CS 4453 Computer Networks

Chapter 5 Wireless and Mobile Networks

2015 Winter

A wireless network communication takes place over a wireless channel (which is usually a radio channel, or sometimes an infrared channel). The challenges for wireless networks are quite different from that of wired networks, especially at the data link layer and the network layer. Mobile networks require more interesting techniques.

5.1 Cellular networks

Originally, cellular networks provided only voice communications services and they could also be used to send and receive short text messages. Today, the range of application is much wider, including data communications, Internet access, multimedia applications (video telephony), and mobile payment services, etc.

Cellular networks are infrastructure-based networks. The infrastructure consists of base stations and a wired backbone network that connects the base stations together, as well as to the wired telephone system and to the Internet.

Each base station serves only a limited physical area, called a cell.

All the base stations of a given network operator together can cover a large area.

In cellular networks, the only wireless part in the system is the link between the mobile phone and the base station. The rest is wired network.

Base stations are connected to the mobile switching center (MSC) which is connected to the public switched telephone network (PSTN).

The frequency spectrum allocated to wireless communications is very limited.

Each cell is assigned a certain number of channels. To avoid radio interference, the channels assigned to one cell must be different from the channels assigned to its neighboring cells. However, the same channels can be reused by two cells that are far apart.

GSM

Global System for Mobile Communications (GMS) is a European initiated standard which is a prominent example of cellular network.

The cellular technologies are often classified to one of several "generations". The earliest generations were designed primarily for voice traffic. First generation (1G) systems were analog FDMA systems designed exclusively for voice-only communication. These 1G systems are almost extinct now, having been replaces by digital 2G systems.

The original 2G systems were also designed for voice, but later extended to support data as well as voice service.

The 3G systems that currently are deployed also support voice and data, but with an ever increasing emphasis on data capabilities and higher-speed radio access links.

2G Cellular network

In GSM, each cell contains a base transceiver station (BTS) that transmits signals to and receivers signals from the mobile station in its cell.

The coverage area of a cell depends on many factors, such as the transmitting power of BTS, the transmitting power of the user devices, obstructing buildings in the cell, and the height of base station antennas.

Originally, each cell contains one base station residing in the center of the cell, many systems today place the BTS at corners where three cells intersect, so that a single BTS with directional antennas can service three cells.

2G cellular systems uses combined FDM/TDM for the air interface.

With pure FDM, the channel is partitioned into a number of frequency bands with each band devoted to a call. With pure TDM, time is partitioned into frames with each frame further partitioned into slots and each call being assigned the use of a particular slot in the revolving frame.

In combined FDM/TDM system, the channel is partitioned into a number of frequency sub-band, and within each sub-band, time is partitioned into frames and slots. Therefore in a combined FDM/TDM system, if the channel is partitioned into F sub-banes and time is partitioned into T slots, then the channel will be able to support $F \cdot T$ simultaneous calls.

GSM systems consist of 200-kHz frequency banks with each band supporting eight TDM calls. GSM encodes speech at 13 kbps and 12.2kbps.

A GSM network's base station controller (BSC) will typically service several tens of base transceiver stations. The role of the BSC is to allocate BTS radio channels to mobile subscribers, perform paging (finding the cell in which a mobile user in resident), and perform handoff (change base station during a call) of mobile users.

The base station controller and its controlled base transceiver stations collectively constitute a GSM base station system (BSS).

The mobile switching center (MSC) is for user authorization and accounting, call establishment and teardown, and handoff. A single MSC will typically contain up to five BSCs resulting in approximately 200K subscribers per MSC.

A cellular provider's network will have a number of MSCs, with special MSCs know as gateway MSCs connecting the provider's cellular network to the larger public telephone network.

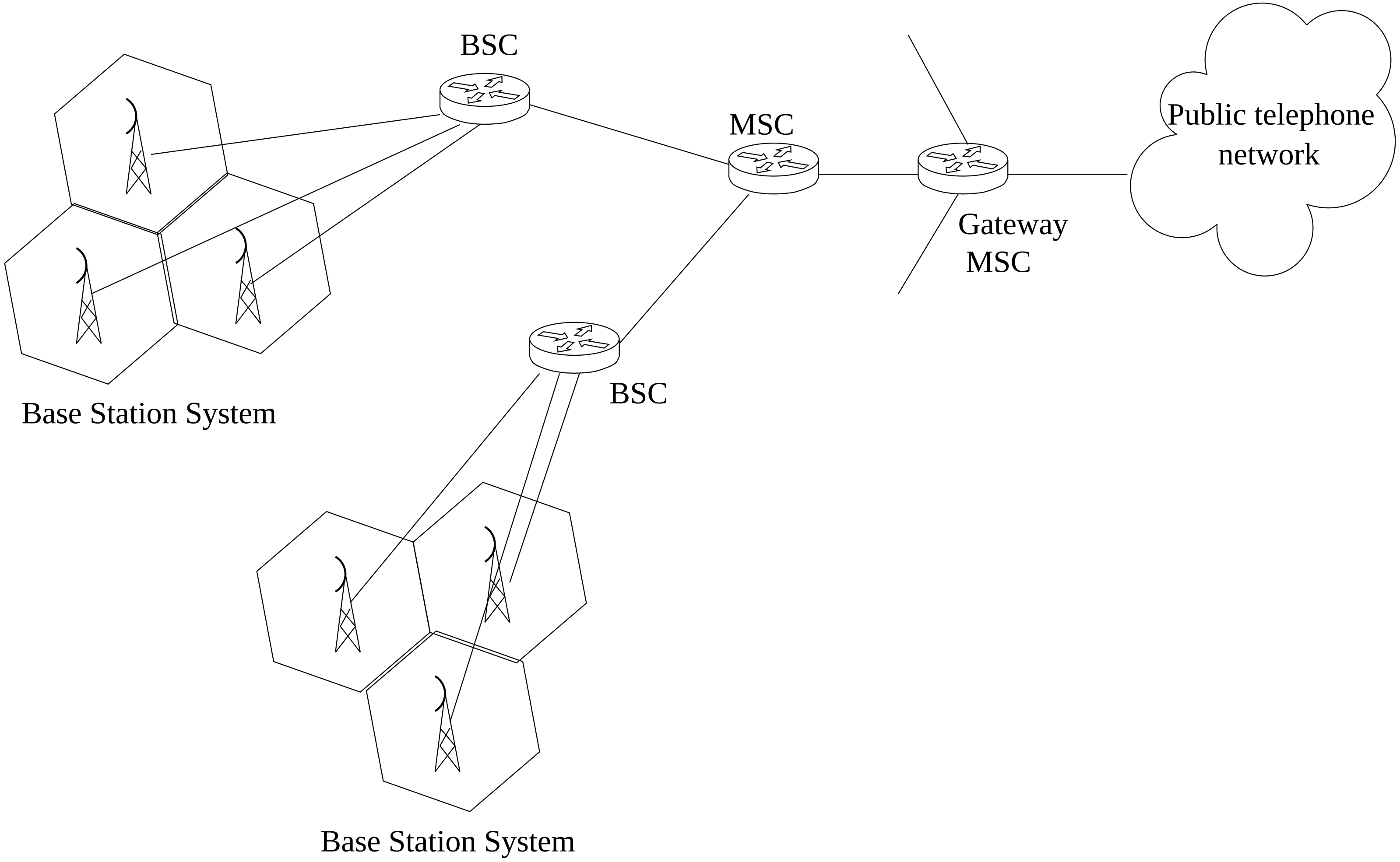


Figure 1: GSM 2G network

3G Cellular network

When we want to use smart phones to communicate with data and access the internet, we need to run a full TCP/IP protocol stack and connect into internet via the cellular data network.

In what follows, we will focus on the UMTS (Universal Mobile Telecommunication Service) 3G standards developed by the 3rd Generation Partnership project (3GPP), a widely deployed 3G technology.

The 3G core cellular data network connects radio access network to the public Internet. The basic idea of the designers of 3G data service is: leave the existing core GSM cellular voice network untouched, adding additional cellular data functionality in parallel to the existing cellular voice network.

There are two types of nodes in the 3G core network: Serving GPRS Support Nodes (SGSNs) and Gateway GPRS Support Nodes (GGSNs).

Here GPRS stands for Generalized Packet Radio Service, an early cellular data service in 2G networks.

An SGSN is responsible for delivering datagrams to/from the mobile nodes in the radio access network to which the SGSN is attached. The SGSN interacts with the cellular voice network's MSC for that area, providing user authorization and handoff, maintaining location information about active mobile nodes, and performing datagram forwarding between mobile nodes in the radio access network and a GGSN.

The GGSN acts as a gateway, connecting multiple SGSNs into the larger Internet. A GGSN is thus the last piece of 3G infrastructure that a datagram originating at a mobile node encounters before entering the larger Internet.

To the outside world, the GGSN looks like any other gateway router. The mobility of the 3G nodes within the GGSN's network is hidden from the outside world behind the GGSN.

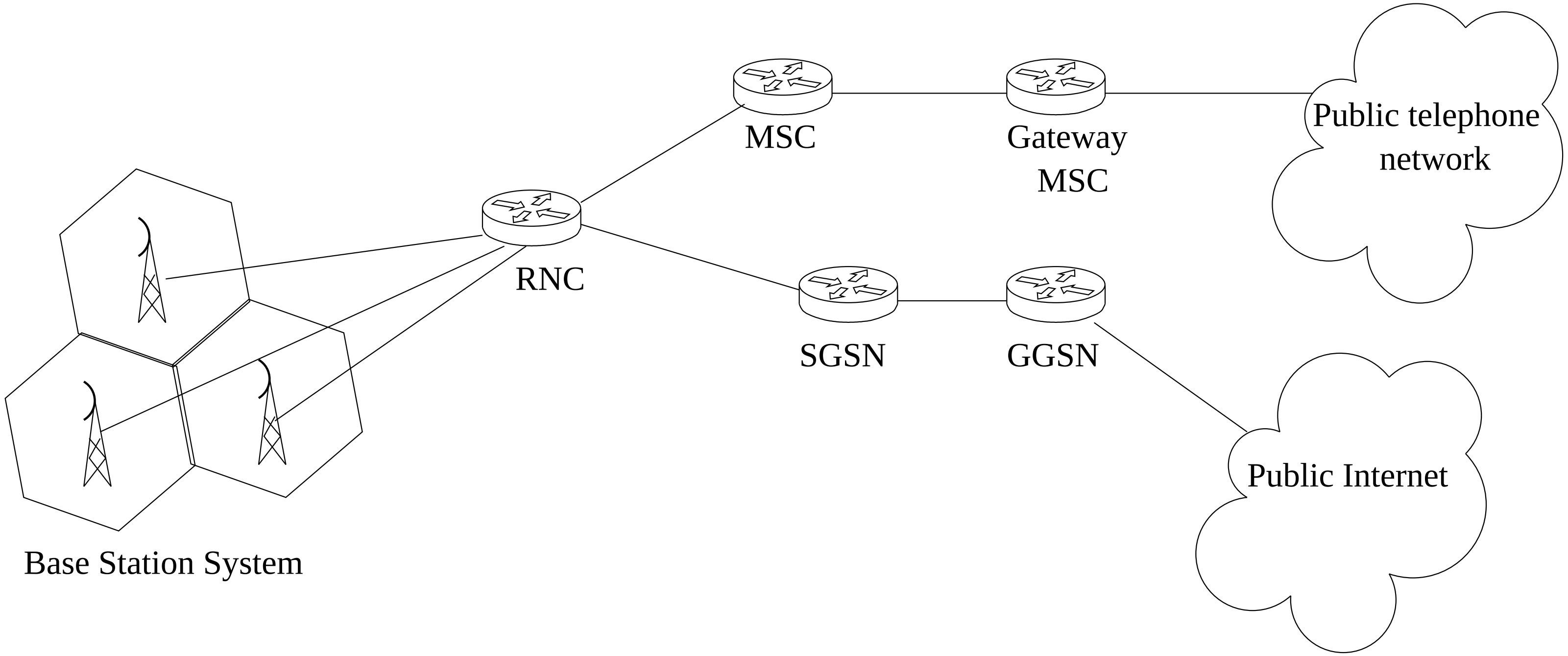


Figure 2: GSM 3G network

Figure 2 gives a simple example of GSM 3G cellular network architecture. The 3G radio access network is the wireless first-hop network that we see as a 3G user.

The Radio Network Controller (RNC) typically controls several cell base transceiver stations similar to the base stations in 2G system. Each cell's wireless link operates between the mobile nodes and a base transceiver station.

The RNC connects to both the circuit-switched cellular voice network via an MSC, and to the packet-switched Internet via an SGSN.

A significant change in 3G UMTS over 2G networks is that UMTS uses a CDMA (Direct Sequence Wideband CDMA, DS-WCDMA) technique within TDMA slots rather than the FDMA/TDMA scheme.

On the other hand, the TDMA slots are available on multiple frequencies. So this is an interesting applications combining of 3 multiplexing techniques.

This change requires a new 3G cellular wireless-access network operating in parallel with the 2G BSS radio network. The data service associated with the WCDMA specification is known as HSP (High Speed Packet Access) and promises downlink data rates of up to 14 Mbps.

4G: LTE and WiMAX

Two 4G candidate systems are commercially deployed: the Mobile WiMAX (Worldwide Interoperability for Microwave Access) standard (first used in South Korea in 2007), and the first-release Long Term Evolution (LTE) standard (in Oslo, Norway and Stockholm, Sweden since 2009).

In the United States, Sprint (previously Clearwire) has deployed Mobile WiMAX networks since 2008, while MetroPCS became the first operator to offer LTE service in 2010.

USB wireless modems were among the first devices able to access these networks, with WiMAX smartphones becoming available during 2010, and LTE smartphones arriving in 2011. 3G and 4G equipment made for other continents are not always compatible, because of different frequency bands. Mobile WiMAX is currently (April 2012) not available for the European market.

In March 2008, the International Telecommunications Union-Radio communications sector (ITU-R) specified a set of requirements for 4G standards, named the International Mobile Telecommunications Advanced (IMT-Advanced) specification, setting peak speed requirements for 4G service at 100 megabits per second (Mbps) for high mobility communication (such as from trains and cars) and 1 gigabit per second (Gbps) for low mobility communication (such as pedestrians and stationary users).

Mobile WiMAX Release 2 (also known as WirelessMAN-Advanced or IEEE 802.16m') and LTE Advanced (LTE-A) are IMT-Advanced compliant backwards compatible versions of the above two systems, standardized during the spring 2011 and promising speeds in the order of 1 Gbps.

As opposed to earlier generations, a 4G system does not support traditional circuit-switched telephony service, but all-Internet Protocol (IP) based communication such as IP telephony.

The spread spectrum radio technology used in 3G systems, is abandoned in all 4G candidate systems and replaced by OFDMA multi-carrier transmission and other frequency-domain equalization (FDE) schemes, making it possible to transfer very high bit rates despite extensive multi-path radio propagation (echoes).

The peak bit rate is further improved by smart antenna arrays for multiple-input multiple-output (MIMO) communications.

LTE has two important innovations over 3G systems.

- Evolved Packet Core (EPC): This is a simplified all-IP core network that unifies the separate circuit-switched cellular voice network and the packet-switched cellular data network. The EPC allows multiple types of radio access networks, including legacy 2G and 3G radio access networks, to attach to the core network.

- LTE Radio Access Network: LTE uses a combination of frequency division multiplexing and time division multiplexing on the downstream channel, know as orthogonal frequency division multiplexing (OFDM).

  In LTE, each active mobile node is allocated one or more 0.5 ms time slots in one or more of the channel frequencies. By being allocated increasingly more time slots, a mobile node is able to achieve increasingly higher transmission rates. Slot reallocation among nodes can be performed as often as once every millisecond.

  Another inovation in the LTE radio network is the use of multiple-input, multiple-output (MIMO) antennas.

WiMAX refers to interoperable implementations of the IEEE 802.16 family of wireless-networks standards ratified by the WiMAX Forum.

The original IEEE 802.16 standard (now called ”Fixed WiMAX”) was published in 2001. WiMAX adopted some of its technology from WiBro, a service marketed in Korea. The term fixed arises because the technology does not provide for handoff among access points.

Mobile WiMAX (originally based on 802.16e-2005) is the revision that was deployed in many countries, and is the basis for future revisions such as 802.16m-2011. The technology of the Mobile WiMAX offers handoff among access points, which means the system can be used with portable devices such as laptop computers and cell phones.

Some key features of WiMAX can briefly summarized as follows:

- Uses licensed spectrum (i.e., offed by carriers).
- Each cell can cover a radius of 3 to 10 km.
- Uses scalable orthogonal FDM.
- Guarantees quality of services (for voice or vidio).
- Can transport 70 Mbps in each direction at short distances.
- Provides 10 Mbps over a long distance (10 km)

5.2 Wireless LANs: WiFi

Although many technologies and standards for wireless LAN were developed, the most common and important standard is the IEEE 802.11 wireless LAN, also known as WiFi. There are several 802.11 standards for wireless LAN technologies, including 802.11.b, 802.11.a and 802.11.g. The main characteristics of these standards are as follows:

Standard	Frequency Range (United States)	Data Rates
802.11a	5.1-5.8 GHz	up to 54 Mbps
802.11b	2.4-2.485 GHz	up to 11Mbnps
802.11g	2.4-2.485 GHz	up to 54 Mbps

A number of dual-mode (802.11a/b) and tri-mode (802.11a/b/g) devices are also available. The three standards share many characteristics. Some of these characteristics are:

- They all use the same medium access protocol CSMA/CA.
- They all use the same frame structure for their link-layer frames.
- They have the ability to reduce their transmission rate in order to reach out over greater distances.
- All of them allow for both "infrastructure mode" and "ad hoc" mode.

The 802.11b and 802.11g wireless LANs operate in the unlicensed frequency band of 2.4 - 2.485 GHz, competing for frequency spectrum with 2.4 GHz phones and microwave ovens. 802.11a wireless LANs can run at significantly higher rates, but do so at higher frequencies. Due to the higher frequency, 802.11a LANs have a shorter transmission distance for a given power level and suffer more from multipath propagation.

A relatively new WiFi standard 802.11n uses multiple input multiple output (MIMO) antennas that are transmitting/receiving different signals. Depending on the modulation scheme used, transmission rates of several hundred megabits per second are possible with 802.11n.

The 802.11 architecture

The basic building block of the 802.11 architecture is the basic service set (BSS). A BSS contains one or more wireless stations and a central base station, know as an access point (AP). The AP in each BSS connects to an interconnection device such as a router, which in turn leads to the Internet. In a typical home network, there is one AP and one router (typically integrated together as on unit) that connects the BSS to the Internet.

Each 802.11 wireless station has a 6-bite MAC address that is stored in the firmware of the station's adapter (network interface card). Each AP also has a MAC address for its wireless interface. As with Ethernet, there MAC addresses are administered by IEEE and are globally unique.

Wireless LANs that deploy APs are often refereed to as infrastructure wireless LANs, with the infrastructure being the APs along with the wired Ethernet infrastructure that interconnects the APs and a router.

IEEE 802.11 stations can also group themselves together to form an ad hoc network, a network with no central control and with no connections to the “out side” world.

Channels and association

In 802.11, each wireless station needs to associate with an AP before it can send or receive network layer data.

When a network administrator installs an AP, the administrator assigns a one or two-word Service Set Identifier (SSID) to the access point. The administrator must also assign a channel number to the AP.

Recall that 802.11 operates in the frequency range of 2.4-2.485 GHz. Within this 85 MHz band, 802.11 defines 11 partially overlapping channels. Any two channels are non-overlapping if an only i they are separated by four or more channels.

In particular, the set of channels 1, 6 and 11 is the only set of three non-overlapping channels. This means that an administrator could create a wireless LAN with an aggregate maximum transmission rate of 33 Mbps by installing three 802.11b APs at the same physical location, assigning channels 1, 6, and 11 to APs, and interconnecting each of the APs with a switch.

The 802.11 standard requires that an AP periodically send beacon frames, , each of which includes the AP's SSID and MAC address.

The wireless station (laptop computer, for example), knowing that AP's are sending out beacon frames, scans the 11 channels, seeking beacon frames from any AP's that may be out there. Having learned about available AP's from the beacon frames, the wireless station selects one of the AP's for association.

The process of scanning channels and listening for beacon frames is known as passive scanning.

A wireless host can also perform active scanning, by broadcasting a probe frame that will be received by all APs within the wireless host's range. APs respond to the probe request frame with a probe response frame. The wireless host can then choose the AP with which to associate from among the responding APs.

After selecting the AP with which to associate, the wireless host sends an association request frame to the AP, and the AP responds with an association response frame. Once associated with an AP, the host will want to join the subnet to which the AP belongs.

Thus the host will typically send a DHCP discovery message into the subnet via the AP in order to obtain an IP address on the subnet. Once the address is obtained, the rest of the Internet views that host simply as another host with an IP address in that subnet.

In order to create an association with a particular AP, the wireless station may be required to authenticate itself to the AP. 802.11 wireless LANs provide several alternatives for authentication and access. One approach, used by many companies, is to permit access to a wireless network based on a station's MAC address. A second approach, employs usernames and passwords. In both cases, the AP communicates with an authentication server, relaying information between the wireless end-point station and the authentication server using a protocol such as RADIUS (RFC 2865) or DIAMETER (RFC 3588).

Separating the authentication server from the AP allows one authentication server to serve many APs, centralizing the decisions of authentication and access within the single server, and keeping AP costs and complexity low.

The 802.11 MAC protocol

Once a wireless station is associated with an AP, it can start sending and receiving data frames to and from the access point.

Since multiple stations may want to transmit data frames at the same time over the same channel, some multiple access protocol is needed to coordinate the transmissions. The designers of 802.11 chose a random access protocol for 802.11 wireless LANs. This access protocol is referred to as CSMA with collision avoidance, or CSMA/CA.

CSMA stands for “carrier sense multiple access”, meaning that each station senses the channel before transmitting, and refrains from transmitting when the channel is sensed busy. Instead of using collision detection (CSMA/CD) in Ethernet, 802.11 uses collision-avoidance technique.

Because of the relatively high bit error rates of wireless channels, 802.11 uses a link-layer acknowledgment/retransisssin (ARQ) scheme.

The link-layer acknowledgment scheme is as follows. When a station in a wireless LAN sends a frame, the frame may not reach the destination station intact a variety of reasons. To deal with this problem, the 802.11 MAC protocol applies link-layer acknowledgments.

When the destination station receives a frame that passes the CRC, it waits a short period of time known as the Short Inter-fram Spacing (SIFS) and then sends back an acknowledgment frame. If the transmitting station does not receive an acknowledgment within a given amount of time, it assumes that an error has occurred and retransmits the frame, using the CSMA/CA protocol to access the channel. If an acknowledgment is not received after some fixed number of retransmissions, the transmitting station gives up and discards the frame.

The outline for CSMA/CA protocol is as follows. Suppose that a station (wireless station or an AP) has a frame to transmit.

1. If initially the station senses the channel idle, it transmits its frame after a short period of time know as the Distributed Inter-frame Space (DIFS).
2. Otherwise, the station chooses a random backoff value using binary exponential backoff (some method to decide the value) and counts down this value when the channel is sensed idle. While the channel is sensed busy, the counter value remains frozen.

3. When the counter reaches zero (note that this can only occur while the channel is sensed idle), the station transmits the entire frame and then waits for an acknowledgment.

4. If an acknowledgment is received, the transmitting station knows that its frame has been correctly received at the destination station. If the station has another frame to send, it begins the CSMA/CA at step 2. If the acknowledgment is not received, the transmitting station reenters the backoff phase in step 2, with the random value chosen from a larger interval.

CSMA/CA uses SIFS and random backoff value to hold off the transmission for a short time. The reason is as follows.

In the case of wireless LAN, when a station transmits a frame, it does not detect collision. There are some reasons for that. To detect collision, the station requires the ability to send and receive at the same time, which will cost the adapter hardware a lot in the case of wireless. Moreover, in some situation, the station will not be able to detect a collision because of the hidden terminal problem (there are some physical obstacle between two transmitting stations, or it is caused by the fading of the signal strength). Therefore, if two stations find that the channel is in idle and start to transmit, then a collision occur. But if two stations choose different random value of backoff, then the collision can be avoided.

RTS and CTS

Considering the example of hidden terminal in Figure 3.

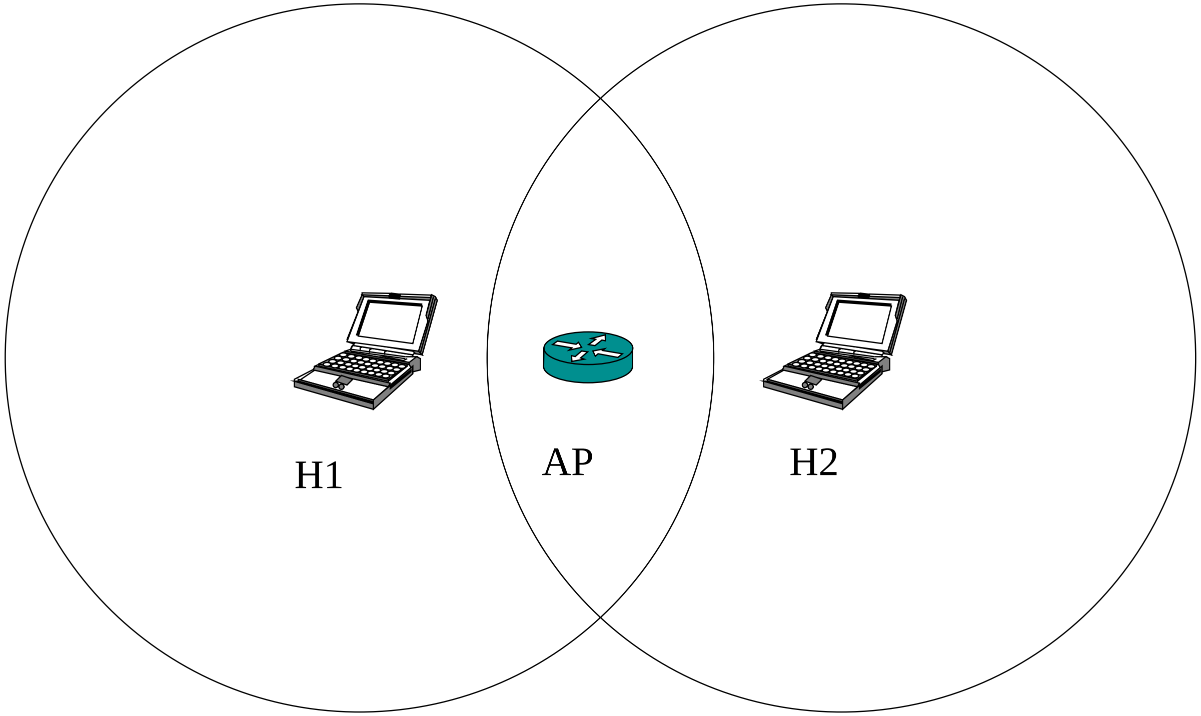


Figure 3: Hidden terminal example

In this example, due to the fading, the signal from H1 cannot reach H2 and the signal from H2 cannot reach H1. So each of the wireless stations is hidden from the other, but neither is hidden from the AP.

Suppose station H1 is transmitting a frame and halfway through H1's transmission, station H2 wants to send a frame to the AP. H2 first wait a DIFS interval and then transmit the frame, resulting a collision (H1 has not finished the transmission). The channel will therefore be wasted during the entire period of H1's transmission as well as during the H2's transmission.

IEEE 802.11 protocol allows a station to use a short Request to Send (RTS) control frame and a short Clear to Send (CTS) control frame to reserve access to the channel.

When a sender wants to send a data frame, it can first sent an RTS to the AP, indicating the total time required to send the data frame and the acknowledgment (ACK) frame.

When the AP receives the RTS frame, it responds by broadcasting a CTS frame. This CTS frame servers two purpose: it gives the sender explicit permission to send and also instructs the other stations not send for the reserved duration.

The use of RTS and CTS can improve the performance because:

- The hidden station problem is mitigated, since a long data frame is transmitted only after the channel has been reserved.
- Because the RTS and CTS frames are short, a collision involving an RTS or CTS frame will last only for the duration of the short RTS or CTS frame. Once the RTS and CTS frames are correctly transmitted, the following data and ACK frames should be transmitted without collisions.

Although the RTS/CTS exchange can help reduce collisions, it also introduces delay and consumes channel resources. For this reason, the RTS/CTS exchange is only used when the frame is long.

In practice, each wireless station can set an RTS threshold such that the RTS/CTS sequence is used only when the frame is longer than the threshold.

The IEEE 802.11 frame

The format of IEEE 802.11 frame is shown as follows:

2	2	6	6	6	2	6	0-2312	4
frame control	duration	addr 1	addr 2	addr 3	seq control	addr 4	payload	CRC

The numbers above each of the fields in the frame represented the lengths of the field in bytes. The fields are as follows:

- Payload: typically consists of an IP datagram of an ARP packet. Usually it is fewer than 1,500 bytes, although this field can be as long as 2,312 bytes.
- CRC: a 32-bit cyclic redundancy checksum.

- Address field: it has four address fields, each of which can hold a 6-byte MAC address. Three address fields are needed for internetworking purpose-specifically, for moving the network-layer datagram from a wireless station through an AP to a router interface. The fourth address field is used when APs forward frames to each other in ad hoc mode. The first three address fields are defined as follows:
  - Address 2 is the MAC address of the station that transmits the frame. If a wireless station transmits the frame, that station's MAC address is inserted in the address 2 field. Similarly, if an AP transmits the frame, the AP's MAC address is inserted to the address 2 field.

- Address 1 is the MAC address of the wireless station that is to receive the frame. For example, if a mobile wireless station transmits the frame, address 1 contains the MAC address of the destination AP.
- To understand address3, recall that the BSS is part of a subnet, and that this subnet connects to other subnets via some router interface. Address 3 contains the MAC address of this router interface.

- Sequence control: whenever a station correctly receives a frame from another station, it sends back an acknowledgment. If the ACK frame get lost, the sending station may send multiple copies of a given frame. The use of sequence numbers allows the receiver to distinguish between a newly transmitted frame and the retreansmission of a previous frame.
- Duration: 802.11 allows a transmitting station to reserve the channel for a period of time that includes the time to transmit its data frame and the time to transmit an acknowledgment. This duration value is included in this field.

- Frame control: This field includes many subfields including: Protocol version, Type, Subtype, To AP, From AP, More fragment, Retry, Power mgt, More data, WEP, Reserved. The type and subtype fields are used to distinguish the association, RTS, CTS, ACK, and data frame. The to and from fields are used to define the meanings of different address fields. WEP field indicates whether encryption is used.

Gigabit WiFi

Since the speed of Ethernet standard has extended in the gigabit per second range, the speed of WiFi is also requested to extend. IEEE 802.11 has introduced two new standards for that purpose.

- IEEE 802.11ac
- IEEE 802.11ad

IEEE 802.11ac operates in the 5 GHz band, same as 802.11a and 802.11n. The new standard achieves much higher data rates than 802.11n by means of enhancements in three areas:

- Bandwidth: The maximum bandwidth of 802.11n is 40MHz, but the maximum bandwidth of 802.11ac is 160 MHz.
- Signal encoding: 802.11n uses 64 QAM with OFDM, and 802.11ac uses 256 QAM with OFDM. (Quadrature Amplitude Modulation is a popular analog signaling technique). Thus more bits are encoded per symbol. Both schemes use forward error correction with a code rate of 5/6 (ratio of data bits to total bits).
- MIMO: With 802.11n, there can be a maximum of 4 channel input and 4 channel output antennas. 802.11 ac increases this to 8×8.

802.11ac includes the option of multiuser MIMO (MU-MIMO). This means that on the downlink, the transmitter is able to use its antenna resources to transmit multiple frames to different stations, all at the same time and over the same simultaneously spectrum. This enables the AP to deliver significantly more data in many environments.

IEEE 802.11ad is a version of 802.11 operating in the 60 GHz frequency band. This band offers the potential for much wider channel bandwidth than the 5 GHz band, enabling high data rates with relatively simple signal encoding and antenna characteristics. Few devices operate in the 60 GHz band, which means communications would experience less interference that in the other bands used by 802.11.

However, at 60 GHz, 802.11ad is operating in the millimeter range, which has some undesirable propagation characteristics:

- Since free space loss increases with the square of the frequency, losses are much higher in this range.
- Multipath losses can be quite high.
- Millimeter wave signals generally don't penetrate solid objects.

For these reasons, 802.11ad is likely to be useful only within a single room. Because it can support high data rates and could easily transmit uncompressed high-definition video, it is suitable for applications such as replacing wires in a home entertainment system, of streaming high-definition movies from your cell phone to your television.

Whereas 802.11ac supports a MIMO antenna configuration, 802.11ad is designed for single antenna operation. And 802.11ad has a huge channel bandwidth of 2160 MHz.

5.3 Bluetooth

Bluetooth is a wireless technology that uses short-range digital radio communications and offers fast and reliable transmission of both voice and data. Bluetooth is defined in the IEEE 802.15.1 standard.

Now Bluetooth is managed by the Bluetooth Special Interest Group (SIG), which has more than 25,000 member companies in the areas of telecommunication, computing, networking, and consumer electronics. The IEEE no longer maintains the standard. The Bluetooth SIG oversees development of the specification, manages the qualification program, and protects the trademarks.

It is essentially a low-power, short-range, low-rate "cable replacement" technology for interconnection devices. Bluetooth incorporates a radio frequency transceiver and a full set of networking protocols on a single chip that is small enough to be included in cellular and cordless phone, portable PCs, headsets, etc. Sometimes, 802.15.1 networks are referred as wireless personal area networks (WPANs).

802.15.1 networks operate in the 2.4GHz unlicensed radio band in a TDM manner, with time slots of 625 microseconds. During each time slot, a sender transmits on one of 79 channels, with the channel changing in a known but pseudo random manner from slot to slot. This form of channel hopping, known as frequency-hopping spread spectrum (FHSS), spreads transmissions in time over the frequency spectrum. It can provide data rate up to 4 Mbps.

Some layers and protocols of Bluetooth.

- Bluetooth Radio layer: This is the lowest defined layer of the bluetooth specification. It is not a protocol, but defines the requirements and operations of the bluetooth transceiver device, transmitting and receiving radio frequency signals in the 2.4GHz ISM band.
- Baseband: This is the physical layer protocol of the bluetooth specification and it lies on top of the bluetooth radio layer.
- Link Manager Protocol(LMP): LMP performs the link setup, configuration and authentication process within the bluetooth stack. After the Link Manager(LM) of one device discovers the LM of another device, the LMP then communicates with the remote LM to establish a link.

- Host Controller Interface (HCI): HCI provides a commend interface between the baseband control and the LM.
- L2CAP (Logical link control and adaptation protocol): The L2CAP resides on data-link layer (OSI model) and provides the link functions for the baseband protocol.
- RFCOMM (Radio frequency communication): is the cable replacement protocol in the bluetooth stack. It creates a virtual seral port through which RF communications can be passed using standard EIA/TIA (Electronics Industries Association/Telecommunications Industry Association) 232 standard, which is the serial port communication standard.

- Object Exchange Protocol (OBEX): Originally specified by the Infrared Data Association (IrDA), OBEX is used to transfer data, graphics and voice objects between devices. OBEX is used in serval devices, such as PDAs (personal digital assistants), mobile phones and computer systems.
- vCard/vcal: A protocol used to store and transfer virtual business cards and personal calenders on mobile devices.
- TCP (Telephony control protocol): Used to set up and control speech and data calls between Bluetooth devices. The protocol is based on the ITU-T standard Q.931, with the provisions of Annex D applied, making only the minimum changes necessary for Bluetooth.

  TCP is used by the intercom (ICP) and cordless telephony (CTP) profiles.

- AT command set: It includes the control commands used to control dial-up modem functions and actions.
- Telephone Control Specification–Binary(TCS BIN): It is a bit-oriented protocol used to establish voice and data links between bluetooth devices.
- Service Discovery Protocol (SDP): Bluetooth requires an SDP to identify and manage the services available on portable devices moving into and out of range with each other. The Bluetooth SDP is specifically designed for bluetooth devices.

- Synchronous connection-oriented (SCO)link: The type of radio link used for voice data. An SCO link is a set of reserved timeslots on an existing ACL (Asynchronous Connection-Less) link. Each device transmits encoded voice data in the reserved timeslot. There are no retransmissions, but forward error correction can be optionally applied. SCO packets may be sent every 1, 2 or 3 timeslots.

  Enhanced SCO (eSCO) links allow greater flexibility in setting up links: they may use retransmissions to achieve reliability, allow a wider variety of packet types, and greater intervals between packets than SCO, thus increasing radio availability for other link.

In bluetooth, communications are between wireless stations (no APs). The operation of bluetooth networks (called piconets) is based on the master-slave principle, where one station is the master and other stations (up to 7) become the slaves. Bluetooth technology can also provide a link to a wired network in a similar way that 802.11 access point do, by installing a bluetooth access point that is connected to a wired network.

An ad-hoc bluetooth network piconet can include up to 8 bluetooth devices. When more than 8 device are attempting to associate with a piconet, the piconet is divided into two or more piconets, and then interconnected into what is called a scatternet.

A bluetooth device cannot act as a master for two piconet. If a piconet master device is also linked to another piconet in a scatternet, it must participate as a master device in one piconet and a slave device in a second piconet. The slaves that share the same master device belong to the same pibonet and to remain as a member of a piconet, each slave must interact with the master on a time interval negotiated between the master and the salve. If the master leaves the piconet, the other devices must elect a new master and the piconet is reformed. When a bluetooth device is a member of two piconets, it can be used as a link between the piconets.

Any bluetooth device is capable of serving as a master or a slave, depending on the networking situation it encounters on-the-fly. A piconet can be formed using one of the following methods:

- A master device actively scans for slave devices and, when it detects one in its range, it can invite the device to join a piconet as a slave.
- A master device can passively wait for a slave to contact it, and then invite the slave to join the piconet as a slave.

Bluetooth devices each have a unique clock signal and device address, which are combined to provide a unique identity. The difference or offset between one device's clock signal and the clock signal of another device is the basis for the FHSS (frequency-hopping spread-spectrum) sequence used between the devices to transmit data.

Bluetooth device use frequency hopping in order to avoid interference with other devices that operate in the same unlicensed ISM (Industrial Scientific and Medical) band. The frequency-hopping scheme uses 79 different channels and changes frequency 1600 times per second in a pseudo-random matter. This makes eavesdropping slightly more difficult.

Bluetooth is a short range radio technology enabling communications over a few meters only (mostly in class 2 that is for 10 meters). That means that an attacker must be physically close to the victims in order to eavesdrop the communications, which also reduces the likelihood of attacks.

5.4 Mobility management

Now we consider the situation about a mobile user how to maintain ongoing connections while moving between notworks.

In the case of mobile, the mobile node (such as a smartphone or a laptop) needs a “permanent home address” known as home network, and an entity within the home network that performs the mobility management functions on behalf of the mobile node known as the home agent.

The network in which the mobile node is currently residing is known as the foreign (or visited) network, and the entity within in the foreign network that helps the mobile node with the mobility management functions is known as a foreign agent. A correspondent is the entity wishing to communicate with the mobile node.

Mobile IP

One role of the foreign agent is to create a so called care-of address (COA) for the mobile node, with the network portion of the COA matching that of the foreign network.

So there are two addresses associated with a mobile node, its permanent address and its COA, sometimes known as a foreign address.

Although we have separated the functionality of the mobile node and the foreign agent, it is worth to note that the mobile node can also assume the responsibility of the foreign agent.

The Internet architecture and protocols for supporting mobility, collectively known as mobile IP, are defined primarily in RFC 5944 for IPv4.

Mobile IP is a flexible standard, supporting many different modes of operation, multiple ways for agents and mobile nodes to discover each other, use of single or multiple COAs, and multiple forms of encapsulation.

The mobile IP standard consists of three main pieces:

- Agent discovery.
- Registration with the home agent.
- Indirect routing of datagrams.

Agent discovery

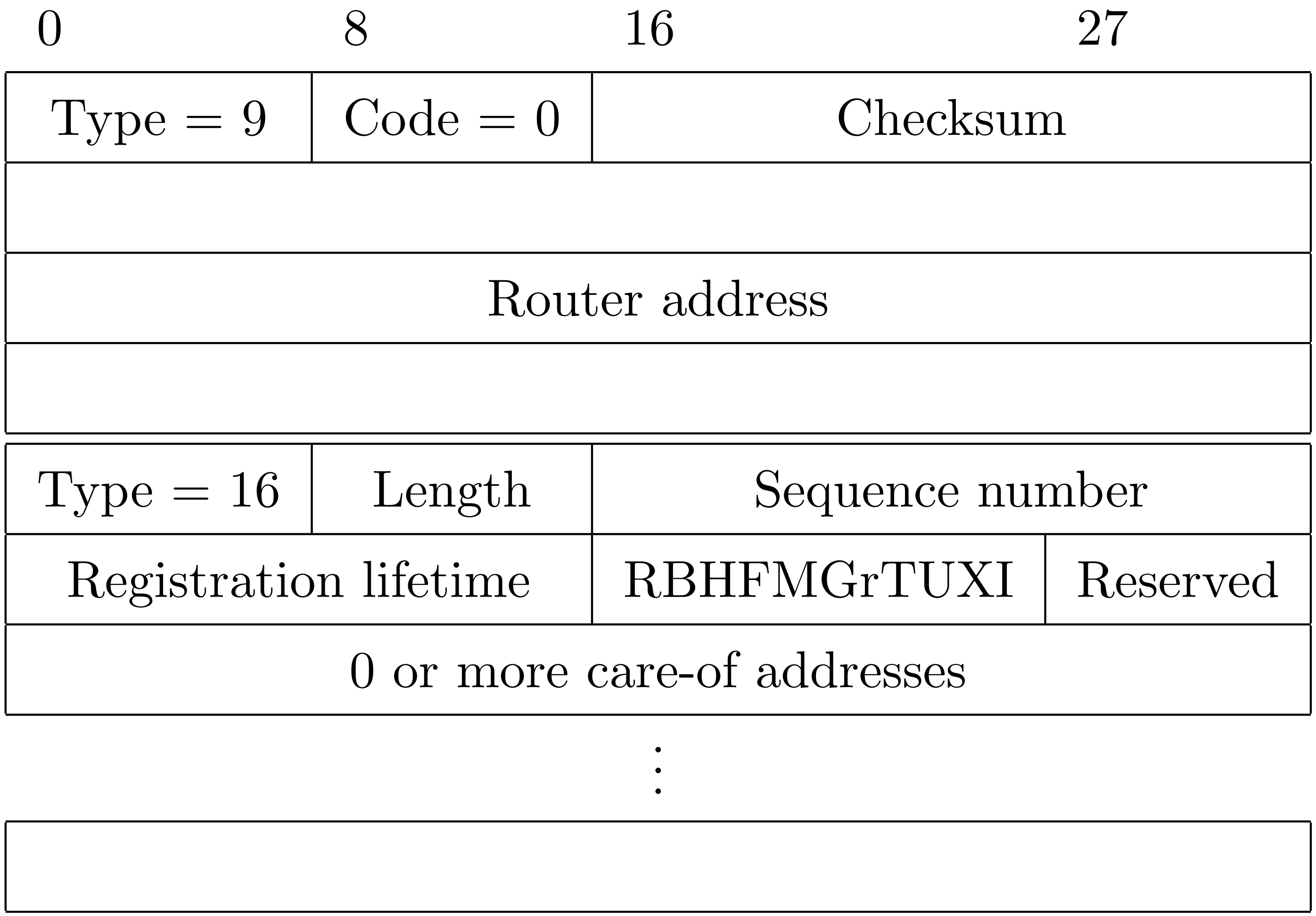
Agent discovery can be accomplished in one of two ways: via agent advertisement or via agent solicitation.

With agent advertisement, a foreign or home agent advertises its services using an extension to the existing router discovery protocol.

The agent periodically broadcast an ICMP message with a type of 9 (router discovery) on all links to which it is connected. The router discovery message contains the IP address of the router (the agent), thus allowing a mobile node to learn the agent's IP address.

The router discovery message also contains a mobility agent advertisement extension that contains additional information needed by the mobile node.

The format of the ICMP router discovery message with mobility agent advertisement extension is as in Figure 4.



0	8	16	27
Type = 9	Code = 0	Checksum	
Router address			
Type = 16	Length	Sequence number	
Registration lifetime		RBHFMGrTUXI	Reserved
0 or more care-of addresses			
⋮			

Figure 4: Discovery message

In Figure 4, the upper part contains the standard ICMP fields and the lower part is the mobility agent advertisement extension.

Some of the fields are explained below.

- Registration required bit (R): Registration with this foreign agent (or another foreign agent on this link) is required even when using a co-located care-of address.
- Busy bit (B): The foreign agent will not accept registrations from additional mobile nodes.
- Home agent bit (H): Indicates that the agent is a home agent for the network in which it resides.
- Foreign agent bit (F): Indicates that the agent is a foreign agent for the network in which it resides.

- Registration required bit (R): Indicates that a mobile user in this network must register with a foreign agent. In particular, a mobile user cannot obtain a care-of address in the foreign network (for example, using DHCP) and assume the functionality of the foreign agent for itself, without registering with the foreign agent.
- M, G encapsulation bits: Indicate whether a form of encapsulation other than IP-in-IP encapsulation will be used.
- Care-of address fields: A list of one or more care-of addresses provided by the foreign agent.

For agent solicitation, a mobile node wanting to learn about agents without waiting to receive an agent advertisement can broadcast an agent solicitation message, which is simply an ICMP message with type value 10.

An agent receiving the solicitation will unicast an agent advertisement directly to the mobile node, which can then proceed as if it had received an unsolicited advertisement.

Registration with the home agent

Once a mobile IP node received a COA, that address must be registered with the home agent.

This can be done either via the foreign agent (who then registers the COA with the home agent) or directly by the mobile IP node itself.

Registering by the foreign agent is as follows.

1. By receipting a foreign agent advertisement, a mobile node sends a mobile IP registration message to the foreign agent. The registration message is carried within a UDP datagram and sent to port 434. The registration message carries a COA advertised by the foreign agent, the address of the home agent (HA), the permanent address of the mobile node (MA), the requested lifetime of the registration, and a 64-bit registration identification. The registration identifier acts like a sequence number and serves to match a received registration reply with a registration request.

2. The foreign agent receives the registration message and records the mobile node's permanent IP address. The foreign agent now knows that it should be looking for datagram containing an encapsulated datagram whose destination address matches the permanent address of the mobile node. The foreign agent then sends a mobile IP registration message to port 434 of the home agent. The message contains the COA, HA, MA, encapsulation format requested requested registration lifetime, and registration identification.

3. The home agent receives the registration request and checks for authenticity and correctness. The home agent binds the mobile node's permanent IP address with the COA. The home agent sends a mobile IP registration reply containing the HA, MA, actual registration lifetime, and the registration identification of the request that is being satisfied with this reply.
4. The foreign agent receives the registration reply and then forwards it to the mobile node.

Indirect routing of datagrams

The mobile node informs its home agent of its current location using the registration procedure described above.

Home agents and foreign agents will support tunneling datagrams using IP-in-IP encapsulation. Any mobile node that uses a care-of address will support receiving datagrams tunneled using IP-in-IP encapsulation.

When connected to its home network, a mobile node operates without the support of mobility services. That is, it operates in the same way as any other (fixed) host or router. ICMP Router Advertisement is one such method as we discussed before.

When registered on a foreign network, the mobile node chooses a default router.

Upon receipt of an encapsulated datagram sent to its advertised care- of address, a foreign agent compares the inner Destination Address to those entries in its visitor list. When the Destination does not match the address of any mobile node currently in the visitor list, the foreign agent will not forward the datagram. Otherwise, the foreign agent forwards the decapsulated datagram to the mobile node.

The home agent is able to intercept any datagrams on the home network addressed to the mobile node while the mobile node is registered away from home.

The home agent must examine the IP Destination Address of all arriving datagrams to see if it is equal to the home address of any of its mobile nodes registered away from home. If so, the home agent tunnels the datagram to the mobile node's currently registered care- of address or addresses.

The mobile IP standard allows many additinal scenarios and capabilities in addition to the above description. RFC 5944 contains more than 100 pages. Mobile IPv6 is defined in RFC 6275, which we omit here.

5.5 Mobile Sensor Networks

Wireless sensor networks (WSN) usually integrate a large number of low-power, low-cost sensor nodes. They are largely deployed to monitor a specific environment.

There are many different applications of WSNs:

- Military applications: Wireless sensor networks be likely an integral part of military command, control, communications, computing, intelligence, battlefield surveillance, reconnaissance and targeting systems.

- Area monitoring: In area monitoring, the sensor nodes are deployed over a region where some phenomenon is to be monitored. When the sensors detect the event being monitored (heat, pressure etc), the event is reported to one of the base stations, which then takes appropriate action.

- Transportation: Real-time traffic information is being collected by WSNs to later feed transportation models and alert drivers of congestion and traffic problems.
- Health applications: Some of the health applications for sensor networks are supporting interfaces for the disabled, integrated patient monitoring, diagnostics, and drug administration in hospitals, tele-monitoring of human physiological data, and tracking and monitoring doctors or patients inside a hospital.
- Environmental sensing: The term Environmental Sensor Networks has developed to cover many applications of WSNs to earth science research. This includes sensing volcanoes, oceans, glaciers, forests etc.

- Structural monitoring: Wireless sensors can be utilized to monitor the movement within buildings and infrastructure such as bridges, flyovers, embankments, tunnels etc enabling Engineering practices to monitor assets remotely with out the need for costly site visits.
- Industrial monitoring: Wireless sensor networks have been developed for machinery condition-based maintenance (CBM) as they offer significant cost savings and enable new functionality. In wired systems, the installation of enough sensors is often limited by the cost of wiring.
- Agricultural sector: using a wireless network frees the farmer from the maintenance of wiring in a difficult environment. Irrigation automation enables more efficient water use and reduces waste.

Sensor networks often have one or more points of centralized control called base stations. sensor nodes are small in size and able to sense, process data and communicate with each other, typically over an RF (radio frequency) channel. In general, there are three categories of traffic:

- Many-to-one traffic.
- One-to-many traffic.
- Local traffic: The nodes in a limited area send localized messages to discover the neighbouring nodes and coordinate with each other. May be broadcast or send messages intended for a single neighbour.

WSN Features

The basic features of WSNs:

- Self-organizing capabilities. The WSNs are able to cope with topology variability and infrastructure variations.
- Short-range broadcast communication and multirouting. The sensor nodes have reduced radio ranges and should cooperate to achieve complete routing of information.
- Dense deployment and cooperative effort of sensor nodes. The shortage of the radio range and the need to have efficient sensing call for a dense deployment of sensors.
- Limitations of energy, transmit power, memory and computing power. WSNs cope with limitation of resources and frequent changes of topology due to fading and node failures.

Some of the challenges for WSNs:

- Extension of lifetime. A typical alkaline battery, for example, provides about 50 watt-hours of energy. Given the expense and the potential infeasibility of monitoring and replacement of batteries for a large WSN, significantly longer lifetimes would be desired.
- Responsiveness. A simple solution to extending network lifetime is to operate the nodes in a duty-cycled manner with periodic switching between sleep and wake-up modes. This causes the time synchronizing requirement, and the responsiveness of and the effectiveness of the sensors.

- Robustness. The use of large number of inexpensive devices characterizes the WSNs. It is important to ensure that the global performance of the system is not sensitive to individual device failure. It is also often desirable that the performance of the system degrade as gracefully as possible with respect to component failure.
- Synergy. Design synergistic protocol, which ensures that the system as a whole is more capable than the sum of the capabilities of its individual component. The protocols must provide an efficient collaborative use of storage, computation and communication resources.

- Self-configuration. WSNs are inherently unattended distributed systems. Autonomous operation of the network is therefore a key design. Nodes in a wireless sensor network have to be able to configure their own network topology, synchronize, and calibrate themselves; coordinate inter-node communication; and determine other important operating parameters.
- Privacy and security. The large scale, prevalence, and sensitivity of the information collected by WSN (as well as their potential deployment in hostile locations) give rise to the final key challenge of ensuring both privacy and security.

Structure of WSN

Structure of a Wireless Sensor Network includes different topologies for radio communications networks.

- Star network (single point-to-multipoint): A star network is a communications topology where a single base station can send and/or receive a message to a number of remote nodes. The remote nodes are not permitted to send messages to each other. The advantage of this type of network for wireless sensor networks includes simplicity, ability to keep the remote node's power consumption to a minimum. It also allows low latency communications between the remote node and the base station. The disadvantage of such a network is that the base station must be within radio transmission range of all the individual nodes and is not as robust as other networks due to its dependency on a single node to manage the network.

- Mesh network: A mesh network allows transmitting data to one node to other node in the network that is within its radio transmission range. This allows for what is known as multi-hop communications. This network topology has the advantage of redundancy and scalability. If an individual node fails, a remote node still can communicate to any other node in its range, which in turn, can forward the message to the desired location. In addition, the range of the network is not necessarily limited by the range in between single nodes; it can simply be extended by adding more nodes to the system. The disadvantage of this type of network is in power consumption for the nodes that implement the multi-hop communications are generally higher than for the nodes that dont have this capability, often limiting the battery life. Additionally, as the number of communication hops to a destination increases, the time to deliver the message also increases.

- Hybrid star–Mesh network: A hybrid between the star and mesh network provides a robust and versatile communications network, while maintaining the ability to keep the wireless sensor nodes power consumption to a minimum. In this network topology, the sensor nodes with lowest power are not enabled with the ability to forward messages. This allows for minimal power consumption to be maintained. However, other nodes on the network are enabled with multi-hop capability, allowing them to forward messages from the low power nodes to other nodes on the network. Generally, the nodes with the multi-hop capability are higher power, and if possible, are often plugged into the electrical mains line. This is the topology implemented by the up and coming mesh networking standard known as ZigBee.

Routing strategies for WSNs.

- Adopt a flat network architecture in which all nodes are considered peers. Flat network architecture has several advantages, including minimal overhead to maintain the infrastructure and the potential for the discovery of multiple routes between communicating nodes for fault tolerance.
- Impose a structure on the network to achieve energy efficiency, stability, and scalability. In this class of protocols, network nodes are organized in clusters in which a node with higher residual energy, for example, assumes the role of a cluster head. The cluster head is responsible for coordinating activities within the cluster and forwarding information between clusters. Clustering has potential to reduce energy consumption and extend the lifetime of the network.

- Use a data-centric approach to disseminate interest within the network. The approach uses attribute-based naming, whereby a source node queries an attribute for the phenomenon rather than an individual sensor node. The interest dissemination is achieved by assigning tasks to sensor nodes and expressing queries to relative to specific attributes. Different strategies can be used to communicate interests to the sensor nodes, including broadcasting, attribute-based multicasting, geo-casting, and any casting.
- Use location to address a sensor node. Location-based routing is useful in applications where the position of the node within the geographical coverage of the network is relevant to the query issued by the source node. Such a query may specify a specific area where a phenomenon of interest may occur or the vicinity to a specific point in the network environment.

Routing protocols

Some of the major routing protocols and algorithms to deal with the energy conservation issue.

- Flooding: Flooding is a common technique frequently used for path discovery and information dissemination in wired and wireless ad hoc networks. The routing strategy of flooding is simple and does not rely on costly network topology maintenance and complex route discovery algorithms. Flooding uses a reactive approach whereby each node receiving a data or control packet sends the packet to all its neighbors. After transmission, a packet follows all possible paths. Unless the network is disconnected, the packet will eventually reach its destination. Furthermore, as the network topology changes, the packet transmitted follows the new routes.

- Gossiping: To address the shortcomings of flooding, a derivative approach, referred to as gossiping, has been proposed. Similar to flooding, gossiping uses a simple forwarding rule and does not require costly topology maintenance or complex route discovery algorithms. Contrary to flooding, where a data packet is broadcast to all neighbors, gossiping requires that each node sends the incoming packet to a randomly selected neighbor. Upon receiving the packet, the neighbor selected randomly chooses one of its own neighbors and forwards the packet to the neighbor chosen. This process continues iteratively until the packet reaches its intended destination or the maximum hop count is exceeded.

- Protocols for Information via Negotiation (SPIN): Sensor protocols for information via negotiation (SPIN), is a data-centric negotiation-based family of information dissemination protocols for WSNs. The main objective of these protocols is to efficiently disseminate observations gathered by individual sensor nodes to all the sensor nodes in the network. Simple protocols such as flooding and gossiping are commonly proposed to achieve information dissemination in WSNs. Flooding requires that each node sends a copy of the data packet to all its neighbors until the information reaches all nodes in the network. Gossiping, on the other hand, uses randomization to reduce the number of duplicate packets and requires only that a node receiving a data packet forward it to a randomly selected neighbor.

- Low-Energy Adaptive Clustering Hierarchy (LEACH): adopts a hierarchical approach to organize the network into a set of clusters. Each cluster is managed by a selected cluster head. The cluster head assumes the responsibility to carry out multiple tasks. The first task consists of periodic collection of data from the members of the cluster. Upon gathering the data, the cluster head aggregates it in an effort to remove redundancy among correlated values. The second main task of a cluster head is to transmit the aggregated data directly to the base station over single hop. The third main task of the cluster head is to create a TDMA-based schedule whereby each node of the cluster is assigned a time slot that it can use for transmission. The cluster head announces the schedule to its cluster members through broadcasting.

To reduce the likelihood of collisions among sensors within and outside the cluster, LEACH nodes use a code-division multiple accessbased scheme for communication. The basic operations of LEACH are organized in two distinct phases. The first phase, the setup phase, consists of two steps, cluster-head selection and cluster formation. The second phase, the steady-state phase, focuses on data collection, aggregation, and delivery to the base station. The duration of the setup is assumed to be relatively shorter than the steady-state phase to minimize the protocol overhead.

- Hierarchical routing protocols TEEN and APTEEN: These protocols were proposed for time-critical applications. In TEEN, sensor nodes sense the medium continuously, but the data transmission is done less frequently. A cluster head sensor sends its members a hard threshold, which is the threshold value of the sensed attribute and a soft threshold, which is a small change in the value of the sensed attribute that triggers the node to switch on its transmitter and transmit. Thus the hard threshold tries to reduce the number of transmissions by allowing the nodes to transmit only when the sensed attribute is in the range of interest. The soft threshold further reduces the number of transmissions that might have otherwise occurred when there is little or no change in the sensed attribute.

A smaller value of the soft threshold gives a more accurate picture of the network, at the expense of increased energy consumption. Thus, the user can control the trade-off between energy efficiency and data accuracy. When cluster-heads are to change, new values for the above parameters are broadcast. The main drawback of this scheme is that, if the thresholds are not received, the nodes will never communicate, and the user will not get any data from the network.

- Power-Efficient Gathering in Sensor Information Systems (PEGASIS): The main objectives of PEGASIS are twofold. First, the protocol aims at extending the lifetime of a network by achieving a high level of energy efficiency and uniform energy consumption across all network nodes. Second, the protocol strives to reduce the delay that data incur on their way to the sink. The network model considered by PEGASIS assumes a homogeneous set of nodes deployed across a geographical area. Nodes are assumed to have global knowledge about other sensors positions. Furthermore, they have the ability to control their power to cover arbitrary ranges.

The nodes may also be equipped with CDMA-capable radio transceivers. The nodes responsibility is to gather and deliver data to a sink, typically a wireless base station. The goal is to develop a routing structure and an aggregation scheme to reduce energy consumption and deliver the aggregated data to the base station with minimal delay while balancing energy consumption among the sensor nodes. Contrary to other protocols, which rely on a tree structure or a cluster-based hierarchical organization of the network for data gathering and dissemination, PEGASIS uses a chain structure.

- Directed Diffusion: The main objective of the protocol is to achieve substantial energy savings in order to extend the lifetime of the network. To achieve this objective, directed diffusion keeps interactions between nodes, in terms of message exchanges, localized within limited network vicinity. Using localized interaction, direct diffusion can still realize robust multi-path delivery and adapt to a minimal subset of network paths. This unique feature of the protocol, combined with the ability of the nodes to aggregate response to queries, results into significant energy savings. The main elements of direct diffusion include interests, data messages, gradients, and reinforcements. Directed diffusion uses a publish-and-subscribe information model in which an inquirer expresses an interest using attributevalue pairs. An interest can be viewed as a query or an interrogation that specifies what the inquirer wants.

- Geographic Adaptive Fidelity (GAF): is an energy-aware location-based routing algorithm designed mainly for mobile ad hoc networks, but may be applicable to sensor networks as well. The network area is first divided into fixed zones and forms a virtual grid. Inside each zone, nodes collaborate with each other to play different roles. For example, nodes will elect one sensor node to stay awake for a certain period of time and then they go to sleep. This node is responsible for monitoring and reporting data to the BS on behalf of the nodes in the zone. Hence, GAF conserves energy by turning off unnecessary nodes in the network without affecting the level of routing fidelity.