Wireless Network Security

Bojan Božić

By: William Stallings and Lawrie Brown

Chapter 24

Wireless Network Security

Wireless Security

- Key factors contributing to higher security risk of wireless networks compared to wired networks include:
  - **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 far more portable and mobile, thus resulting in a number of risks
  - **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, thus greatly increasing their vulnerability to physical attacks

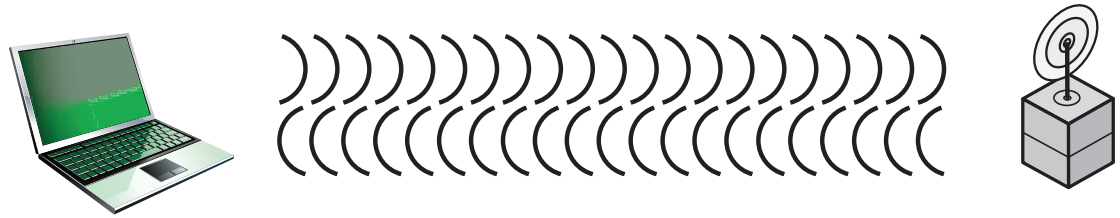


Figure 24.1 Wireless Networking Components

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

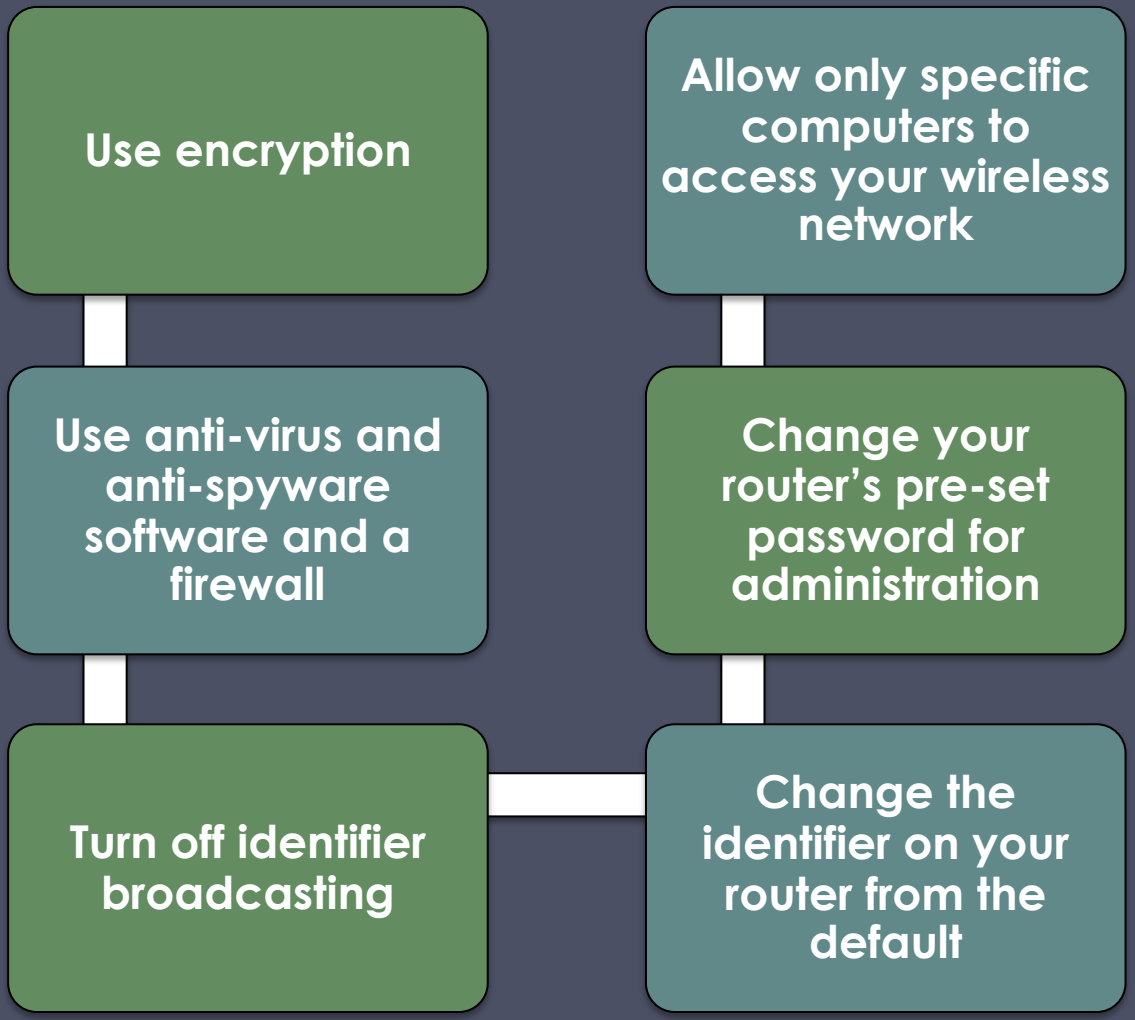
Securing Wireless Transmissions

- Principal threats are eavesdropping, altering or inserting messages, and disruption
- Countermeasures for eavesdropping:
  - Signal-hiding techniques
  - Encryption
- The use of encryption and authentication protocols is the standard method of countering attempts to alter or insert transmissions

Securing Wireless Networks

- The main threat involving wireless access points is unauthorized access to the network
- 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
- Use of 802.1X can prevent rogue access points and other unauthorized devices from becoming insecure backdoors

Wireless Network Security Techniques



Mobile Device Security

- An organization's networks must accommodate:
  - **Growing use of new devices**
    - Significant growth in employee's use of mobile devices
  - **Cloud-based applications**
    - Applications no longer run solely on physical servers in corporate data centers
  - **De-perimeterization**
    - There are a multitude of network perimeters around devices, applications, users, and data
  - **External business requirements**
    - The enterprise must also provide guests, third-party contractors, and business partners network access using various devices from a multitude of locations

Security Threats

- Lack of physical security controls
- Use of untrusted networks
- Use of untrusted mobile devices
- Use of untrusted applications
- Interaction with other systems
- Use of untrusted content
- Use of location services

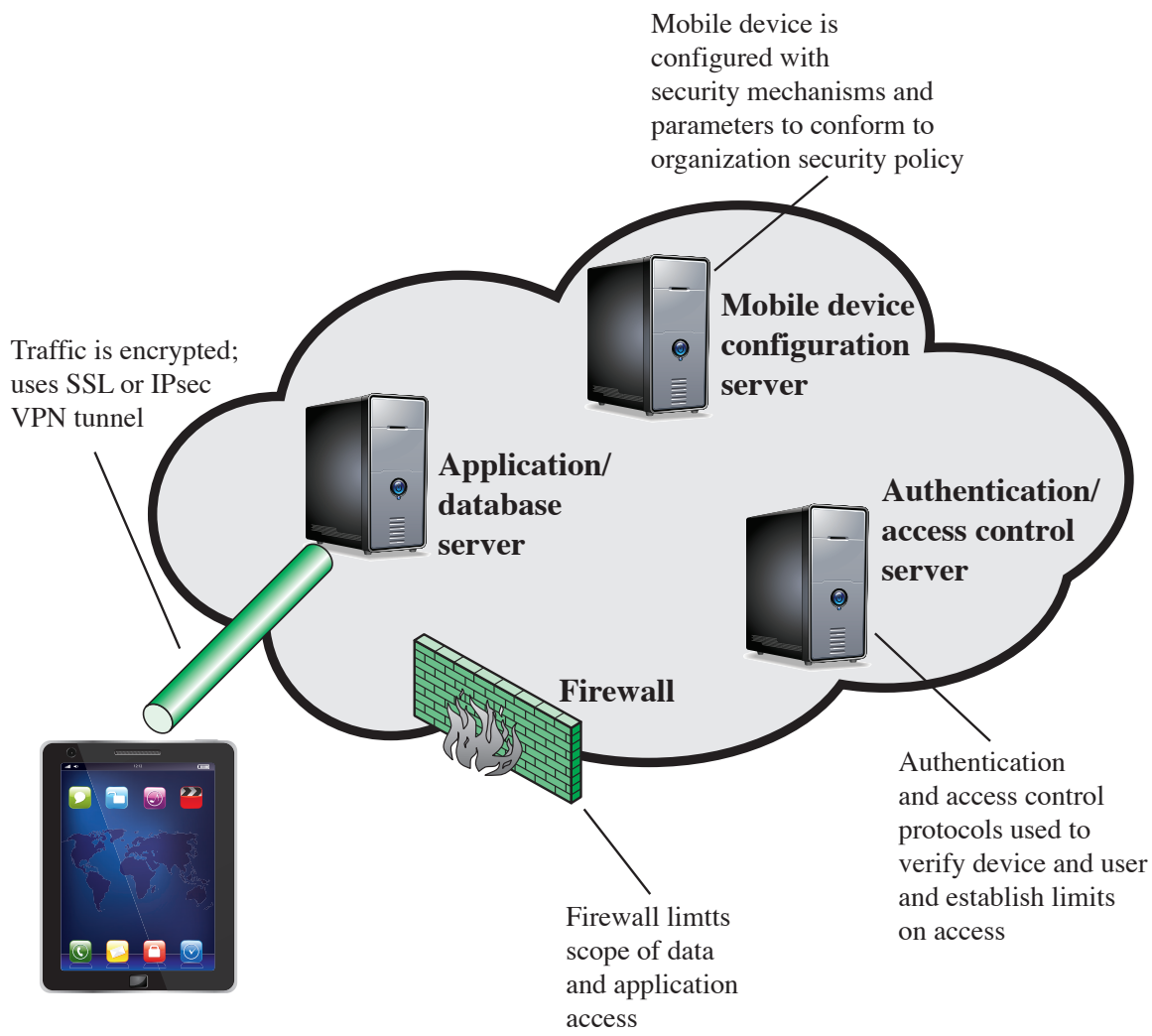


Figure 24.2 Mobile Device Security Elements

Table 24.1
IEEE 802.11 Terminology

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.

Wireless Fidelity (Wi-Fi) Alliance

- 802.11b
  - First 802.11 standard to gain broad industry acceptance
- Wireless Ethernet Compatibility Alliance (WECA)
  - Industry consortium formed in 1999 to address the concern of products from different vendors successfully interoperating
  - Later renamed the Wi-Fi Alliance
- Term used for certified 802.11b products is *Wi-Fi*
  - Has been extended to 802.11g products
- Wi-Fi Protected Access (WPA)
  - Wi-Fi Alliance certification procedures for IEEE802.11 security standards
  - WPA2 incorporates all of the features of the IEEE802.11i WLAN security specification

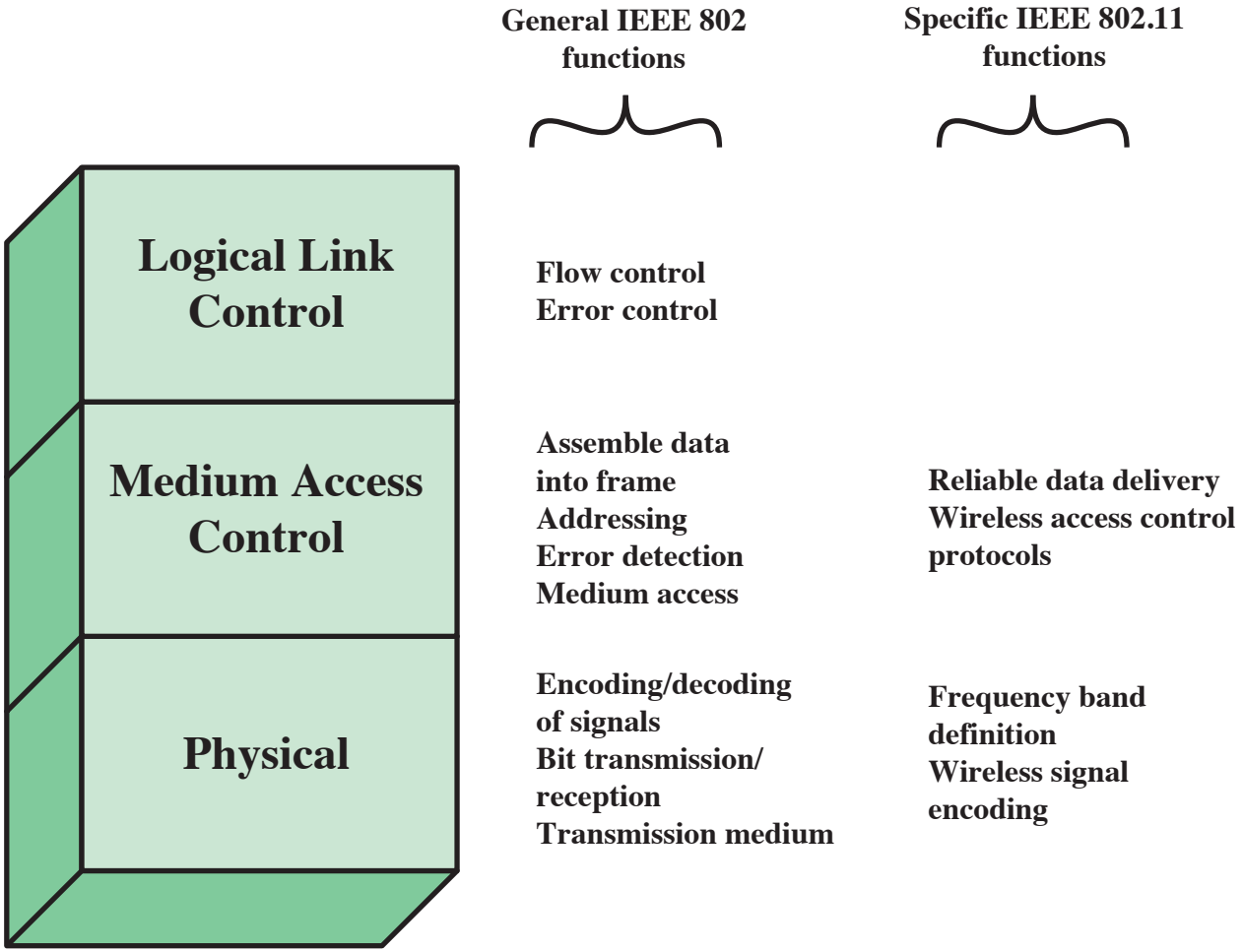


Figure 24.3 IEEE 802.11 Protocol Stack

Figure 24.4 General IEEE 802 MPDU Format

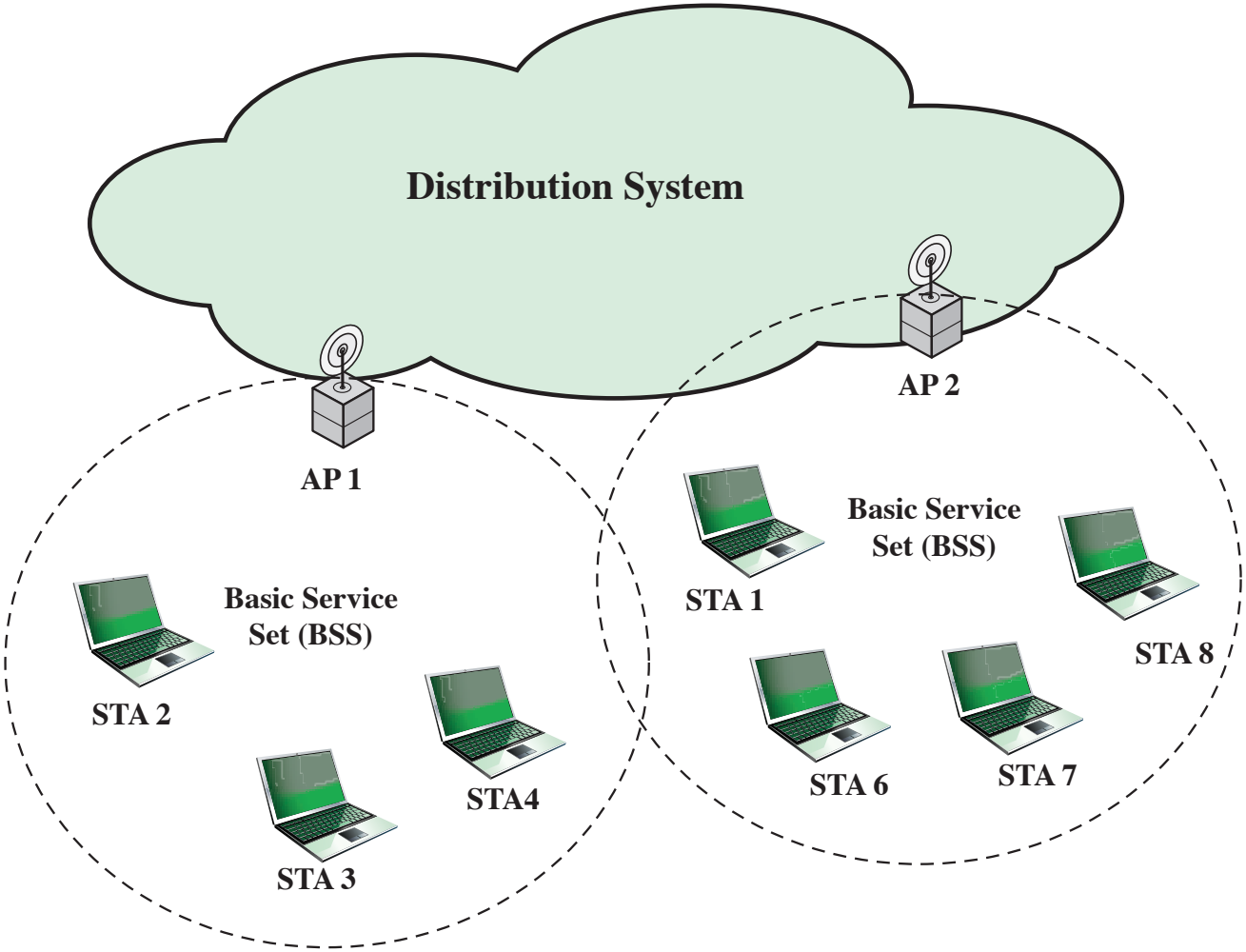


Figure 24.5 IEEE 802.11 Extended Service Set

Table 24.2
IEEE 802.11 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

Distribution of Messages Within a DS

- The two services involved with the distribution of messages within a DS are:
  - Distribution
  - Integration

Distribution

- The primary service used by stations to exchange MPDUs when the MPDUs must traverse the DS to get from a station in one BSS to a station in another BSS

Integration

- Enables transfer of data between a station on an IEEE 802.11 LAN and a station on an integrated IEEE 802x LAN
- Service enables transfer of data between a station on an IEEE 802.11 LAN and a station on an integrated IEEE 802.x LAN

Association-Related Services

- Transition types, based on mobility:
  - No transition
    - A station of this type is either stationary or moves only within the direct communication range of the communicating stations of a single BSS
  - BSS transition
    - Station movement from one BSS to another BSS within the same ESS; delivery of data to the station requires that the addressing capability be able to recognize the new location of the station
  - ESS transition
    - Station movement from a BSS in one ESS to a BSS within another ESS; maintenance of upper-layer connections supported by 802.11 cannot be guaranteed

Services

Association

- Establishes an initial association between a station and an AP

Reassociation

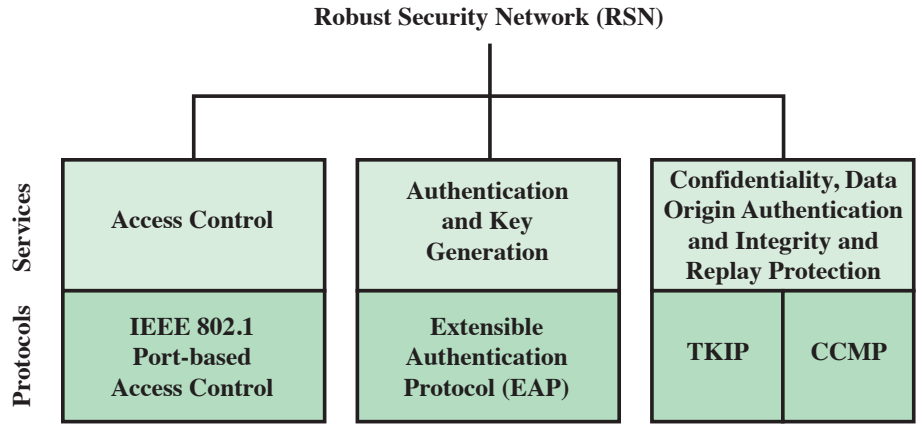
- Enables an established association to be transferred from one AP to another, allowing a mobile station to move from one BSS to another

Disassociation

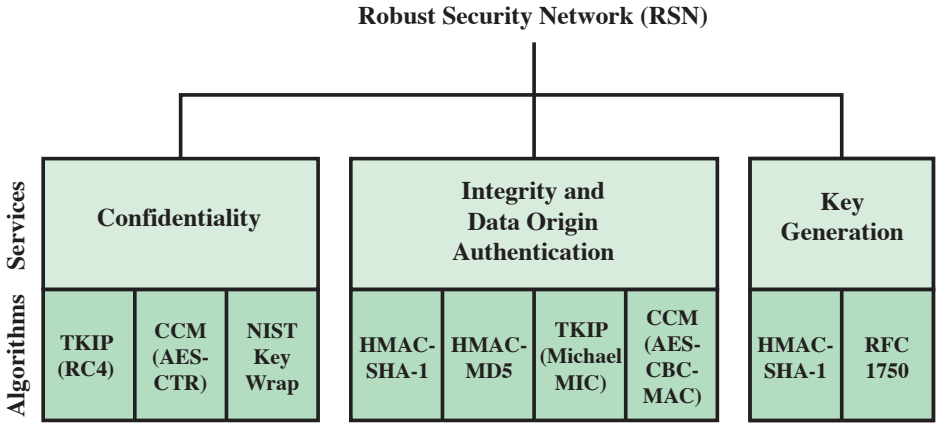
- A notification from either a station or an AP that an existing association is terminated

Wireless LAN Security

- Wired Equivalent Privacy (WEP) algorithm
  - 802.11 privacy
- Wi-Fi Protected Access (WPA)
  - Set of security mechanisms that eliminates most 802.11 security issues and was based on the current state of the 802.11i standard
- Robust Security Network (RSN)
  - Final form of the 802.11i standard
- Wi-Fi Alliance certifies vendors in compliance with the full 802.11i specification under the WPA2 program



(a) Services and Protocols



(b) Cryptographic Algorithms

CBC-MAC = Cipher Block 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

Figure 24.6 Elements of IEEE 802.11i

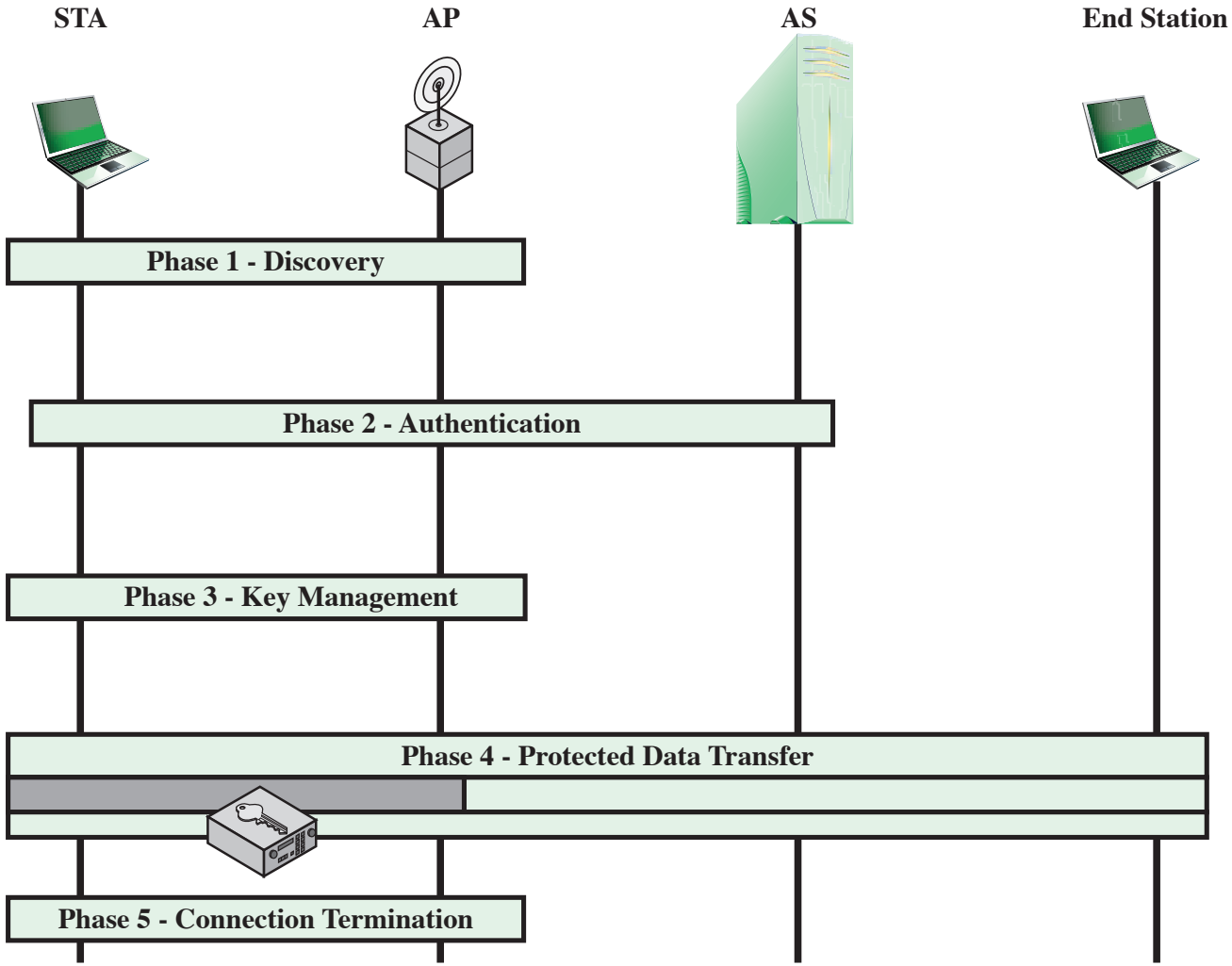


Figure 24.7 IEEE 802.11i Phases of Operation

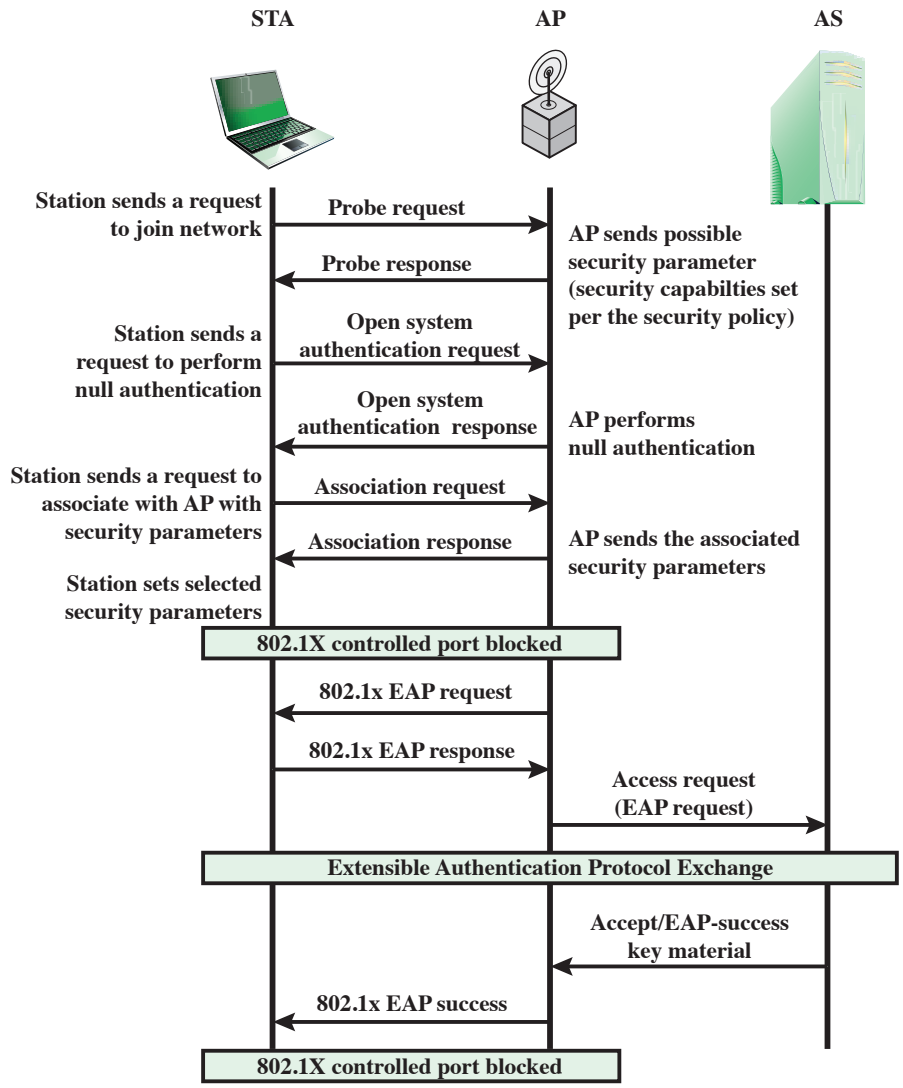


Figure 24.8 IEEE 802.11i Phases of Operation: Capability Discovery, Authentication, and Association

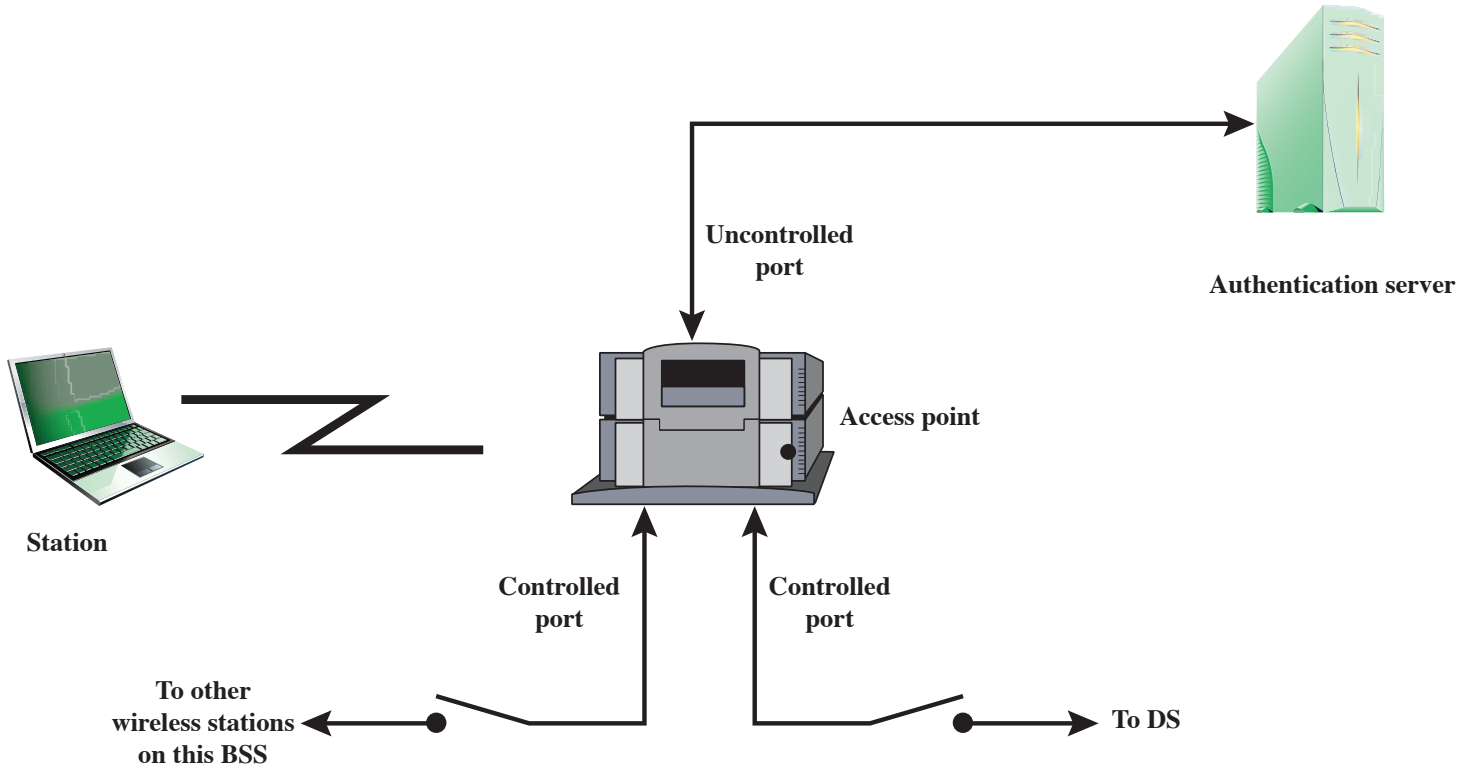
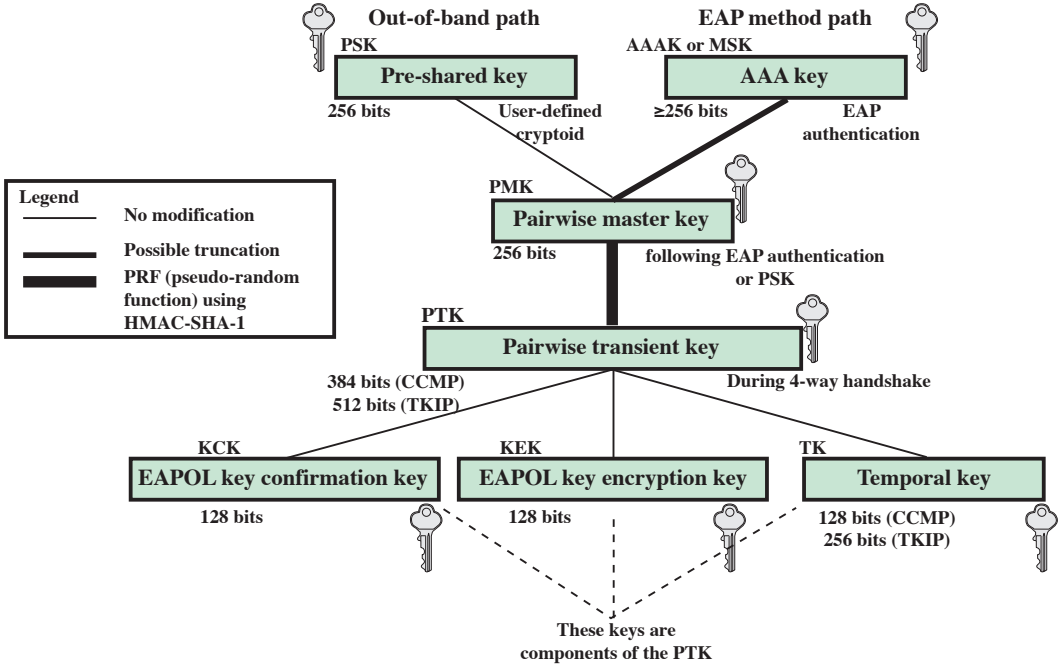


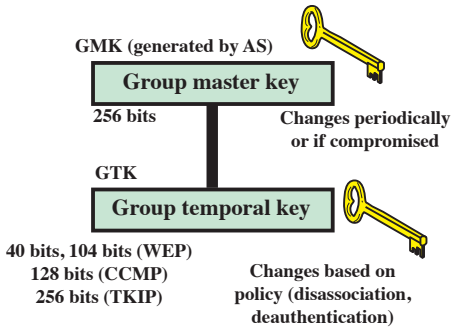
Figure 24.9 802.1X Access Control

MPDU Exchange

- Authentication phase consists of three phases:
  - Connect to AS
    - The STA sends a request to its AP that it has an association with for connection to the AS; the AP acknowledges this request and sends an access request to the AS
  - EAP exchange
    - Authenticates the STA and AS to each other
  - Secure key delivery
    - Once authentication is established, the AS generates a master session key and sends it to the STA



(a) Pairwise key hierarchy



(b) Group key hierarchy

Figure 24.10 IEEE 802.11i Key Hierarchies

Table 24.3

IEEE 802.11i Keys for Data Confidentiality and Integrity Protocols

Abbrev-iation	Name	Description / Purpose	Size (bits)	Type
AAA Key	Authentication, Accounting, and Authorization Key	Used to derive the PMK. Used with the IEEE 802.1X authentication and key management approach. Same as MMSK.	≥ 256	Key generation key, root key
PSK	Pre-Shared Key	Becomes the PMK in pre-shared key environments.	256	Key generation key, root key
PMK	Pairwise Master Key	Used with other inputs to derive the PTK.	256	Key generation key
GMK	Group Master Key	Used with other inputs to derive the GTK.	128	Key generation key
PTK	Pair-wise Transient Key	Derived from the PMK. Comprises the EAPOL-KCK, EAPOL-KEK, and TK and (for TKIP) the MIC key.	512 (TKIP) 384 (CCMP)	Composite key
TK	Temporal Key	Used with TKIP or CCMP to provide confidentiality and integrity protection for unicast user traffic.	256 (TKIP) 128 (CCMP)	Traffic key
GTK	Group Temporal Key	Derived from the GMK. Used to provide confidentiality and integrity protection for multicast/broadcast user traffic.	256 (TKIP) 128 (CCMP) 40, 104 (WEP)	Traffic key
MIC Key	Message Integrity Code Key	Used by TKIP's Michael MIC to provide integrity protection of messages.	64	Message integrity key
EAPOL-KCK	EAPOL-Key Confirmation Key	Used to provide integrity protection for key material distributed during the 4-Way Handshake.	128	Message integrity key
EAPOL-KEK	EAPOL-Key Encryption Key	Used to ensure the confidentiality of the GTK and other key material in the 4-Way Handshake.	128	Traffic key / key encryption key
WEP Key	Wired Equivalent Privacy Key	Used with WEP.	40, 104	Traffic key

(Table can be found on page 724 in the textbook.)

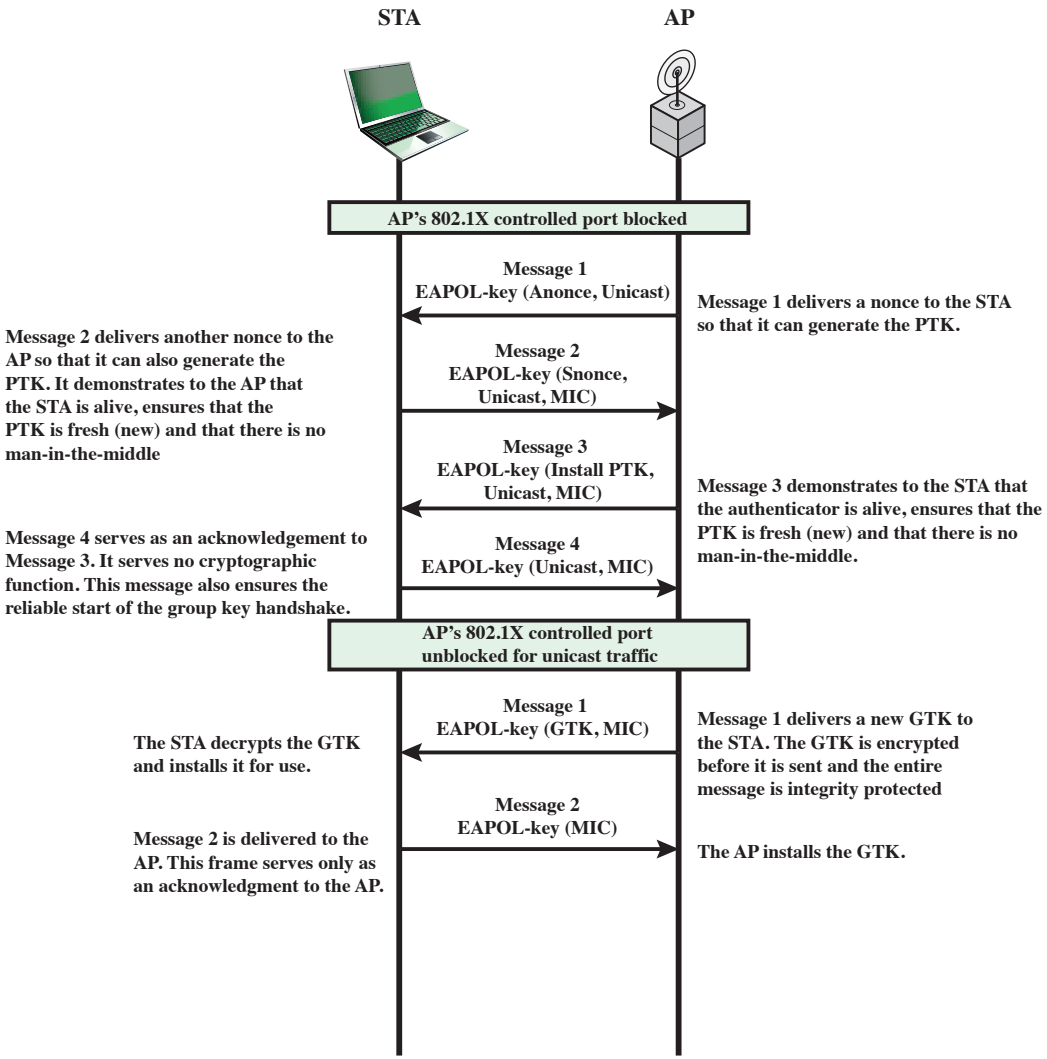


Figure 24.11 IEEE 802.11i Phases of Operation: Four-Way Handshake and Group Key Handshake

Temporal Key Integrity Protocol (TKIP)

- Designed to require only software changes to devices that are implemented with the older wireless LAN security approach called WEP
- Provides two services:

Message integrity

Adds a message integrity code to the 802.11 MAC frame after the data field

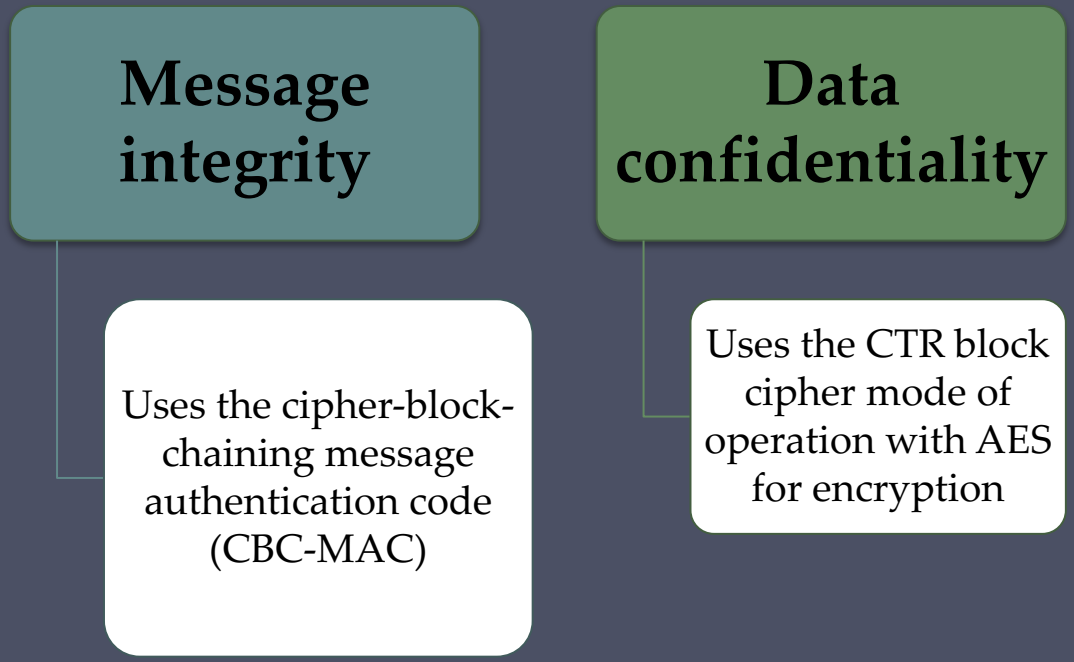
Data confidentiality

Provided by encrypting the MPDU

Counter Mode-CBC MAC Protocol (CCMP)

- Intended for newer IEEE 802.11 devices that are equipped with the hardware to support this scheme

- Provides two services:



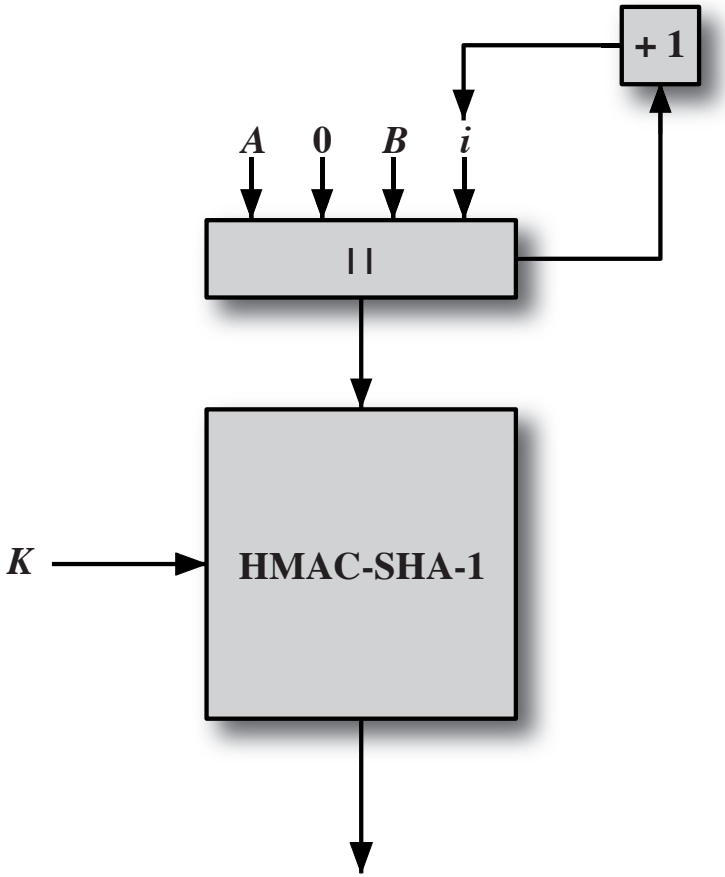


Figure 24.12 IEEE 802.11i Pseudorandom Function

Summary

- Wireless Security
  - Wireless network threats
  - Wireless security measures
- Mobile device security
  - Security threats
  - Mobile device security strategy
- IEEE 802.11 wireless LAN overview
  - The Wi-Fi alliance
  - IEEE 802 protocol architecture
  - IEEE 802.11 network components and architectural model
  - IEEE 802.11 services
- IEEE 802.11i wireless LAN security
  - IEEE 802.11i services
  - IEEE 802.11i phases of operation
  - Discovery phase
  - Authentication phase
  - Key management phase
  - Protected data transfer phase
  - The IEEE 802.11i pseudorandom function