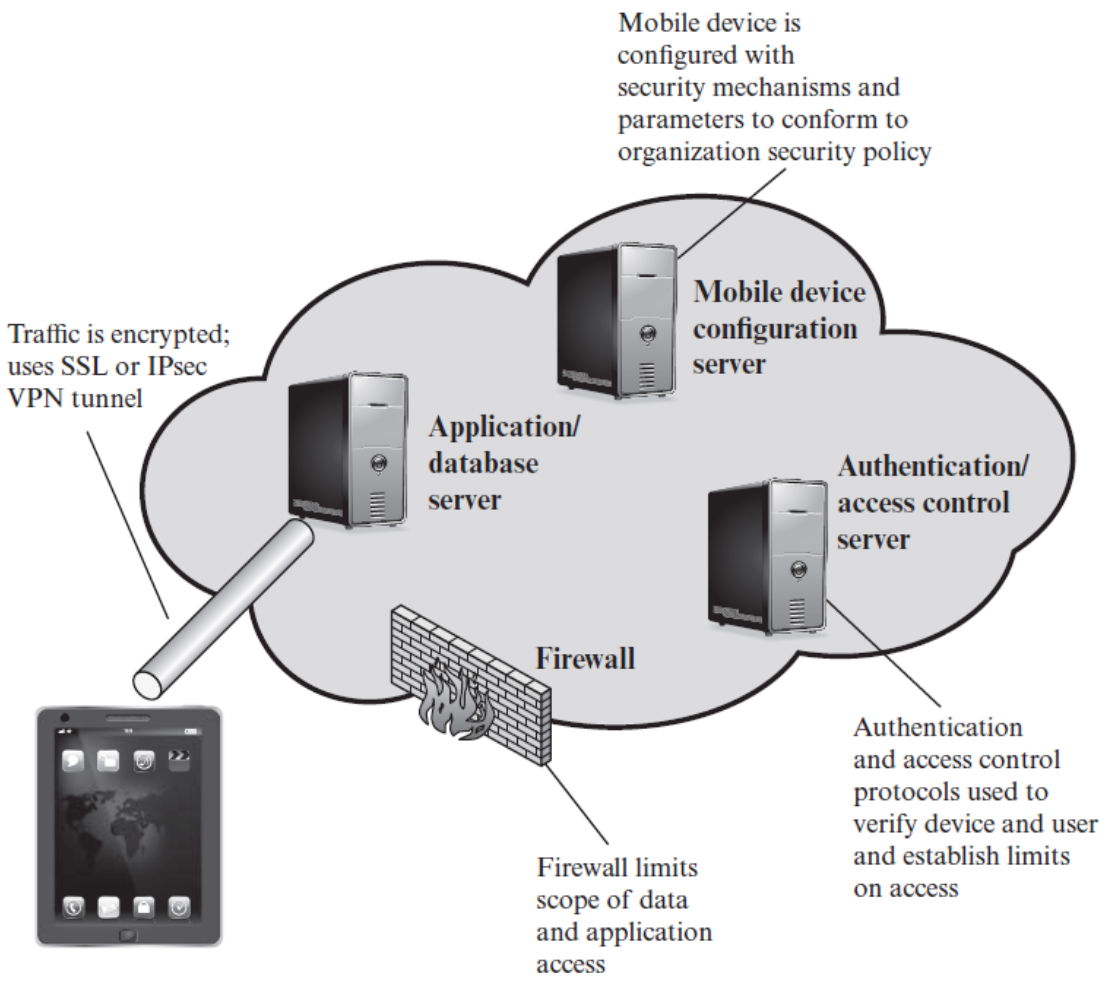
- The main threat involving wireless access points is unauthorized access to the network.
- The principal approach for preventing such access is the IEEE 802.1X standard for port-based network access control.
- The standard provides an authentication mechanism for devices wishing to attach to a LAN or wireless network.
- The use of 802.1X can prevent rogue access points and other unauthorized devices from becoming insecure backdoors.

Wireless Security Measures

STEPS FOR SECURING WIRELESS NETWORKS

1. **Use encryption.** Wireless routers are typically equipped with built-in encryption mechanisms for router-to-router traffic.
2. **Use antivirus and antispyware software, and a firewall.** These facilities should be enabled on all wireless network endpoints.
3. **Turn off identifier broadcasting**. Wireless routers are typically configured to broadcast an identifying signal so that any device within range can learn of the router's existence. If a network is configured so that authorized devices know the identity of routers, this capability can be disabled, so as to thwart attackers.
4. **Change the identifier on your router from the default**. Again, this measure thwarts attackers who will attempt to gain access to a wireless network using default router identifiers.
5. **Change your router's pre-set password for administration**. This is another prudent step.
6. **Allow only specific computers to access your wireless network**. A router can be configured to only communicate with approved MAC addresses. Of course, MAC addresses can be spoofed, so this is just one element of a security strategy.

Mobile Device Security Strategy



IEEE 802.11 Wireless LAN

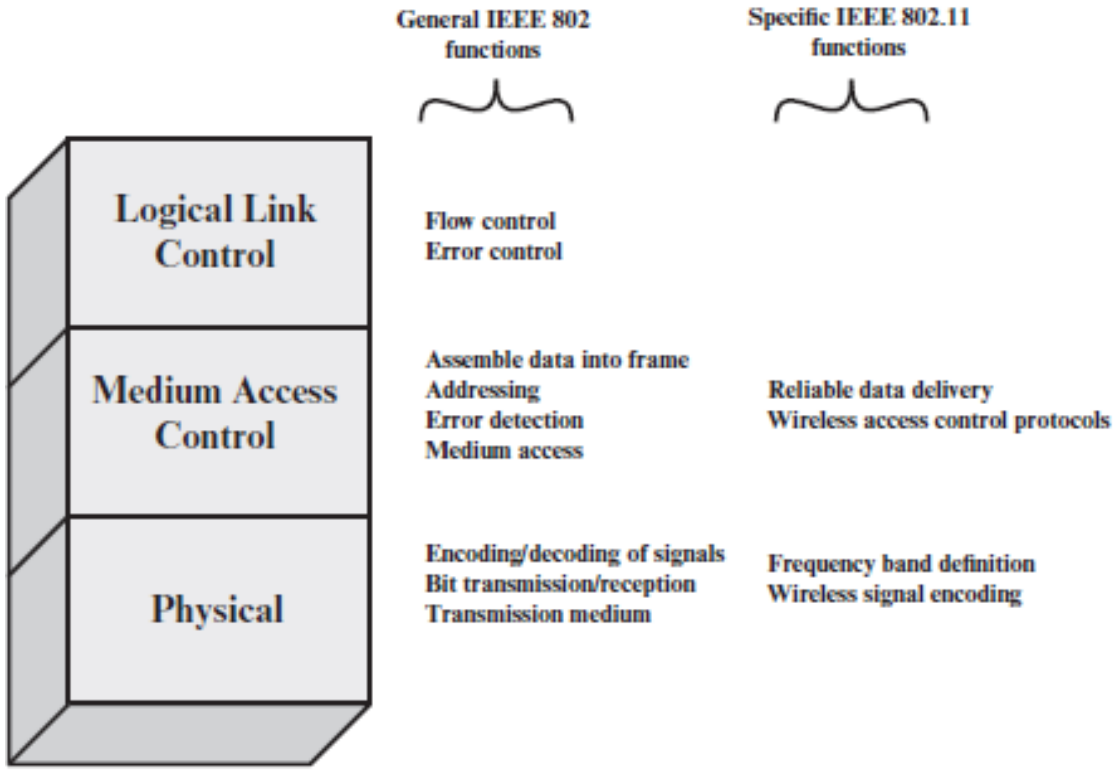
- IEEE 802 is a committee that has developed standards for a wide range of local area networks (LANs).
- In 1990, the IEEE 802 Committee formed a new working group, IEEE 802.11, with a charter to develop a protocol and transmission specifications for wireless LANs (WLANs).
- Since that time, the demand for WLANs at different frequencies and data rates has exploded. Keeping pace with this demand, the IEEE 802.11 working group has issued an ever-expanding list of standards

Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations.
Basic service set (BSS)	A set of stations controlled by a single coordination function.
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs.
Distribution system (DS)	A system used to interconnect a set of BSSs and integrated LANs to create an ESS.
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs.
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entities using the services of the physical layer.
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users.
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer.

The Wi-Fi Alliance

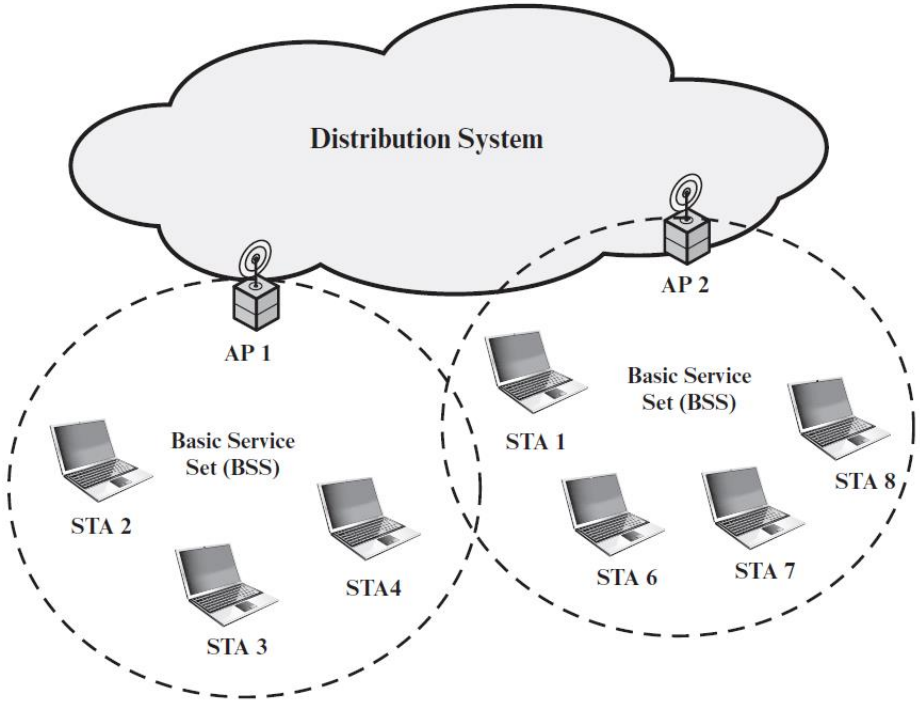
- 802.11b products are all based on the same standard, there is always a concern whether products from different vendors will successfully interoperate.
- To meet this concern, the Wireless Ethernet Compatibility Alliance (WECA), an industry consortium, was formed in 1999.
- This organization, subsequently renamed the Wi-Fi (Wireless Fidelity) Alliance, created a test suite to certify interoperability for 802.11b products.
- The term used for certified 802.11b products is ***Wi-Fi*.**
- Wi-Fi certification has been extended to 802.11g products.
- The Wi-Fi Alliance has also developed a certification process for 802.11a products, called ***Wi-Fi5***.
- The Wi-Fi Alliance is concerned with a range of market areas for WLANs, including enterprise, home, and hot spots.
- More recently, the Wi-Fi Alliance has developed certification procedures for IEEE 802.11 security standards, referred to as **Wi-Fi Protected Access (WPA**).
- The most recent version of WPA, known as WPA2, incorporates all of the features of the IEEE 802.11i WLAN security specification.

IEEE 802.11 Protocol Stack



IEEE 802.11 Network Components and Architectural Model

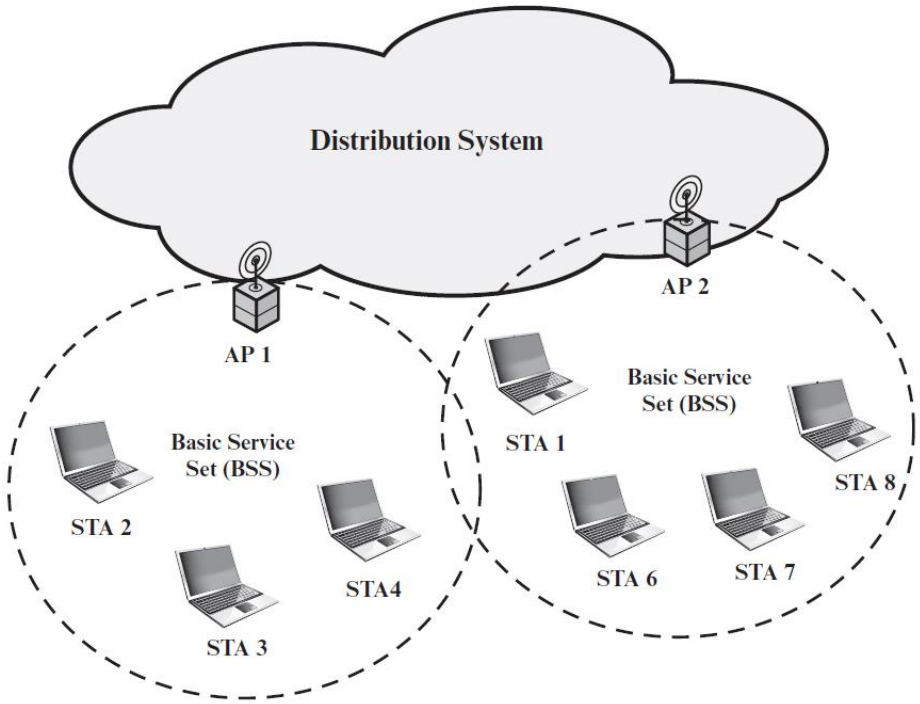
- The smallest building block of a wireless LAN is a **basic service set (BSS)**,
- BSS consists of wireless stations executing the same MAC protocol and competing for access to the same shared wireless medium.
- A BSS may be isolated, or it may connect to a backbone **distribution system (DS)** through an **access point (AP)**.
- The **AP** functions as a bridge and a relay point.
- In a **BSS**, client stations do not communicate directly with one another.



In the figure, each station belongs to a single **BSS**; that is, each station is within wireless range only of other stations within the same **BSS**.

IEEE 802.11 Network Components and Architectural Model

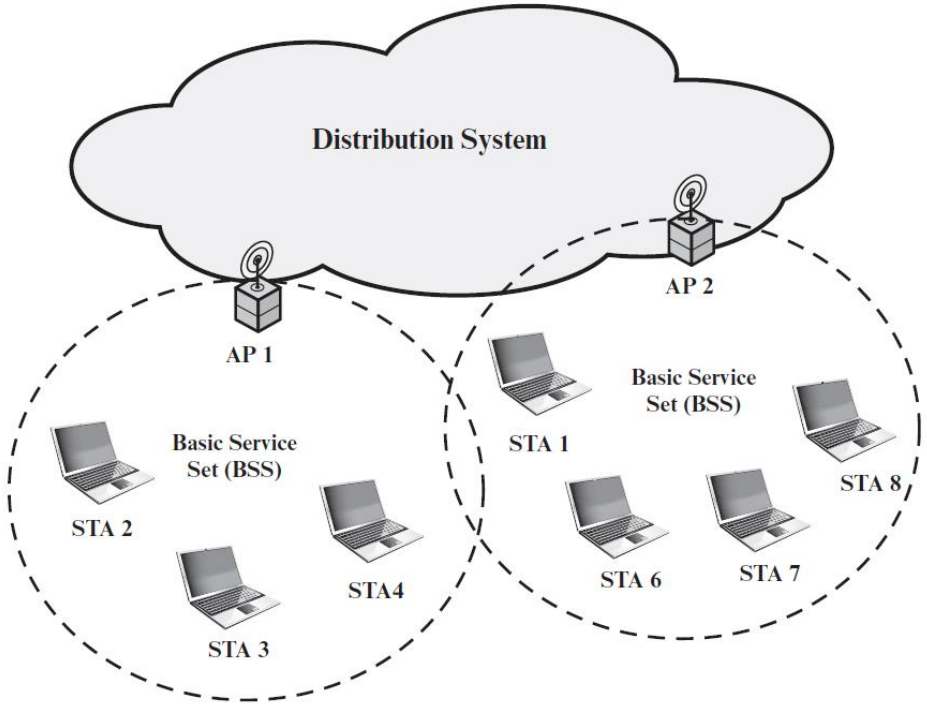
- If one station in the **BSS** wants to communicate with another station in the same **BSS**, the **MAC** frame is first sent from the originating station to the **AP** and then from the **AP** to the destination station.
- Similarly, a **MAC** frame from a station in the **BSS** to a remote station is sent from the local station to the **AP** and then relayed by the **AP** over the **DS** on its way to the destination station.
- The **BSS** generally corresponds to a **cell**.
- The **DS** can be a switch, a wired network, or a wireless network.



- An extended service set (ESS) consists of two or more basic service sets interconnected by a distribution system.
- The extended service set appears as a single logical LAN to the logical link control (LLC) level.

IEEE 802.11 Network Components and Architectural Model

- When all the stations in the **BSS** are mobile stations that communicate directly with one another (not using an **AP**), the **BSS** is called an **independent BSS (IBSS).**
- An **IBSS** is typically an ad hoc network.
- In an **IBSS**, the stations all communicate directly, and no **AP** is involved.
- It is also possible for two BSSs to overlap geographically, so that a single station could participate in more than one BSS.
- The association between a station and a BSS is dynamic. Stations may turn off, come within range, and go out of range.



IEEE 802.11 Services

- IEEE 802.11 defines nine services that need to be provided by the wireless LAN to achieve functionality equivalent to that which is inherent to wired LANs.
- The service provider can be either the station or the DS.
- Station services are implemented in every 802.11 station, including AP stations.
- Distribution services are provided between BSSs; these services may be implemented in an AP or in another special-purpose device attached to the distribution system.

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassociation	Distribution system	MSDU delivery

- The MAC layer receives data from a higher-layer protocol, typically the Logical Link Control (LLC) layer, in the form of a block of data known as the **MAC service data unit (MSDU)**.
- On transmission, MAC layer assemble data into a frame, known as a **MAC protocol data unit (MPDU)** with address and error-detection fields.

IEEE 802.11 Services

- Three of the services are used to control IEEE 802.11 LAN access and confidentiality.
- Six of the services are used to support delivery of MSDUs between stations.
- If the MSDU is too large to be transmitted in a single MPDU, it may be fragmented and transmitted in a series of MPDUs.

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassociation	Distribution system	MSDU delivery

- The MAC layer receives data from a higher-layer protocol, typically the Logical Link Control (LLC) layer, in the form of a block of data known as the **MAC service data unit (MSDU)**.
- On transmission, MAC layer assemble data into a frame, known as a **MAC protocol data unit (MPDU)** with address and error-detection fields.

IEEE 802.11 Wireless LAN

- There are two characteristics of a wired LAN that are not inherent in a wireless LAN.

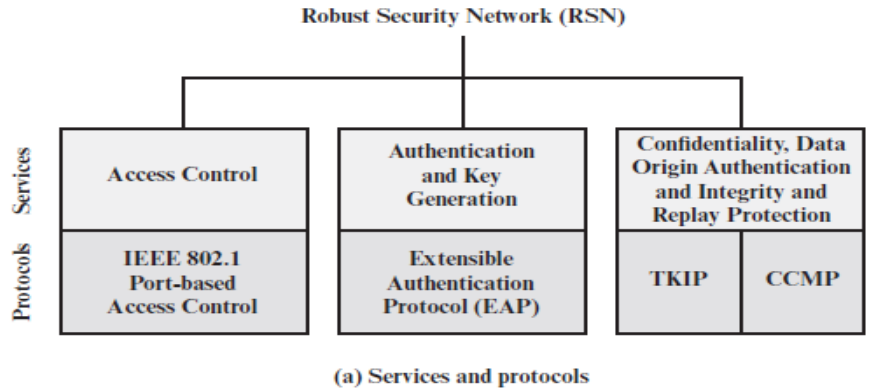
1. In order to transmit over a wired LAN, a station must be physically connected to the LAN.
   - On the other hand, with a wireless LAN, any station within radio range of the other devices on the LAN can transmit.
   - In a sense, there is a form of authentication with a wired LAN in that it requires some positive and presumably observable action to connect a station to a wired LAN.
2. **I**n order to receive a transmission from a station that is part of a wired LAN, the receiving station also must be attached to the wired LAN.
   - On the other hand, with a wireless LAN, any station within radio range can receive.
   - Thus, a wired LAN provides a degree of privacy, limiting reception of data to stations connected to the LAN.

IEEE 802.11 Wireless LAN

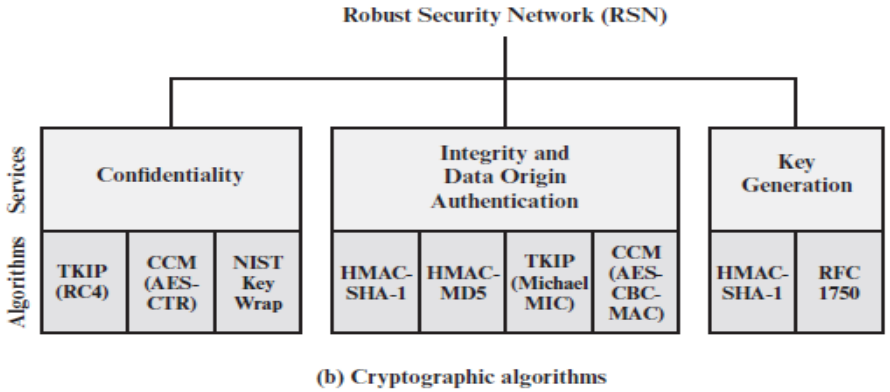
- These differences between wired and wireless LANs suggest the increased need for robust security services and mechanisms for wireless LANs.
- The original 802.11 specification included a set of security features for privacy and authentication that were quite weak. For privacy, 802.11 defined the **Wired Equivalent Privacy (WEP)** algorithm.
- The privacy portion of the 802.11 standard contained major weaknesses. Subsequent to the development of WEP, the 802.11i task group has developed a set of capabilities to address the WLAN security issues.
- In order to accelerate the introduction of strong security into WLANs, the Wi-Fi Alliance promulgated **Wi-Fi Protected Access (WPA)** as a Wi-Fi standard.
- **WPA** is a set of security mechanisms that eliminates most 802.11 security issues and was based on the current state of the 802.11i standard.
- The final form of the 802.11i standard is referred to as **Robust Security Network (RSN)**.
- The Wi-Fi Alliance certifies vendors in compliance with the full 802.11i specification under the WPA2 program.

IEEE 802.11i Services

- **Authentication:** A protocol is used to define an exchange between a user and an AS that provides mutual authentication and generates temporary keys to be used between the client and the AP over the wireless link.
- **Access control:** This function enforces the use of the authentication function, routes the messages properly, and facilitates key exchange. It can work with a variety of authentication protocols.
- **Privacy with message integrity:** MAC-level data (e.g., an LLC PDU) are encrypted along with a message integrity code that ensures that the data have not been altered.



(a) Services and protocols



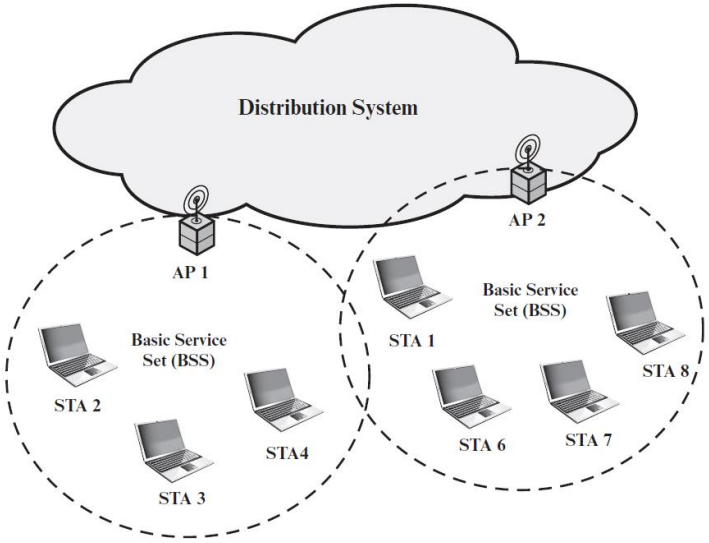
(b) Cryptographic algorithms

CBC-MAC = Cipher Block Chaining Message Authentication Code (MAC)
CCM = Counter Mode with Cipher Block Chaining Message Authentication Code
CCMP = Counter Mode with Cipher Block Chaining MAC Protocol
TKIP = Temporal Key Integrity Protocol

IEEE 802.11i Phases of Operation

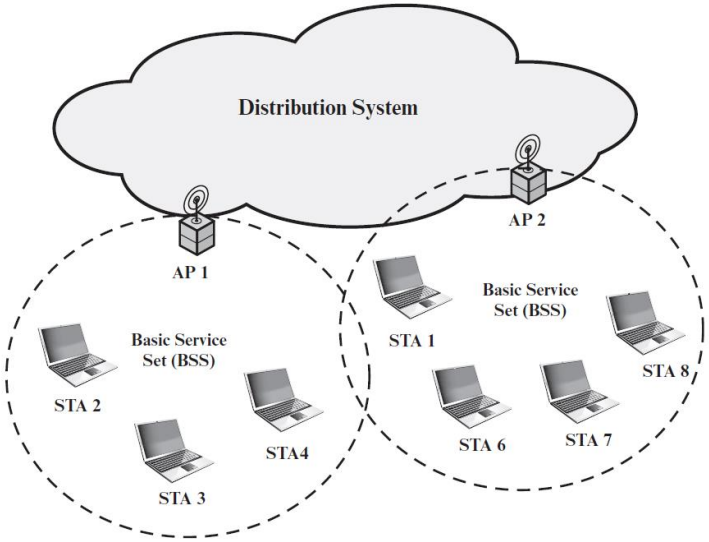
- The operation of an IEEE 802.11i RSN can be broken down into five distinct phases of operation.
- The exact nature of the phases will depend on the configuration and the end points of the communication.
- **Cases:**

1. Two wireless stations in the same BSS communicating via the access point (AP) for that BSS.
2. Two wireless stations (STAs) in the same ad hoc IBSS communicating directly with each other.
3. Two wireless stations in different BSSs communicating via their respective APs across a distribution system.
4. A wireless station communicating with an end station on a wired network via its AP and the distribution system.



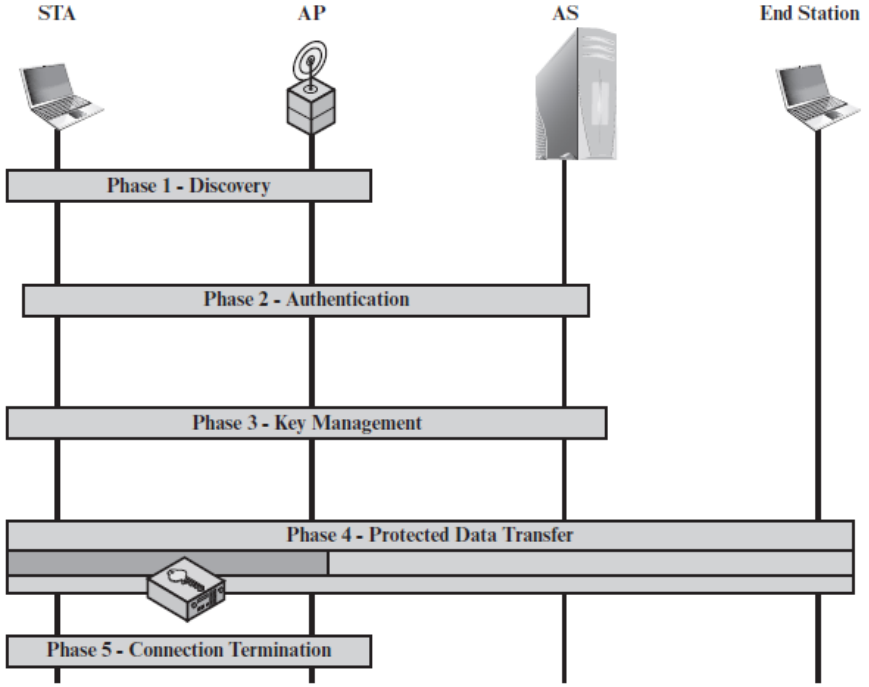
IEEE 802.11i Phases of Operation

- IEEE 802.11i security is concerned only with secure communication between the STA and its AP.
- In case 1 in the preceding list, secure communication is assured if each STA establishes secure communications with the AP.
- Case 2 is similar, with the AP functionality residing in the STA.
- For case 3, security is not provided across the distribution system at the level of IEEE 802.11, but only within each BSS. End-to-end security (if required) must be provided at a higher layer.
- Similarly, in case 4, security is only provided between the STA and its AP.



IEEE 802.11i Phases of Operation

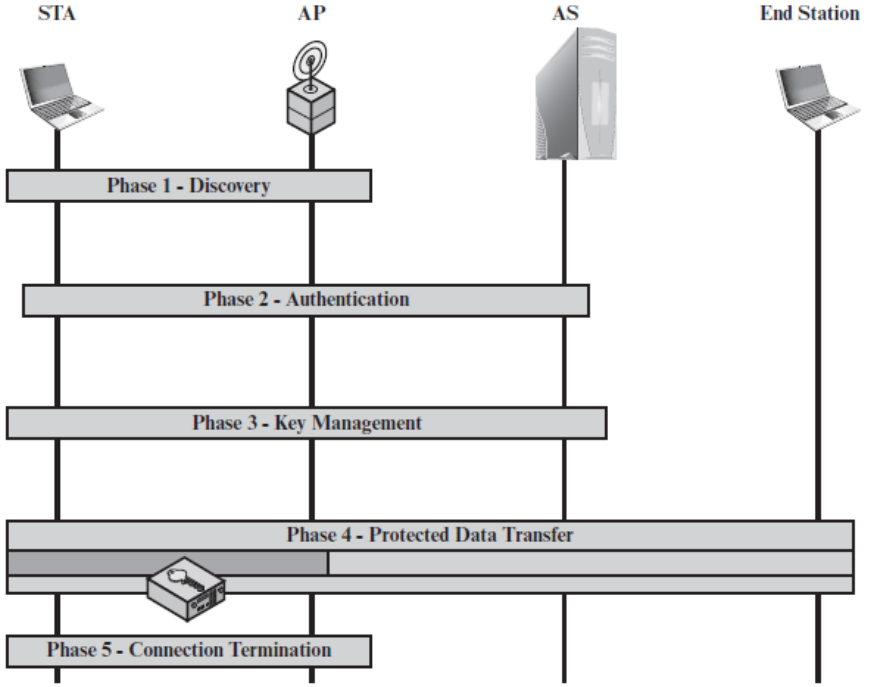
- **Discovery:**
  - An AP uses messages called Beacons and Probe Responses to advertise its IEEE 802.11i security policy.
  - The STA uses these to identify an AP for a WLAN with which it wishes to communicate.
  - The STA associates with the AP, which it uses to select the cipher suite and authentication mechanism when the Beacons and Probe Responses present a choice.
- **Authentication:**
  - During this phase, the STA and AS prove their identities to each other.
  - The AP blocks non-authentication traffic between the STA and AS until the authentication transaction is successful.
  - The AP does not participate in the authentication transaction other than forwarding traffic between the STA and AS.



IEEE 802.11i Phases of Operation.
The rectangles indicate the exchange of sequences of MPDUs

IEEE 802.11i Phases of Operation

- **Key generation and distribution:**
  - The AP and the STA perform several operations that cause cryptographic keys to be generated and placed on the AP and the STA.
  - Frames are exchanged between the AP and STA only.
- **Protected data transfer:**
  - Frames are exchanged between the STA and the end station through the AP.
  - As denoted by the shading and the encryption module icon, secure data transfer occurs between the STA and the AP only; security is not provided end-to-end.
- **Connection termination:**
  - The AP and STA exchange frames.
  - During this phase, the secure connection is torn down and the connection is restored to the original state.



IEEE 802.11i Phases of Operation.
The rectangles indicate the exchange of sequences of MPDUs


Thanks
kids!!