Cryptography and Network Security

Chapter 12

Wireless Network Security

Lectured by
Nguyễn Đức Thái

Outline

- IEEE 802.11 Wireless LAN Overview
- IEEE 802.11i Wireless LAN Security
- Wireless Application Protocol Overview
- Wireless Transport Layer Security
- WAP End-to-End Security

Key Points (1/2)

- **IEEE 802.11** is a ***standard*** for wireless LANs. Interoperable standardscompliant implementations are referred to as **Wi-Fi**.
- IEEE 802.11i specifies ***security standards*** for IEEE 802.11 LANs, including:
  - authentication,
  - data integrity,
  - data confidentiality, and
  - key management.
- Interoperable implementations are also referred to as Wi-Fi Protected Access (**WPA**).

Key Points (2/2)

- The Wireless Application Protocol (**WAP**) is a ***standard*** to provide ***mobile users*** of wireless phones and other wireless terminals access to telephony and information services, including the Internet and the Web
- WAP security is primarily provided by the Wireless Transport Layer Security (**WTLS**), which provides security services between the mobile device and the WAP gateway to the Internet.
- There are several approaches to WAP end-to-end security. One notable approach assumes that the mobile device implements TLS over TCP/IP and the wireless network supports transfer of IP packets.

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*** contributing to the higher security risk of wireless networks compared to wired networks include the following:
  - Channel
  - Mobility
  - Resources
  - Acessibility

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*, described subsequently

Resources

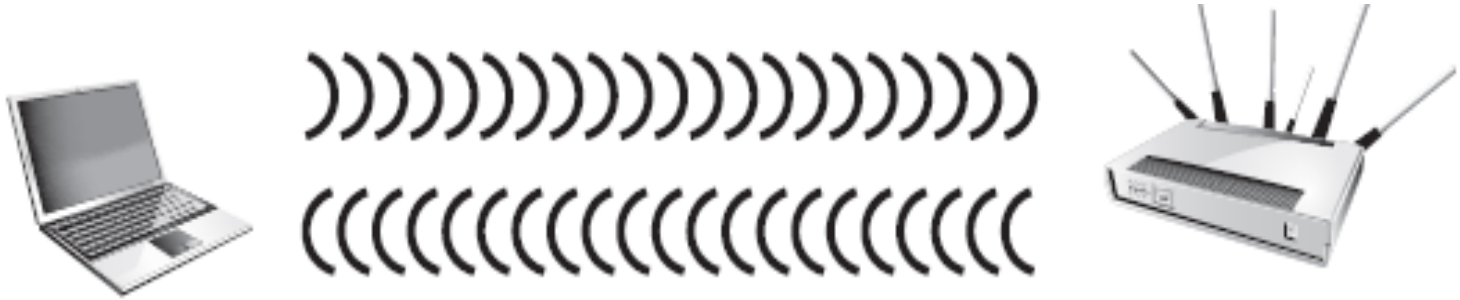
- Some wireless devices, such as *smartphones* and *tablets*, have sophisticated operating systems but limited memory and processing resources with which to counter *threats*, including ***denial of service*** and ***malware***

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 Network

- The 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.
- Examples of access points are 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



Endpoint Wireless medium Access point

Wireless Network Threats

- Accidental association
- Malicious association
- Ad hoc networks
- Nontraditional networks
- Identity theft (MAC spoofing)
- Man-in-the middle attacks
- Denial of service (DoS)
- Network injection

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

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.

Denial of service (DoS)

- In the *context of a wireless network*, 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

- We can group wireless security measures into those dealing with
  - *wireless transmissions,*
  - *wireless access points, and*
  - *wireless networks (consisting of wireless routers and endpoints).*

Securing Wireless Transmission

- 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*
  - *Encryption*

Signal-Hiding Techniques

- ***Turn of*** SSID,
- Assign ***cryptic names*** to SSIDs
- ***Reduce*** signal strength to the lowest level that still provides requisite coverage
- ***Locate*** 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

Encryption

- Encryption of all wireless transmission is effective against eavesdropping to the extent that the encryption keys are secured

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.

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.

Securing Wireless Networks

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.

Wireless LAN Security Overview

- **IEEE 802 committee for LAN standards**
- **IEEE 802.11 formed in 1990's**
  - charter to develop a protocol & transmission specifications for ***wireless LANs*** (WLANs)
- **since then *demand* for WLANs, at different *frequencies* and *data rates*, has exploded**
- **hence seen ever-expanding list of standards issued**

IEEE 802.11 Terminologies

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 entites 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

Wi-Fi Alliance (1/2)

- The first 802.11 standard to gain broad industry acceptance was 802.11**b**.
- Although 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,.

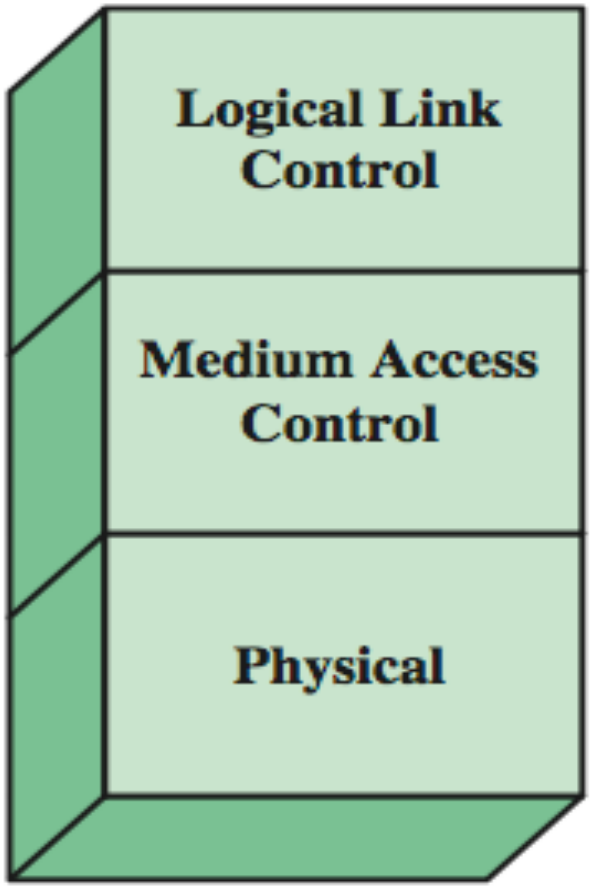
Wi-Fi Alliance (2/2)

- 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 Protocol Architecture



	General IEEE 802 functions	Specific IEEE 802.11 functions
Logical Link Control	Flow control Error control	
Medium Access Control	Assemble data into frame Addressing Error detection Medium access	Reliable data delivery Wireless access control protocols
Physical	Encoding/decoding of signals Bit transmission/ reception Transmission medium	Frequency band definition Wireless signal encoding

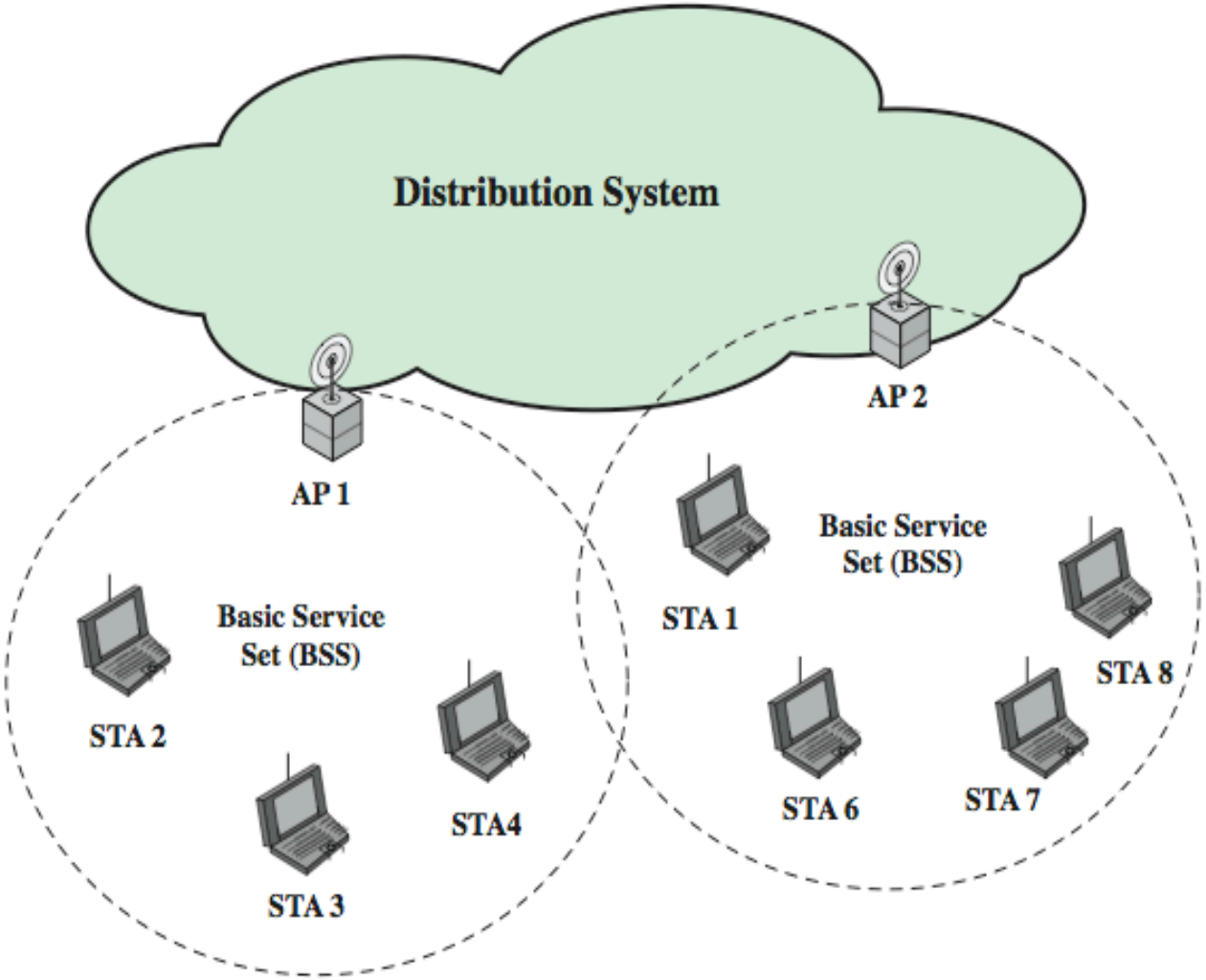
IEEE 802 Protocol Architecture

- ***Physical layer*:**
  - encoding/decoding of signals and bit transmission/reception.
  - specification of the transmission medium
  - defines frequency bands and antenna characteristics
- ***Media Access Control***
  - On transmission, assemble data into a frame, known as a MAC protocol data unit (MPDU) with address and error-detection fields.
  - On reception, disassemble frame, and perform address recognition and error detection.
  - Govern access to the LAN transmission medium.

IEEE 802 Protocol Architecture

- ***Logical Link Control***: (MAC + LLC)
  - In most data-link control protocols, the data-link protocol entity is ***responsible*** ***not only*** ***for detecting errors*** using the CRC, ***but*** for ***recovering*** from those errors by retransmitting damaged frames.
  - ***Two functions*** are split between the MAC and LLC layers.
  - The ***MAC layer*** is responsible for ***detecting errors*** and ***discarding*** any frames that contain errors.
  - The ***LLC layer*** optionally ***keeps track*** of which frames have been successfully received and retransmits unsuccessful frames.

Network Components & Architecture



Extended Service Set

IEEE802.11 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.

Two categories

1. 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.
2. ***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.

IEEE802.11 Services

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Dissassociation	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

IEEE 802.11i – Wireless LAN Security

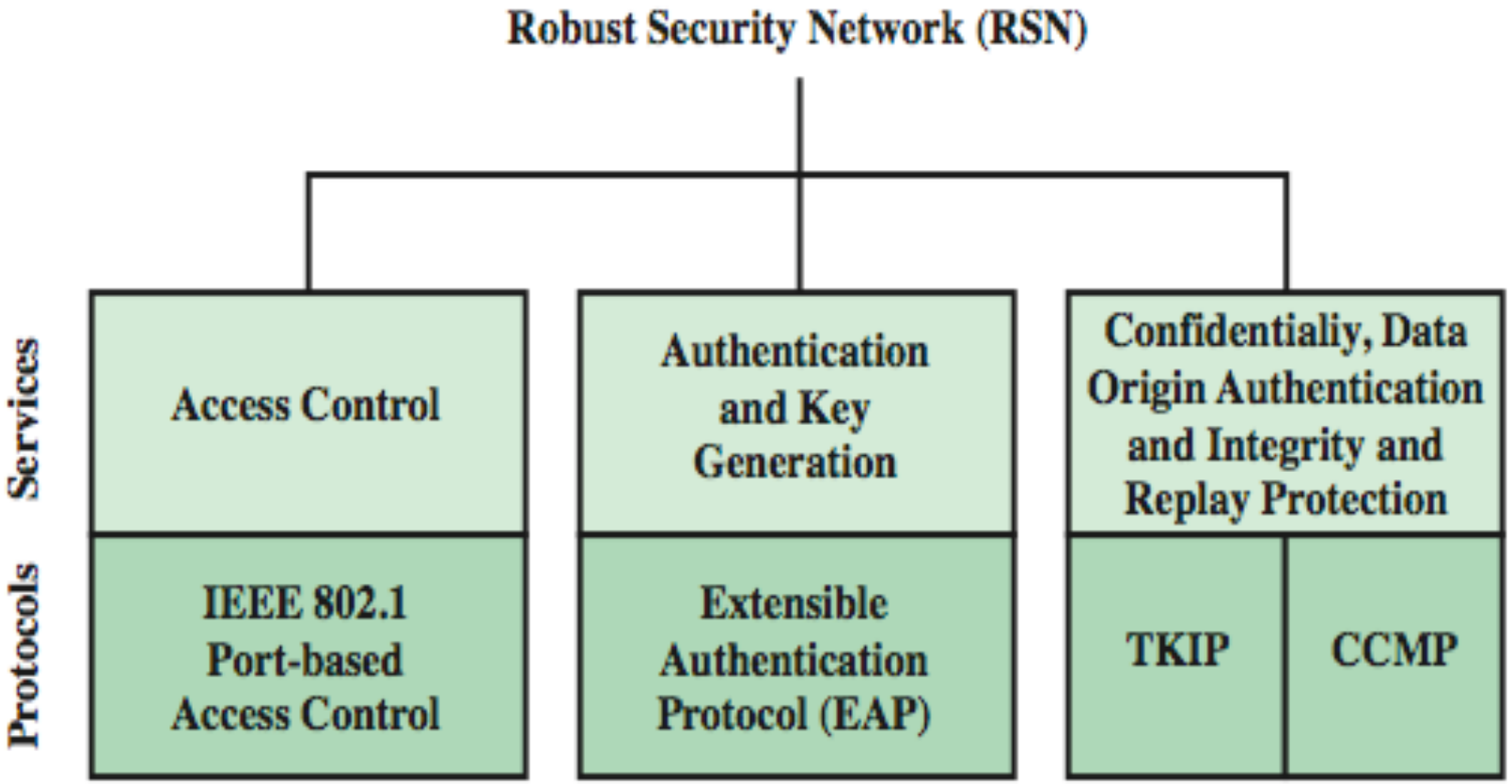
- For privacy, 802.11 defined the **W**ired **E**quivalent **P**rivacy (**WEP**) algorithm.
- **Wi-Fi Alliance** promulgated **W**i-Fi **P**rotected **A**ccess (**WPA**) as a Wi-Fi standard.
- WPA is a ***set of security mechanisms*** that eliminates most 802.11 security issues and was based on the current 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

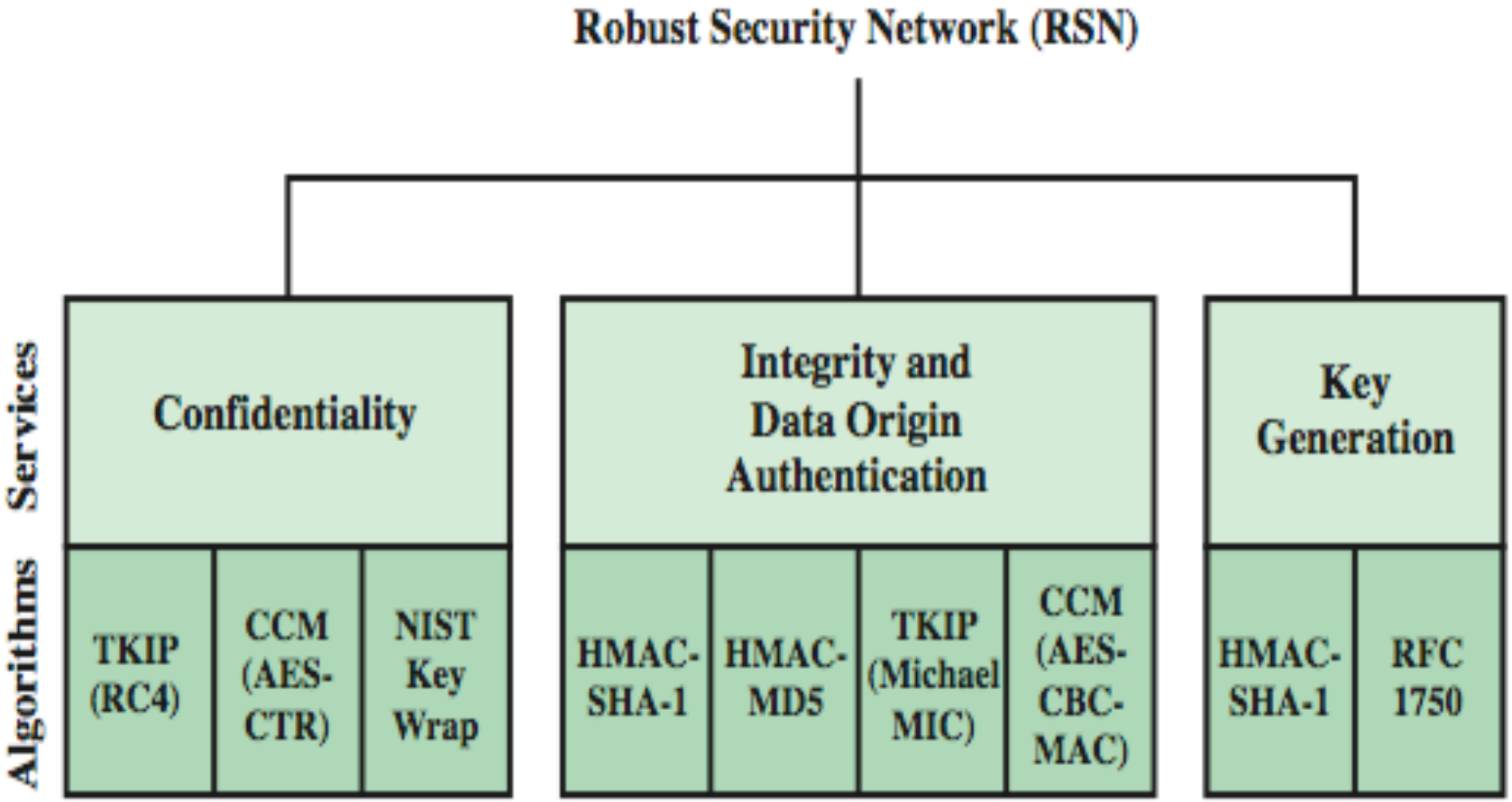
The 802.11i RSN security specification defines the following services.

- **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.

IEEE 802.11i Services



802.11i RSN Cryptographic Algorithms

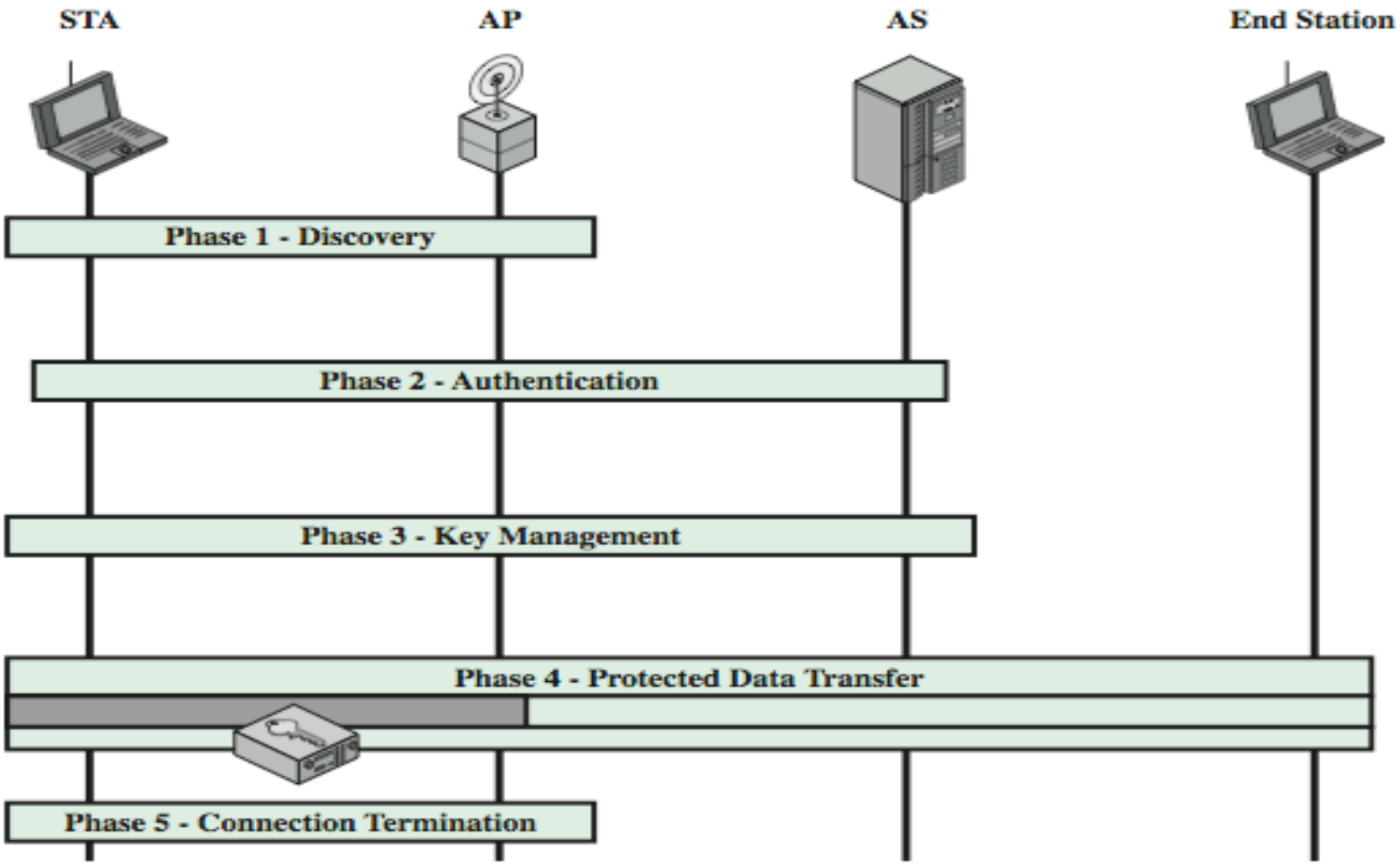


IEEE 802.11i RSN Phases of Operation

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:

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 RSN Phases of Operation



Summary

- IEEE 802.11 Wireless LAN Overview
- IEEE 802.11i Wireless LAN Security
- Wireless Application Protocol Overview
- Wireless Transport Layer Security
- WAP End-to-End Security

References

1. Cryptography and Network Security, Principles and Practice, William Stallings, Pearson, Seventh Edition, 2017