Lecture 4
Wireless LANs and PANs

Reading:

- “Wireless LANs and PANs,” in *Ad Hoc Wireless Networks: Architectures and Protocols*, Chapter 2.

Use of WLANs

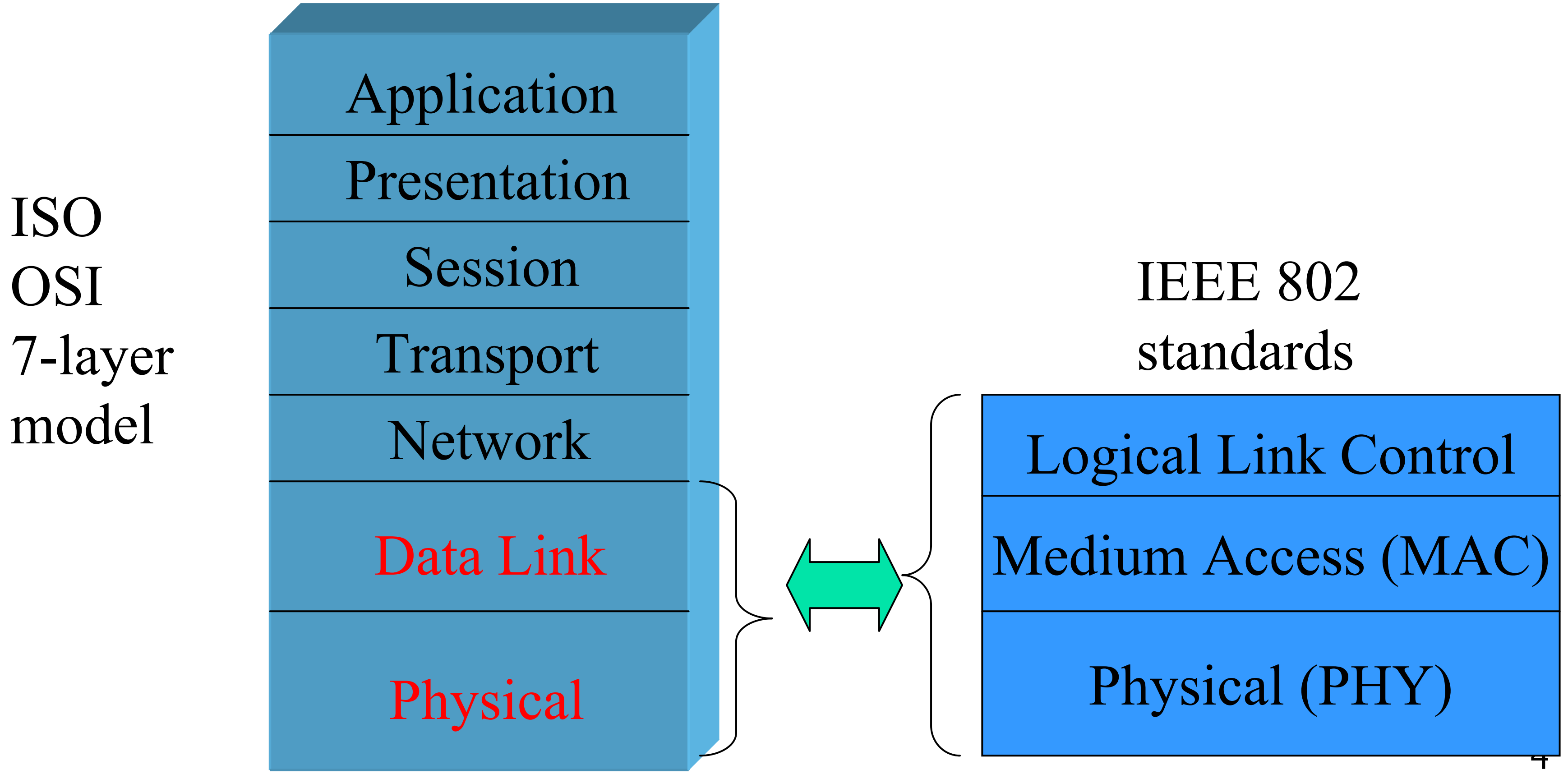
- Mobile Internet
- Home networking
- Office networking
- Temporary networks
- Coffee shop networks
- Airports
- …

Goals

- EASE OF USE
  - Easy to set up network
  - Easy to connect to network
  - Easy to roam across networks
- Power efficiency
- Cheap
  - License-free operation
- Robust to noise
  - Environmental
  - Other license-free systems
- Global usability
- Secure
  - Hard to access network without permission
  - Hard to access others' transmissions

Standardization

- Wireless networks standardized by IEEE
- Under 802 LAN MAN standards committee



IEEE 802.11 (WiFi) Overview

- Adopted in 1997
- Defines
  - MAC sublayer
  - MAC management protocols and services
  - Physical (PHY) layers
    - IR
    - FHSS
    - DSSS

Goals
• To deliver services in wired networks
• To achieve high throughput
• To achieve highly reliable data delivery
• To achieve continuous network connection

IEEE 802.11 Architecture

- Designed so that most decisions distributed to mobile stations
  - Fault tolerant
  - Eliminates bottlenecks
- Components of an 802.11 system
  - Stations
  - Access point (AP)
  - Basic service set (BSS)
  - Extended service set (ESS)
  - Distribution system (DS)

Station

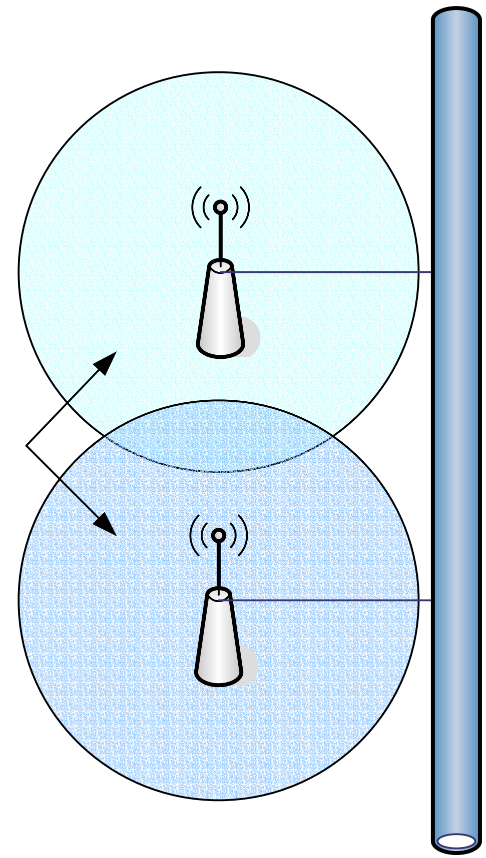
- Component that connects to the wireless medium
- Contains 802.11 MAC and PHY layers
- Supports “station services”
  - Authentication
  - Deauthentication
  - Privacy
  - Delivery of data

Basic Service Set

- Set of stations that communicate with each other
- Independent BSS (IBSS)
  - When all stations in a BSS are mobile and there is no connection to a wired network
  - Typically short-lived with a small number of stations
  - Ad-hoc in nature
  - Stations communicate directly with one another
  - No relay capabilities– nodes must be in direct range
- Infrastructure BSS (BSS)
  - Includes an Access Point (AP)
  - All mobiles communicate directly to AP
    - AP provides connection to wired LAN and relay functionality
    - Use of AP may increase BW (2-hop rather than 1-hop data tx)
    - AP provides central control, allows packet buffering, etc.

Extended Service Set (ESS)

- Set of infrastructure BSS's
  - AP's communicate with each other
  - Forward traffic from one BSS to another
  - Facilitate movement of stations from one BSS to another
- Extends range of mobility beyond reach of a single BSS



Distribution System (DS)

- Mechanism that allows APs to communicate with each other and wired infrastructure (if available)
- Backbone of the WLAN
- May contain both wired and wireless networks
- Functionality in each AP that determines where received packet should be sent
  - To another station within the same BSS
  - To the DS of another AP (e.g., sent to another BSS)
  - To the wired infrastructure for a destination not in the ESS
- When DS of AP receives packet, it is sent to station in BSS

Hidden Mobility

- All mobile stations within ESS appear to outside networks as a single MAC-layer network where all stations are physically stationary
- Provides level of indirection to hide station mobility
- Allows existing network protocols (e.g., TCP/IP) to function properly within a WLAN where stations are mobile

802.11 Services

- Services divided into
  - Station services
    - Authentication
    - Deauthentication
    - Privacy
    - Data delivery
  - Distribution services
    - Association
    - Disassociation
    - Reassociation
    - Distribution
    - Integration

Station Services

- Authentication
  - Used to prove identity of one station to another
  - Station must be authenticated in order to access WLAN for data delivery
- Deauthentication
  - Used to remove previously authenticated station
  - Deauthenticated station cannot access WLAN for data delivery
- Privacy
  - Prevents message contents from being read by unintended recipient
  - Wired equivalency protocol (WEP)– designed to provide same level of protection as found on wired networks
  - Only protects data over wireless links, not end-to-end
- Data delivery
  - Provides reliable delivery of data from MAC of one station to MAC of other stations

Distribution Services

- Provide services to allow station mobility within ESS and allow connections to wired networks
- Association service
  - Makes logical connection between station and AP
  - Allows DS of AP to know where to deliver data to station
  - Allows AP to accept data from station
  - AP must allocate channel resources for station
  - Typically association only invoked when station first enters WLAN
- Reassociation service
  - Used when station moves to new BSS (new AP)
  - Allows new AP to contact old AP to get packets that may be buffered there for the station

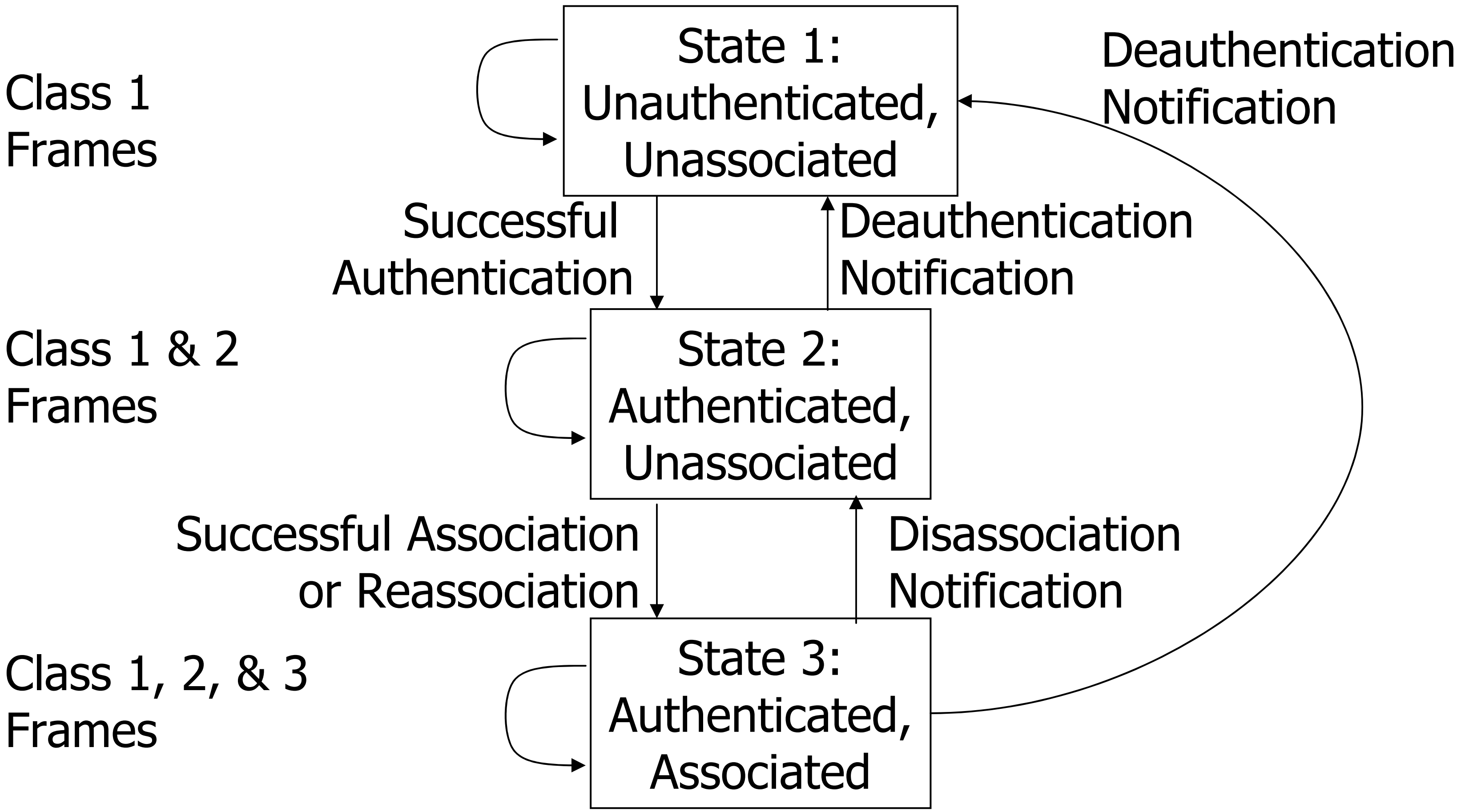
Distribution Services (cont.)

- Disassociation service
  - Station can use this service to inform AP that it no longer requires service from WLAN
    - 802.11 card being removed
    - Station shutting down
  - AP may force disassociation
    - Cannot support all stations currently associated
    - AP shutting down
  - Station must associate again to access WLAN after disassociation
- Distribution service
  - Determines where to send packets
    - Back to own BSS, to another AP, to wired network

Distribution Services (cont.)

- Integration service
  - Allows 802.11 WLAN to connect to other wireless and wired LANs
  - Translates 802.11 frames to formats for other networks
  - Translates frames in other formats to 802.11 format

States



Class 1
Frames
State 1:
Unauthenticated,
Unassociated
Deauthentication
Notification
Successful
Authentication
Deauthentication
Notification
Class 1 & 2
Frames
State 2:
Authenticated,
Unassociated
Successful Association
or Reassociation
Disassociation
Notification
Class 1, 2, & 3
Frames
State 3:
Authenticated,
Associated

Protocol Architecture

- Layers
  - Physical layer
  - Medium access control
  - Logical link control
- Functions of physical layer
  - Preamble generation/removal (for synchronization)
  - Digital modulation
  - Bit transmission/reception
  - Includes specification of the transmission medium

Protocol Architecture (cont.)

- Functions of medium access control (MAC) layer
  - To provide reliable data delivery
  - Control access to the WLAN transmission medium
    - Distributed coordination function (DCF)
    - Point coordination function (PCF)
  - Security using WEP
- Functions of logical link control (LLC) Layer:
  - Provide an interface to higher layers and perform flow and error control

Physical Media Defined by Original 802.11 Standard

- Direct-sequence spread spectrum
  - Operating in 2.4 GHz ISM band
  - Data rates of 1 and 2 Mbps
- Frequency-hopping spread spectrum
  - Operating in 2.4 GHz ISM band
  - Data rates of 1 and 2 Mbps
- Infrared
  - 1 and 2 Mbps
  - Wavelength between 850 and 950 nm

IEEE 802.11a and IEEE 802.11b PHY

- IEEE 802.11a
  - Makes use of 5-GHz band
  - Provides rates of 6, 9 , 12, 18, 24, 36, 48, 54 Mbps
  - Uses orthogonal frequency division multiplexing (OFDM)
  - Subcarrier modulated using BPSK, QPSK, 16-QAM or 64-QAM
- IEEE 802.11b
  - Provides data rates of 5.5 and 11 Mbps
  - Can fall back to 1 and 2 Mbps
    - Poor channel conditions
    - Interoperate with 802.11 equipment
  - Complementary code keying (CCK) modulation scheme

802.11 MAC

- More efficient to deal with errors at the MAC level than higher layer (such as TCP)
- DFWMAC protocol
  - Carrier sense multiple access with collision avoidance (CSMA/CA) with binary exponential backoff
- Physical carrier sense
  - Sense medium for certain time to ensure channel free
- Virtual carrier sense
  - In addition to physical carrier sense, stations keep a *network allocation vector* (NAV)
  - Determines when current transmission will end
  - Set by parameters in all packets that indicate tx length
  - Allows hidden nodes to backoff appropriately

802.11 MAC (cont.)

- Collision avoidance
  - Frame exchange protocol
    - Source station transmits data
    - Destination responds with acknowledgment (ACK)
    - If source does not receive ACK, it retransmits frame
  - Four frame exchange
    - Source issues request to send (RTS)
    - Destination responds with clear to send (CTS)
    - Source transmits data
    - Destination responds with ACK

Interframe Space (IFS) Values

- Short IFS (SIFS)
  - Shortest IFS
  - Used for immediate response actions
- Point coordination function IFS (PIFS)
  - Mid-length IFS
  - Used by centralized controller in PCF scheme when using polls
- Distributed coordination function IFS (DIFS)
  - Longest IFS
  - Used as minimum delay of asynchronous frames contending for access

IFS Usage

- SIFS
  - Clear to send (CTS)
  - Acknowledgment (ACK)
  - Poll response
- PIFS
  - Used by centralized controller in issuing polls
  - Takes precedence over normal contention traffic
- DIFS
  - Used for all ordinary asynchronous traffic

Distributed Coordination Function (DCF)

- When station wants to transmit a packet, MAC checks physical and virtual carrier sense
- If channel sensed idle for DIFS, MAC transmits frame
- If channel sensed busy during DIFS, MAC selects backoff interval
  - Counter decremented for each slot during which channel sensed idle
  - When counter reaches zero, MAC transmits frame
- If transmission not successful, assumed collision occurred
  - Contention window (CW) doubled
  - New backoff interval selected between 0 and CW
  - Backoff countdown begun again
- Process continues until packet successfully transmitted or dropped

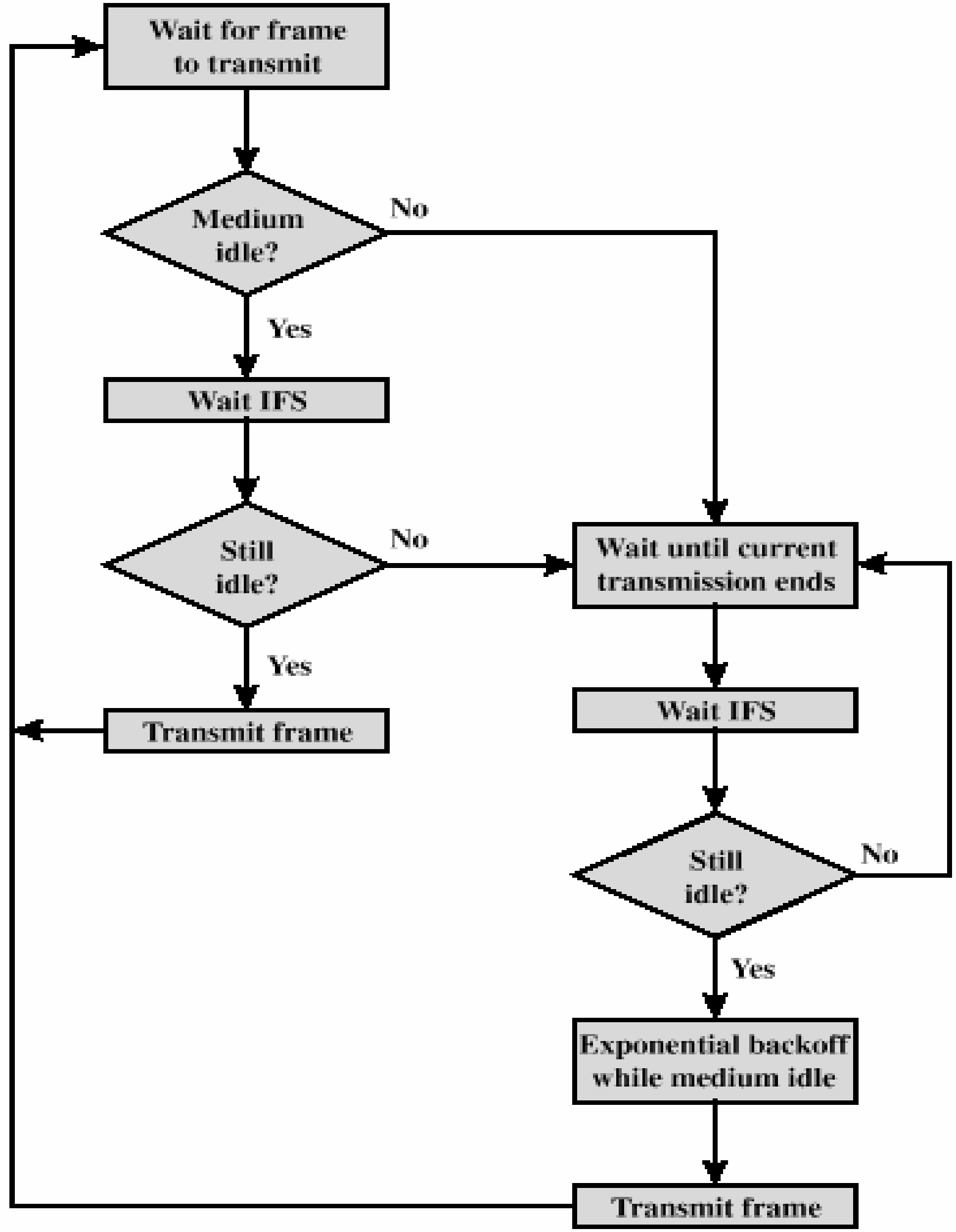
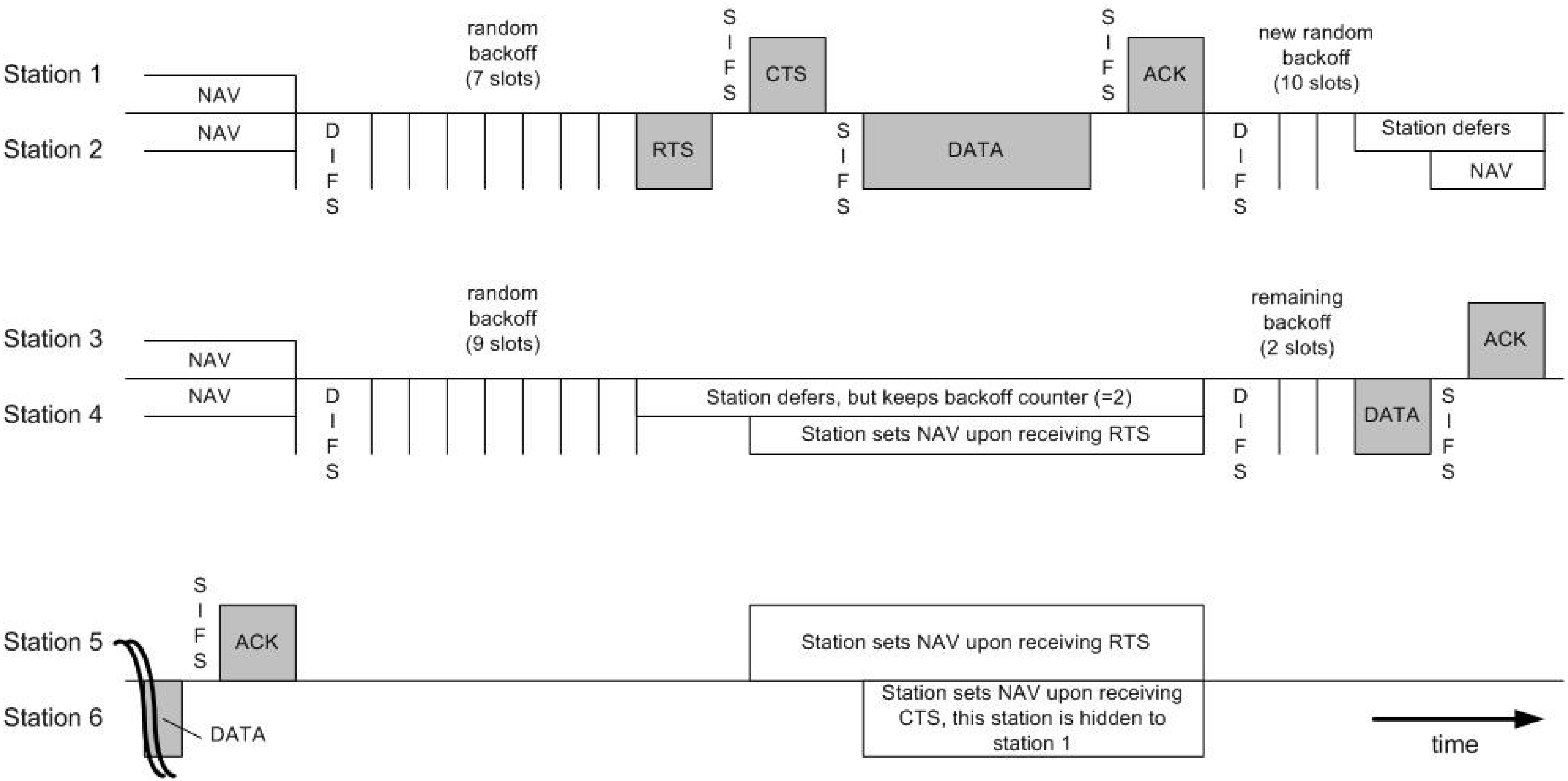


Figure 14.6 IEEE 802.11 Medium Access Control Logic

4-way Handshaking Protocol



Point Coordination Function

- Centrally controlled access
- Poll and response protocol run by point coordinator (PC) at AP
  - Removes contention
- Stations request that PC register them on polling list
- PC regularly polls stations on polling list and delivers traffic
- Both PCF and DCF operate simultaneously
- Time broken into *contention-free period* (CFP), *contention period* (CP)
  - During CFP, access to channel controlled by PC
  - During CP, DCF applies, stations compete for channel access
- PC gains access to medium during DCF period using a PIFS < DIFS time
  - PC transmits beacon to start CFP, contains CFP length for NAV
  - Once CFP started, PC transmits packets to stations and polls stations that requested contention-free service
  - During CFP, all spacing uses PIFS rather than DIFS to remain in CFP

Power Management in IBSS

- Functions
  - Entering low-power state
  - Communicating with stations in low-power state
- Entering low-power state
  - Transmitter and receiver turned off to save energy
  - Station must complete data frame handshake with any other station in IBSS with power management bit set in frame in order to enter low-power state
    - Station may use null frame type if no data to send
    - Otherwise, can piggyback power-save information on data packet
- Once in low-power state, station must wake up for periodic beacons
  - Traffic indications announced following beacon
  - If traffic announced for station, it must acknowledge announcement and remain awake until next traffic announcement to receive data

Power Management in IBSS (cont.)

- If a station A wants to send data to another station B, A must first try to determine if B is in power-save mode
  - If A thinks B is in power save mode, it must buffer the packet until the next traffic announcement window and send an announcement for B
  - B cannot send packet to A until it receives an ACK for the announcement
- Power-save algorithm puts greater burden on sending station than receiving station
  - Sending station must buffer packet and transmit one or more announcements in addition to data packet transmission
- Power versus latency tradeoff
- Stations cannot sleep long

Power Management in BSS

- Controlled by AP
- Stations can remain asleep much longer
  - AP buffers packets
  - Station not required to awaken for every beacon
- Station must inform AP when it enters power-save mode
- Station informs AP of maximum number of beacon periods it will be in power-save mode
  - AP must buffer frames for at least this period
  - Buffered frames indicated in traffic announcements following each beacon
  - When station acknowledges traffic announcement, AP sends buffered packets

Wired Equivalency Protocol

- WEP encrypts the data portion of each frame but not frame headers
  - Frames with no data not provided any protection
  - WEP protects contents of data, but eavesdroppers can determine other information from packets
- WEP uses RC4 encryption
  - Symmetric stream cipher that supports variable length key
  - Symmetric → same key used for encryption and decryption
  - Stream → can process an arbitrary number of bytes
  - Variable length key up to 256 bytes
    - Key generation and distribution not part of standard
    - Hard problem to solve

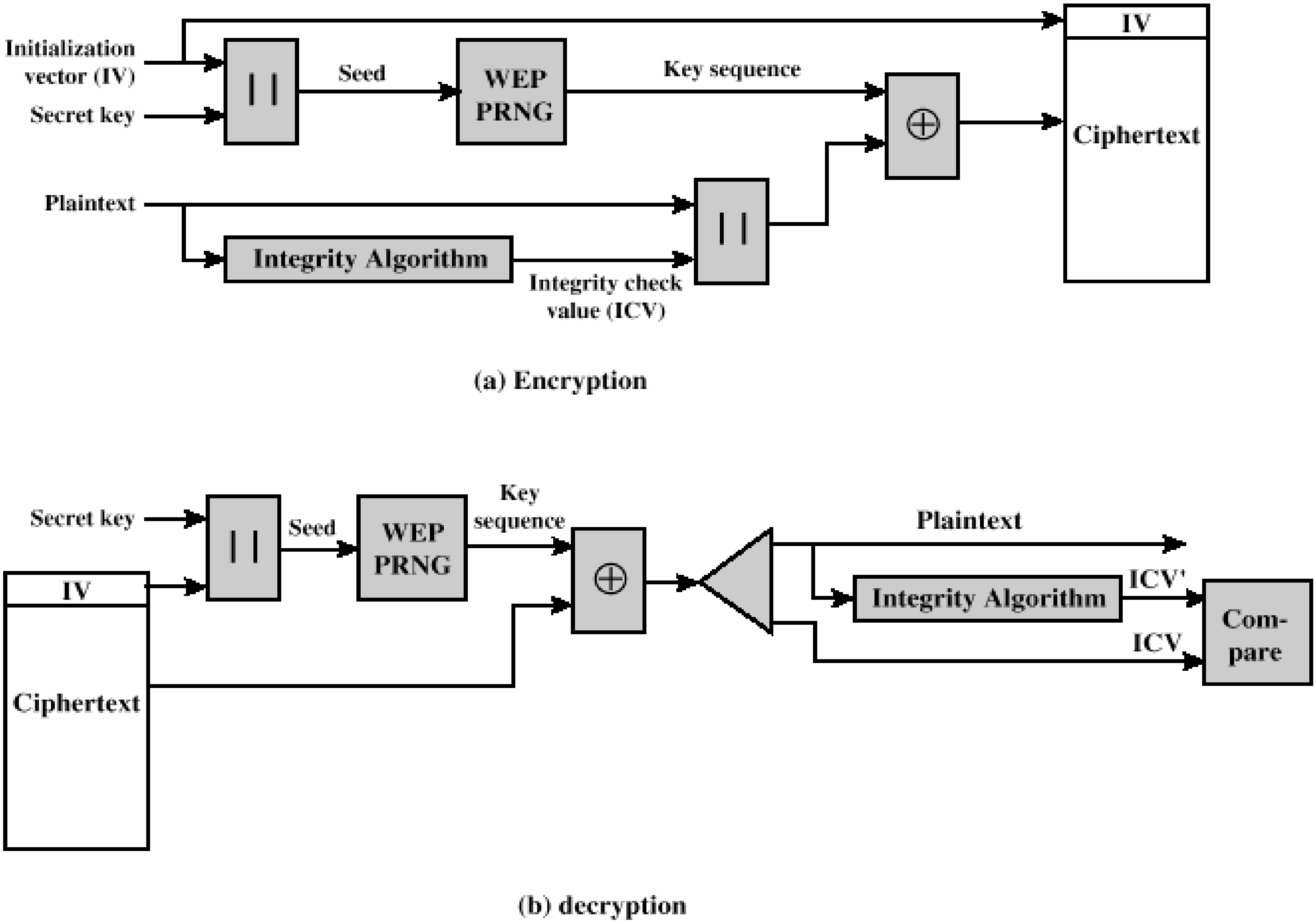


Figure 14.9 WEP Block Diagram

802.11x Protocols

- 802.11a
  - 5 GHz, 12 radio channels
  - Up to 54 Mbps (with achievable data rates up to about 27 Mbps)
  - Data rate decreases with increasing distance to AP
- 802.11b
  - 2.4 GHz, 3 radio channels
  - Up to 11 Mbps
  - Data rate decreases with increasing distance to AP
- 802.11d
  - Supplementary to the MAC of 802.11
  - Allows APs to exchange information on permissible radio channels and acceptable power levels
  - Allows 802.11 devices to operate in countries with different spectrum limitations from North America

802.11x Protocols (cont.)

- 802.11e
  - Supplementary to the MAC of 802.11
  - Provides QoS for voice and video applications
- 802.11f
  - "Recommended practice" document
  - Aim is to achieve interoperability of APs/stations from different vendors
- 802.11g
  - Dual-mode 2.4 GHz and 5 GHz operability
  - Up to 54 Mbps

802.11x Protocols (cont.)

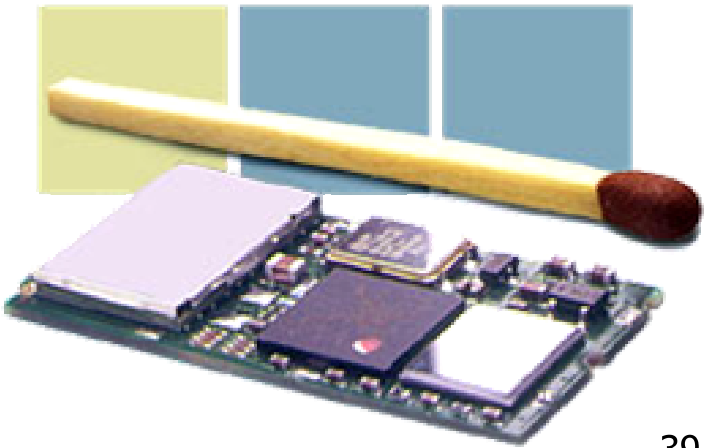
- 802.11h
  - Supplementary to the MAC of 802.11
  - Includes transmission power control and dynamic frequency selection to reduce interference and comply with European regulations in the 5 GHz band
- 802.11i
  - Supplementary to the MAC layer
  - Aim is to improve security

Personal Area Networks

- Networks that connect devices within a small range
  - Typically on the order of 10-100 meters
- Application areas
  - Data and voice access points
    - Real-time voice and data transmissions
  - Cable replacement
    - Eliminates need for numerous cable attachments
    - Hook your laptop to your PDA, headphones, mouse, keyboard, printer, camera, etc.
  - Ad hoc networking
    - Device with PAN radio can establish connection with another when in range

Bluetooth Standard

- Universal short-range wireless capability
- Bluetooth standardization began in 1998
- Sponsors
  - Initial: Ericsson, Nokia, IBM, Toshiba, and Intel
  - Expanded in 1999 to include 3 Com, Lucent, Microsoft, and Motorola
  - Thousands of companies are now adopters
- Goals of system design
  - Global operation
  - No fixed infrastructure required for network set-up or maintenance
  - Voice and data connections
  - Small, low power radio
  - Low cost: $5-$10 per node



Bluetooth Standard (cont.)

- Low power
  - 1 mW transmit power to get 10 m range
  - Can amplify signal to 100 mW transmit power to get 100 m range
  - 50-100 mW active power
  - Standby current < 0.3 mA → 3 months
  - Voice mode = 8-30 mA → 75 hours
  - Data mode averages 5 mA (20 kbps) → 120 hours
- Specifies the physical, link, and MAC layers of the protocol stack
- Applications built on top of Bluetooth using HCI—host controller interface
  - Specifies how to “talk” to Bluetooth device
  - Contains sets of commands for hardware
- Defined in a global band (2.45 GHz ISM band)
  - Bluetooth devices should work anywhere in the world (mostly)
  - Devices within 10 m can share up to 865 kbps of capacity

Bluetooth Standard (cont.)

- Network topology
  - Master-slave connection
  - Several slaves and a master form a piconet
  - Several piconets form a scatternet
- Frequency-hopped spread spectrum
  - Low cost, low power implementations possible
  - Better immunity to near-far problem than DSSS
  - Error correction schemes used to provide protection against interference on the same narrowband channel
- Radio Parameters
  - RF band: 2.4 GHz, ISM band
  - Modulation: BFSK
  - Peak data rate: 1 Mb/s
  - Number of hopping channels: 79
  - Carrier spacing: 1 MHz
  - Peak Tx power: $\leq$ 20 dBm

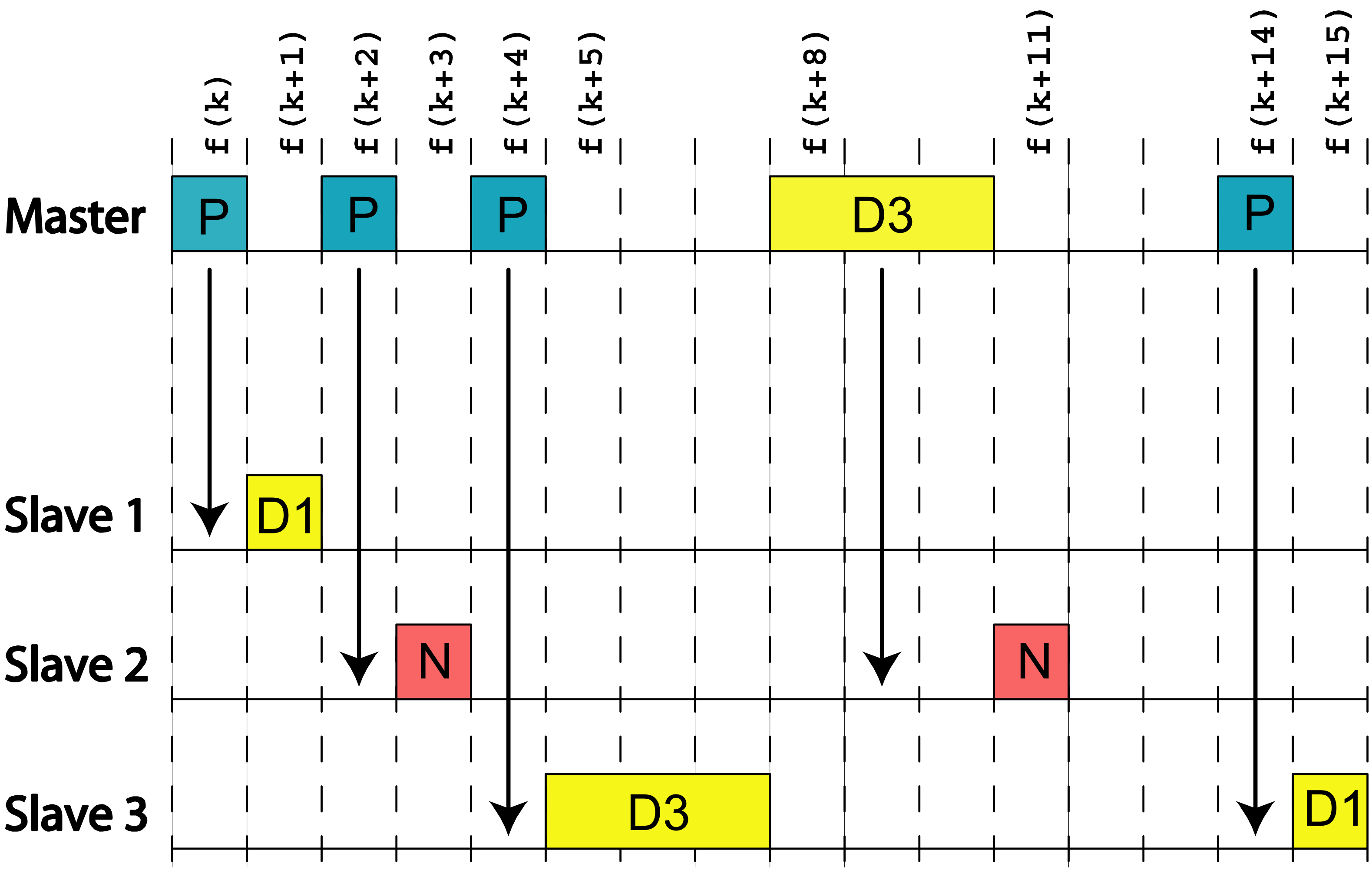
Network Architecture

- Piconets
  - Master and up to seven slave devices
  - Paging unit that established connection becomes piconet master by default
  - Slaves must synchronize to master
  - Master announces its clock and device ID to slaves
  - Master-slave switch
    - Slave can take on role of master if desired
  - Can only be one master per piconet
    - Hopping pattern determined by master's 48-bit Bluetooth Device Address
    - Phase in hopping pattern determined by master clock
    - Piconet access code determine by master ID

Bluetooth Channel

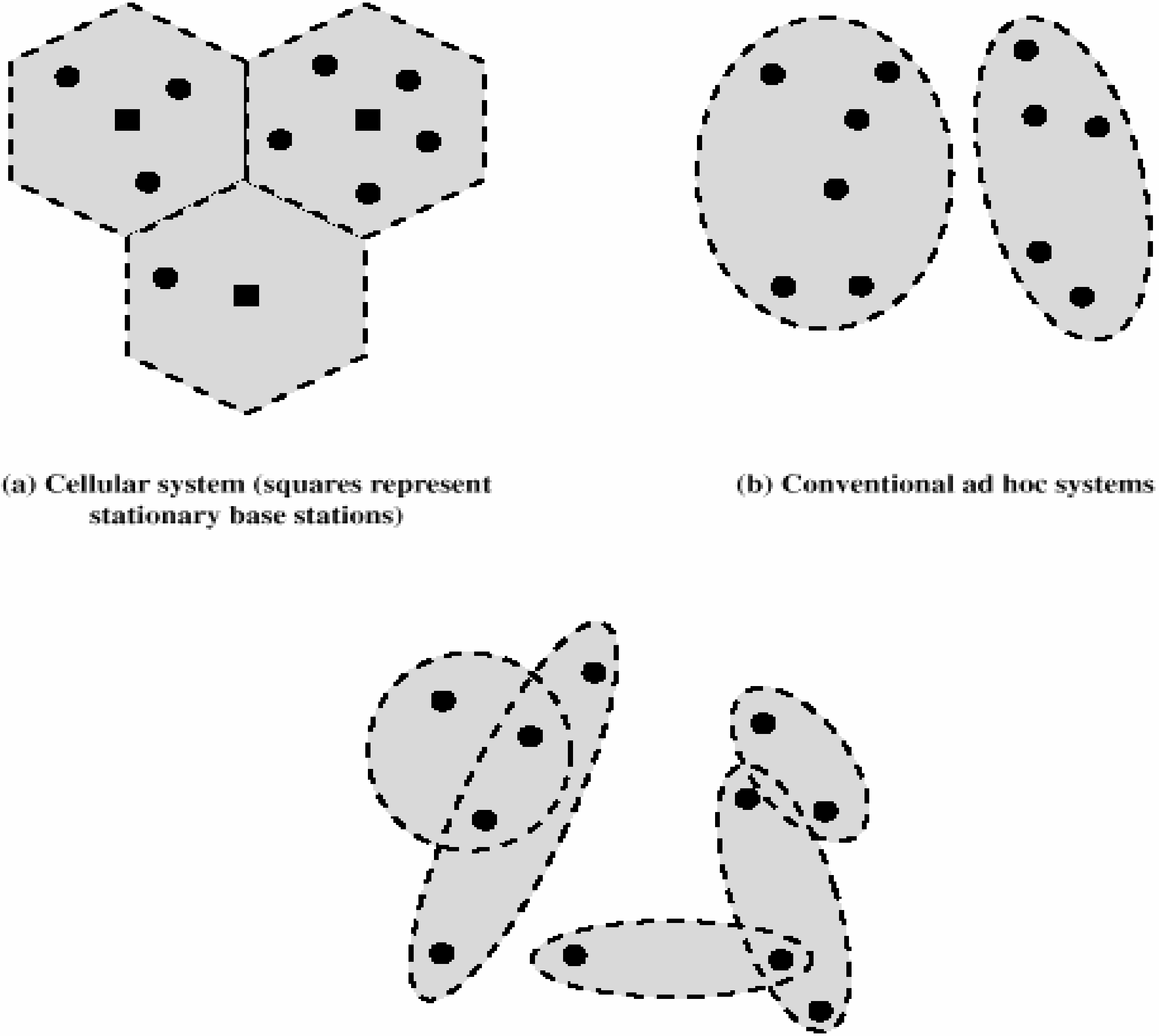
- 79 1 MHz channels
- Channel divided into 625 μs slots
- Hop occurs after each packet transmitted
- Packets can be 1, 3, or 5 slots in length
- 1600 hops / second
- Time division duplex
  - Transmit and receive in alternate time slots
  - Master-slave architecture
    - Master transmits in a slot
    - Slave transmits in following slot
- Master schedules all traffic
  - Master must poll slaves explicitly or implicitly by sending a master-to-slave data/control packet
  - Master can dynamically adjust scheduling algorithm
  - Scheduling algorithm not specified in Bluetooth standard

Bluetooth Polling



Scatternets

- Slaves within a piconet share 1 MHz bandwidth
- Piconets can co-exist by hopping independently
  - Each piconet can access 1 MHz bandwidth
  - Increase capacity compared with all nodes sharing 1 MHz channel
- Scatternets share 79 MHz bandwidth among different piconets
- Data from a nearby piconet not received by nodes in another piconet
- Nodes can belong to multiple piconets
  - Time division multiplexing
  - Can be a slave in two different piconets
  - Can be a master in one piconet and a slave in another piconet
  - Currently no standard for synchronization between different piconets
    - Inefficient use of resources
    - Can cause connections to be dropped



(a) Cellular system (squares represent stationary base stations)

(b) Conventional ad hoc systems

(c) Scatternets

Figure 15.5 Wireless Network Configurations

Bluetooth Power Saving

- Receiver can determine quickly if continued reception required or not
  - Correlate incoming packet with piconet access code
    - If code does not correlate (takes 100 μs), node can return to sleep for duration of receive slot as well as for transmit slot if node not a master
      - No packet sent
      - Packet corrupted by noise and not worth receiving
  - If code does correlate, node can decode slave address
      - If slave address matches, node continues receiving
      - Otherwise, packet not for node and can go to sleep for receive and transmit slots

Low Power States

- Devices connected but not participating
- Hold mode
  - If no communication needed for some time, master can put slave in HOLD mode
  - Hold allows slave to
    - Go to sleep
    - Switch to another piconet
    - Perform scanning, inquiry or paging
  - After Hold expires, slave returns immediately to channel (synchronization remains during Hold period)

Low Power States (cont.)

- Park mode
  - Low duty-cycle mode → low power
  - Slave wakes up occasionally to resynchronize with master and check for broadcast messages
  - Master establishes beacon channel
    - Enables parked slaves to remain synchronized to piconet
    - Allows master to communicate with slaves
  - Slave cannot communicate until unparked
- Sniff mode
  - Similar to Hold mode
  - Slave can skip some receive slots to save power
  - Master and slave agree on which slots slave will listen to channel