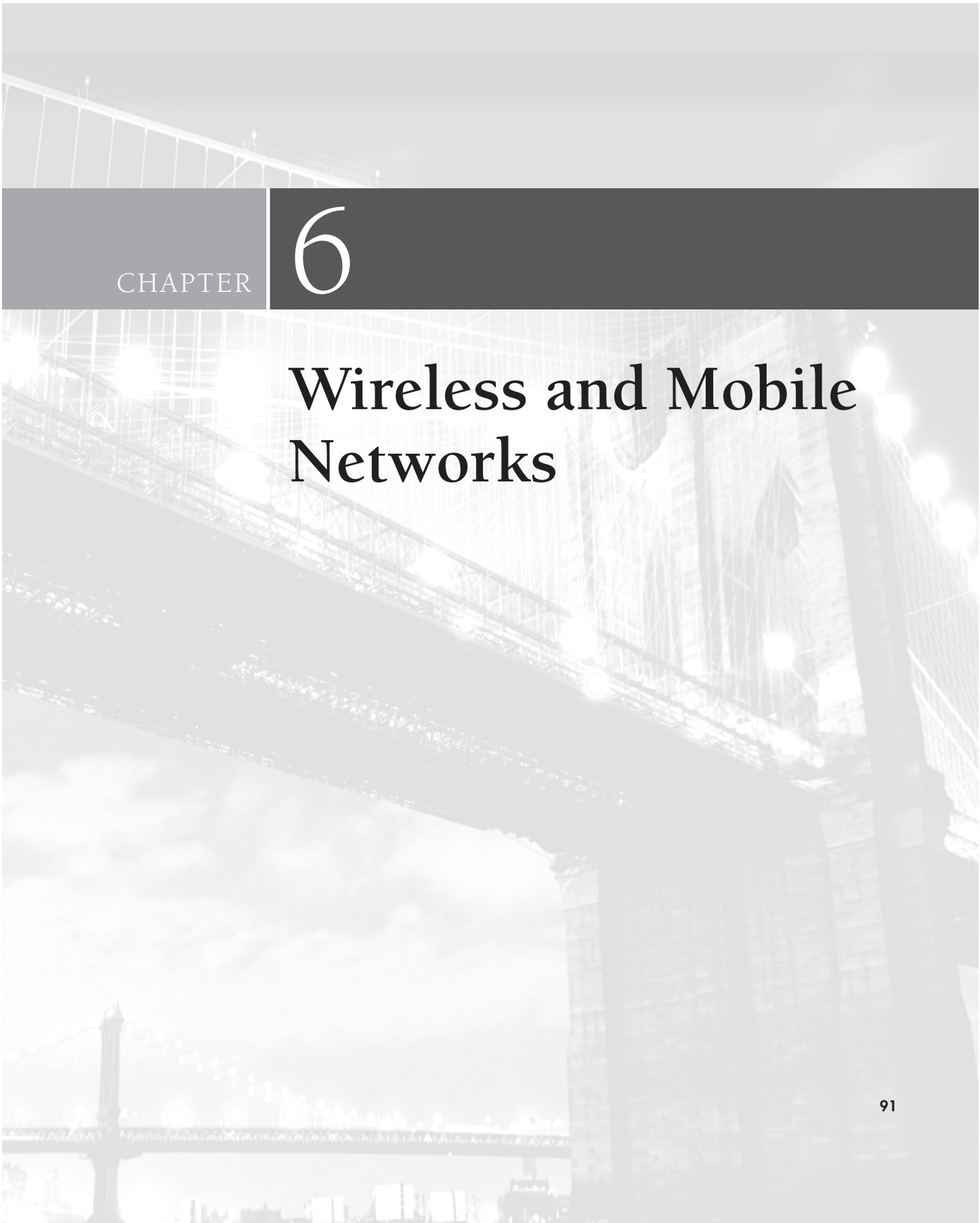


CHAPTER 6

Wireless and Mobile Networks

Most Important Ideas and Concepts from Chapter 6

- **Wireless and mobility: each poses very different challenges.** In this chapter, we drew an important distinction between *communication over a wireless link*, and the *mobility* that wireless links enable. These topics, which roughly comprise the first and second half of the chapter, pose very different challenges. Communication over a wireless link is, as the name implies, primarily a link layer (that is, a single hop) problem. Wireless link communication protocols send link-layer frames between a sender and a receiver(s) over a single hop, in much the same way as the wired LAN protocols (for example, Ethernet) that we studied in Chapter 5. However, wireless communication protocols must deal with the more difficult characteristics of the wireless link—the hidden terminal problem, and link errors resulting from interference, fading, and multipath (see "How a wireless broadcast link differs from a wired broadcast link" below).

  Mobility—the challenge of communicating with a host that changes its point of attachment to the network—is made possible by wireless links. But as shown in Figure 6.16 on page 536 of the textbook, mobility is also possible in wired networks. For example, a host can change its point of attachment to the network from one wired location to another wired location. Many discussions of wireless and mobility treat the two topics as inextricably intertwined. Here, we'll consider the problems posed by each separately.

- **Wireless networks: infrastructure mode versus ad hoc.** In Section 6.1, we learned that there are two types of wireless networks: those that operate in *infrastructure mode*, and those that operate in *ad hoc mode*. We encounter infrastructure-mode networks in our daily lives, for example, when we attach our wireless device to an 802.11 wireless access point in an Internet café or classroom. In infrastructure mode networks, an access point (a.k.a. base station) is present, and typically connected directly to the wired network (see Figure 6.1 on page 506 of the textbook). When a wireless host first enters an infrastructure network (for example, when you sit down in the café or classroom, and power up your laptop), it must first *associate* with the access point (see pages 515–516 of the textbook). All communication to and from the wireless host is then over the wireless channel between the host and the base station. Indeed, two wireless hosts in the same wireless infrastructure network (for example, two café patrons, or two of the wireless hosts in the upper-left circle shown in Figure 6.1) will communicate with each other via the base station. Note the important role of the base station—it connects the wireless host to the rest of the network, where services such as network-layer address assignment (typically via DHCP) and routing are performed, in much the same way that a wired Ethernet switch (Section 5.6.2) connects a wired host to the rest of the network.

  In an ad hoc network, no base station is present. An ad hoc network might be formed for example, when users are in proximity of each other on a train, or bet-

ter yet on a remote island beach, where no infrastructure is present. Consequently, the individual hosts themselves must perform functions such as address-assignment and routing (when the hosts in the wireless ad hoc network are connected via multiple wireless hops). Currently, ad hoc networking is an area of active research, and thus is a topic beyond the scope of our introductory text.

- **Code Division Multiple Access (CDMA).** In Chapter 5, we learned that hosts can share a broadcast channel in either frequency (for example, FDMA) or in time (for example, TDMA). In Sections 5.3.2 and 5.3.3, we studied various random access protocols that share the channel in time. CDMA provides yet another way for multiple users to share a broadcast channel. In CDMA, each user has a different *M*-bit code. Each original data bit to be sent by the user is first multiplied by each of the *M* bits in the code, producing a sequence of *M* bits (that is, each original bit is transformed into *M* bits via this multiplication) that are sent into the channel. The properties of the codes are such that when two or more users send their *M* bits simultaneously, a receiver knowing a given sender's code can extract the sender's original data bit out of the additively-interfering bits sent by the multiple users. Recall that simultaneous transmissions by two or more users in the time-sharing random access protocols that we studied in Chapter 5 result in interference, with no message being received successfully. In CDMA, two users can send simultaneously and a receiver can still extract the message from one of the senders. Indeed, two different receivers can extract two different messages sent by two different "interfering" CDMA senders if the receivers each have the codes of the different senders (see review Questions 2 and 3 on pages 98 and 99).
- **How a wireless broadcast link differs from a wired broadcast link.** The physical characteristics of a wireless link are significantly different from those of a wired link, with these differences resulting in wireless multiple access protocols that are significantly different from their wired counterparts. First, *signal attenuation*—the decrease in a signal's strength as it propagates—is much more significant in a wireless network than in a wired network. In a wired network, all hosts connected to the broadcast medium (for example, the same Ethernet segment) can "hear" each other. In a wireless network, signal fading results in scenarios such as that shown in Figure 6.3(b) in the textbook, where host B can hear both hosts A and C, but hosts A and C cannot hear each other. As a result, A cannot hear a transmission from C to B, and may thus transmit a frame to B that collides with an ongoing frame transmission from C to B. A second difference between wireless and wired networks is that physical objects may block or degrade wireless signals, again resulting in a situation in which not all wireless hosts can hear the transmissions of the other wireless hosts (for example, see Figure 6.3(a) in the textbook). Finally, a third difference is that bit errors are more likely in a wireless link than in a wired link, as a result of electromagnetic interference and multipath propagation.
- **CSMA/CA and the RTS/CTS mechanism.** The CSMA/CA protocol and the RTS/CTS mechanism are part of the IEEE 802.11 specification. With more than

100 million Wi-Fi chipsets sold per year, 802.11 is arguably the most important wireless network access protocol, and thus a good topic for our top-10 list here! Since the details of the CSMA/CA and RTS/CTS protocols are provided in the text, we won't repeat them here, but instead provide some context and insight into the mechanisms. Similar to the other CSMA protocols we studied in Chapter 5, CSMA/CA senses the channel and will only transmit when the channel is sensed idle. Unlike CSMA/CD, however, CSMA/CA does *not* detect collisions and thus *cannot* abort transmissions when a collision occurs. Instead, frames are transmitted in their entirety—making a collision an expensive event, since the channel will be wasted for the entire duration of the frame's transmission. CSMA/CA has several features that cope with the challenges caused by signal attenuation and the hidden terminal problem shown in Figure 6.9 on page 521 of the textbook. First, CSMA/CA has an explicit ACK mechanism, allowing the sender to know that a frame has been received successfully. Recall from our discussion above and in the text that a node cannot necessarily "hear" whether its transmission was successfully received at the destination due to attenuation and the hidden terminal problem. A second important feature of 802.11 is the RTS/CTS mechanism, which allows a station to reserve the channel for a data message and its subsequent ACK. When RTS/CTS is used, collisions among RTS/CTS messages (rather than data frames) can still occur, but since the RTS/CTS messages are smaller than data frames, the overhead incurred by a collision is less.

- **Direct versus indirect routing to a mobile host.** In Chapter 6, we identified two basic approaches by which a correspondent can send data to a mobile host—the *indirect* approach and the *direct* approach. An *indirect approach* is taken by both mobile IP (for routing datagrams to a mobile IP host) and GSM (for routing a phone call to a mobile telephone user). In the indirect approach, the correspondent sends all traffic (IP datagrams in the case of mobile IP, or the telephone call, in the case of GSM) to the mobile host's home network. The home network knows the foreign network where the mobile host is located (see "Home and foreign agents" in the next bulleted entry). The home network then relays the data that it receives from the correspondent to the foreign network where the mobile host is located. The indirect approach works by adding a level of indirection—the home agent—between the sender and the receiver. This use of indirection is another example of the aphorism attributed variously to Butler Lampson and David Wheeler: "All problems in computer science can be solved by another level of indirection."

  In the *direct approach*, a correspondent sends its traffic (IP datagrams in the case of mobile IP, or the telephone call in the case of GSM) directly to the mobile host in the foreign network. Of course, first the correspondent must determine the address of the mobile host in the foreign network, and must be notified if the mobile host moves from one foreign network to another. This requires that the correspondent knows whether the mobile is in its home network; it also requires that the correspondent use a different protocol to communicate with the destination host de-

pending on whether or not the destination host is in its home network. Recall that in the indirect approach, the correspondent doesn't need to know whether the destination host is in its home network or visiting a foreign network—that is, the mobility of the destination host is *transparent* to the correspondent. This transparency tremendously simplifies the correspondent's task in communicating with a potentially mobile host. Indeed, the correspondent's actions are exactly the same in both scenarios.

- **Home and foreign agents.** The home agent and foreign agent are software processes that execute in the mobile host's home and foreign network, respectively. They interact with each other to play a crucial role in supporting a host's mobility. In our discussion here, we'll assume that an indirect approach is taken (see "Direct versus indirect routing to a mobile host" above). The *home agent's* role is two-fold. First, it keeps track of the foreign network in which the mobile host is located. This is done via a foreign-agent-to-home-agent registration protocol (see page 543 of the textbook) in which a foreign agent notifies the home agent when the mobile host joins the foreign agent's network. The second job of the home agent is to relay incoming traffic (IP datagrams in the case of mobile IP, or the telephone call in the case of GSM) received from a correspondent to the mobile host (Step 2 in Figure 6.18 in the textbook). The foreign agent is a process running in the foreign network; it too has two principal roles. First, it forwards traffic that that has been relayed by the home agent to the mobile host (Step 3 in Figure 6.18). Its second job is to let the mobile host's home agent know when the mobile host joins its (the foreign agent's) network.
- **Handoffs.** A *handoff* occurs when a mobile host moves from one foreign network to another—that is, changes its point of attachment to the network. If the mobile host is receiving relayed data when it moves between foreign networks, then this relayed data must be re-directed to the foreign network to which the mobile host is newly attached (see Review Question 10 on pages 102–103). In mobile IP, redirection occurs when the foreign agent in the new network notifies the home agent in the mobile host's home network that the mobile host has newly joined its (the foreign agent's) network. The home agent then redirects incoming datagrams to the new foreign agent, who relays the datagrams to the mobile host. In GSM cellular telephony, the redirection point is not in the home network, but rather in the mobile switching center (MSC) that is responsible for routing calls to the foreign network; this MSC is typically "close" to the foreign network. Figure 6.26 on page 555 of the textbook shows the steps involved in a handoff when the old base station and the new base station to which the mobile host is attaching are controlled by the same MSC. When the old base station and the new base station are controlled by different MSCs, an inter-MSC handoff is required, making the handoff is a bit more complex. Inter-MCS handoff is shown in Figure 6.27 on page 556 of the textbook.
- **Mobile IP.** Mobile IP is a proposed Internet Standard protocol (see RFC 3344 for Mobile IPv4 and RFC 3775 for Mobile IPv6); our discussion below involves Mo-

bile IPv4. Mobile IPv4 takes an indirect routing approach (see "Direct versus indirect routing to a mobile host" above), and a home agent and a foreign agent, as described above. The mobile host has a home address, that is, "a long-term IP address on a home network" [RFC 3344], and a care-of-address in the foreign network being visited. As discussed above (and in detail in the textbook), the role of the home agent is to relay incoming datagrams that are initially delivered to the mobile host's home network, to the mobile node in the foreign network. This is accomplished via *tunneling*—a process in which the home agent takes the initial datagram from the correspondent and encapsulates it within another IP datagram and then addresses and sends this latter datagram to the mobile host's care-of-address in the foreign network. A useful analogy here is the mobile twenty-something-year-old who has moved out of her parent's home. Friends may still send her letters at her parent's address. (Of course, realistically, few if any twenty-something-year-olds write letters these days, preferring e-mail, IM, and SMS. But let's assume for pedagogical purposes, that twenty-something-year-olds still write letters). Suppose that a friend has sent a letter to our mobile twenty-something-year-old at her parents' address. A parent (the home agent in IP parlance) takes such a letter (the IP datagram), unopened, places (encapsulates) it in a larger envelope (another IP datagram), and then addresses the larger envelope to the twenty-something-year-old's new address (care-of-address). The postal service (IP network) then delivers the envelope (IP datagram) to the person's current address (care-of-address).

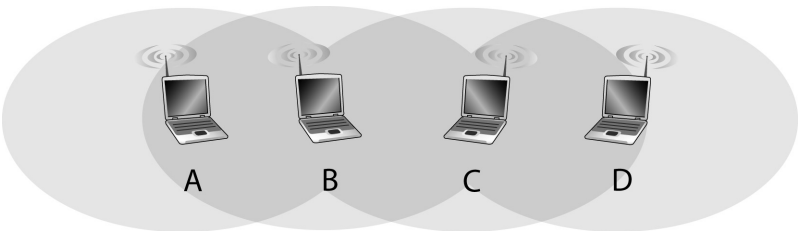
- **Mobility, wireless, and upper layer protocols.** The challenges posed by wireless links and mobile hosts are not confined to the link and networks layers, even though in the textbook our focus is on these lower layers. A packet that is lost on a noisy wireless link will be interpreted by TCP as a congestion-induced loss, and will result in a decrease in TCP's sending rate even though the end-to-end path may well be congestion-free. Handoff delays may result in long packet delivery delays and loss, causing glitches in the audio and video playout. Of course, many exciting applications are enabled by mobility, particularly location-aware applications.

Review Questions

This section provides additional study questions. Answers to each question are provided in the next section.

1. **The performance consequences of channel fading in multi-hop wireless networks.**

   a. Consider the scenario shown below, in which there are four wireless nodes, A, B, C, and D. The radio coverage of the four nodes is shown via the shaded ovals; all nodes share the same frequency. When A transmits, it can only be heard/received by B; when B transmits, both A and C can hear/receive from B; when C transmits both B and D (but not A) can hear/receive from C; when D transmits, only C can hear/receive from D. Now suppose that node A has an infinite supply of messages that it wants to send to D; there are no other messages in the network. A message from A must first be sent to B, which then sends the message to C, which then sends the message to D. Time is slotted, with a message transmission time taking exactly one time slot, for example, as in slotted Aloha. During a slot, a node can do one of the following: (*i*) send a message (if it has a message to be forward toward D); (*ii*) receive a message (if exactly one is being sent to it), (*iii*) remain silent. As always, if a node hears two or more simultaneous transmissions, a collision occurs and none of the transmitted messages are received successfully. You can assume that there are no bit level errors, and thus, if exactly one message is sent, it will be received correctly by those within the transmission radius of the sender.

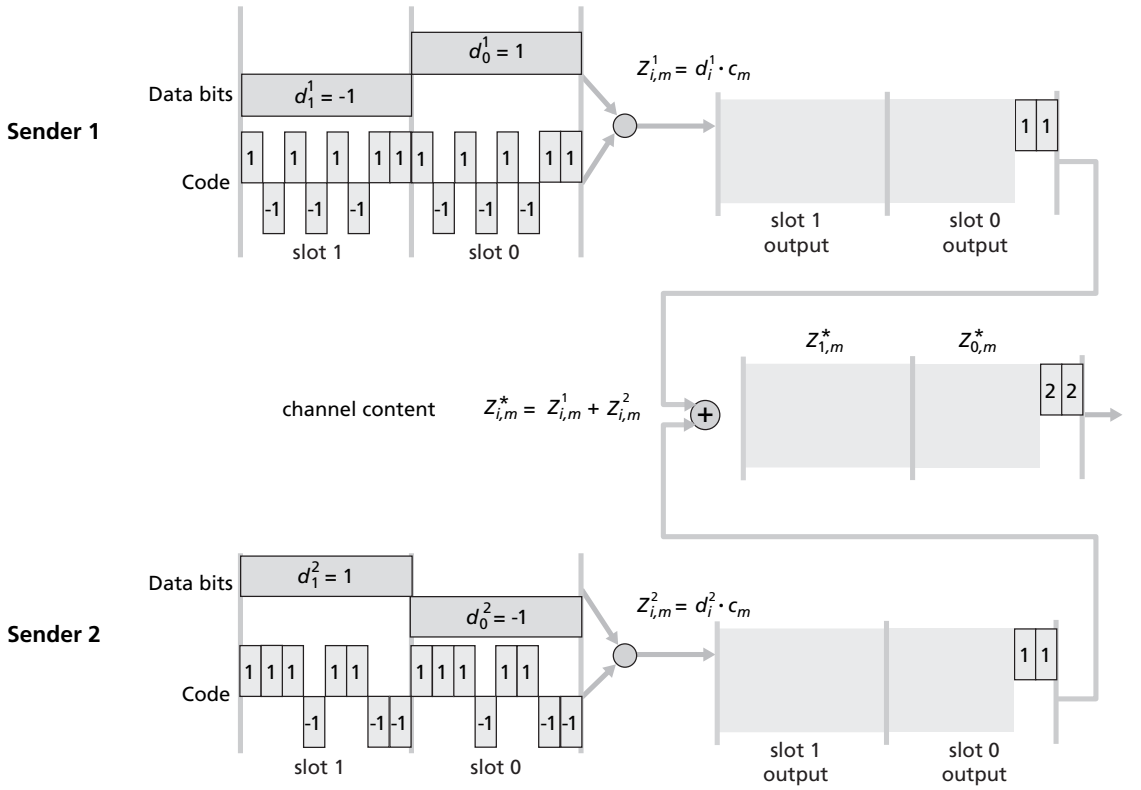


   Now suppose that an omniscient controller (that is, a controller that knows the state of every node in the network) can command each node to do whatever it (the omniscient controller) wishes, that is, to send a message, to receive a message, or to remain silent. Given this omniscient controller, what is the maximum rate at which messages can be transferred from A to D?

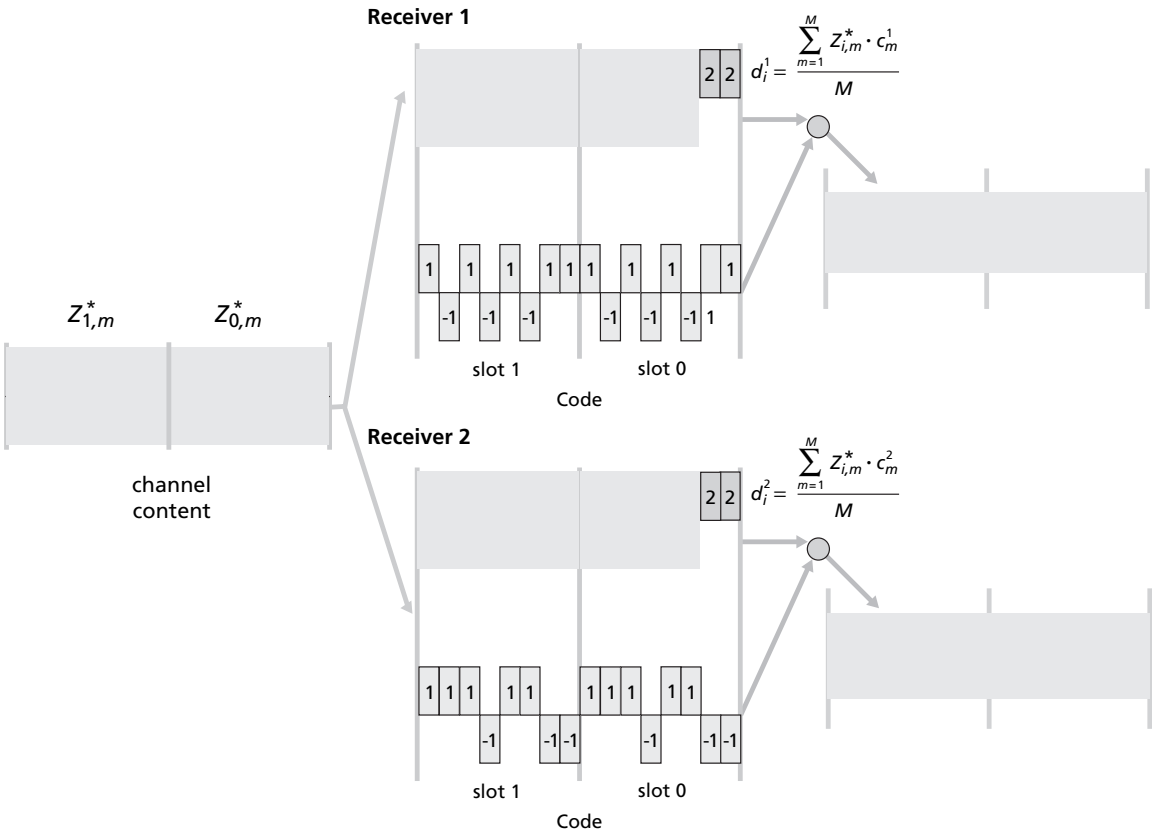
b. Now suppose that the wireless links in the figure above are replaced by wired links. Again, a node can send exactly one message per time slot over a link, but now a node can send a message while it is receiving a message, and simultaneous transmission over two different links do not interfere. In this wired scenario, what is the maximum rate at which messages can be transferred from A to D?

c. Now suppose we are again in the wireless scenario, and that for every data message going from A to D, D will send an ACK message that must be forwarded back to A. What is the maximum rate at which data messages can be transferred from A to D?

2. **A multi-sender CDMA example.** In this example, we consider a CDMA scenario with two senders and two receivers. The chipping rate is 8 mini-slots for each data bit, that is, M = 8, as shown in Figure 6.4 in the textbook. The 8-bit CDMA code for sender 1 is 1, –1, 1, –1, 1, –1, 1, and 1. The 8-bit CDMA code for sender 2 is 1, 1, 1, –1, 1, 1, –1, and –1, as shown in the figure below. Sender 1 has two data bits to send: a 1 followed by a –1; sender 2 also has two data bits to send: a –1 followed by a 1. Compute the sequence of mini-slot bits sent into the channel by sender 1 and by sender 2. Also compute the combined bit values on the channel. The figure below shows the first two mini-slot bits sent by each sender, and the first two mini-slot combined bits values in the channel. You should compute the values for the remaining 14 mini-slots, that is, for the gray-shaded regions in the figure to the right.



3. **A multi-receiver CDMA example.** This problem builds on the answer to the previous problem; you'll need to use the answer to the previous problem to do this problem. Assume now that there are two receivers. Receiver 1 wants to obtain the two data bits sent from sender 1 and knows sender 1's CDMA code; similarly, receiver 2 wants to receive the two data bits sent from sender 2 and knows sender 2's CDMA code. Both receivers receive the 16 mini-slotted bits in the combined channel, that is, the sum of the mini-slotted bits sent by sender 1 and sender 2. These 16 bits are shown in the three leftmost grey-shaded boxes in the figure below (all three boxes contain this same 16-bit sequence). Perform the CDMA decoding operation for each receiver, that is, calculate the values of d_i^1 and d_i^2 shown in the figure below. This will show you that a receiver can indeed calculate the original bits sent by the sender in which it is interested.

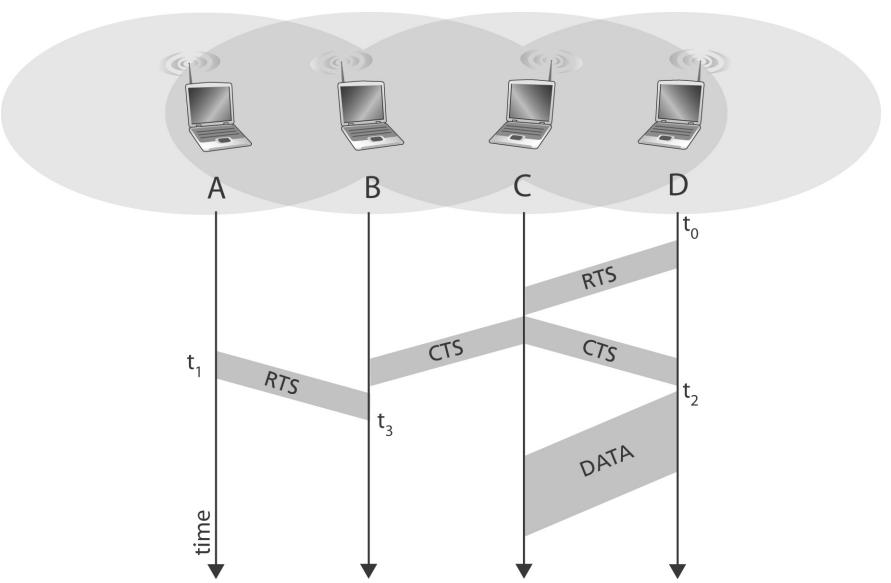


4. **Time-varying access point associations.** Consider the scenario described on page 516 of the textbook, in which you enter a Wi-Fi jungle in a café with your laptop, a blueberry muffin, and many Wi-Fi networks with which your laptop's wireless interface can associate. Suppose that your laptop associates with the access point with the strongest signal. Suppose also that the signal strengths of the access points vary over time, so your association will also change over time. We are interested in the effects of a changing link-level association, and the consequent change of IP address when an association changes.

   a. Suppose that initially your access point association changes relatively slowly over time, and that you are browsing the web using HTTP 1.0, and only occasionally downloading Web pages. Is the changing link-layer association and change of IP address likely to be a problem for you?

   b. Now suppose that you want to perform a file transfer over TCP that is so large that it is likely that your laptop's link-level association will change during the file transfer. Is the changing link-layer association and consequent change of IP address likely to be an issue for you?

5. **802.11 networks using different channels.** Let us return to Review Question 1. We learned on page 516 of the textbook that an 802.11 network can choose to operate using any of the 11 different available channels (frequency bands). Consider again the figure shown in Review Question 1. Can you assign channels to nodes such that the wireless network achieves the same throughput as in the wired case? (Note: you may assume that each node has two interfaces, with each interface having a different channel).
6. **802.11 ACK timeout values.** Certain 802.11 implementations use a fixed ACK timeout value, with a default value that is set for indoor (for example, less than 100 meters) communication. The timeout value determines the amount of time that the 802.11 sender will wait for an ACK frame after sending a DATA frame. If the ACK does not arrive within this amount of time, the DATA frame is assumed to be lost, and the DATA frame will be retransmitted. Suppose we want to use 802.11 with an outdoor, long-distance directional antenna that can transmit over a distance of say, 5 miles. What do you think will happen if the ACK timeout value remains set for the 100 m indoor case?
7. **RTS/CTS.** Consider the scenario shown below, in which node D sends an RTS to node C at t_0. Node C responds to the RTS with a CTS (which is heard by nodes B and C) in accordance with 802.11 protocol, and node D begins the transmission of its message at t_2. In the meantime, node A sends an RTS message to B at time t_1.



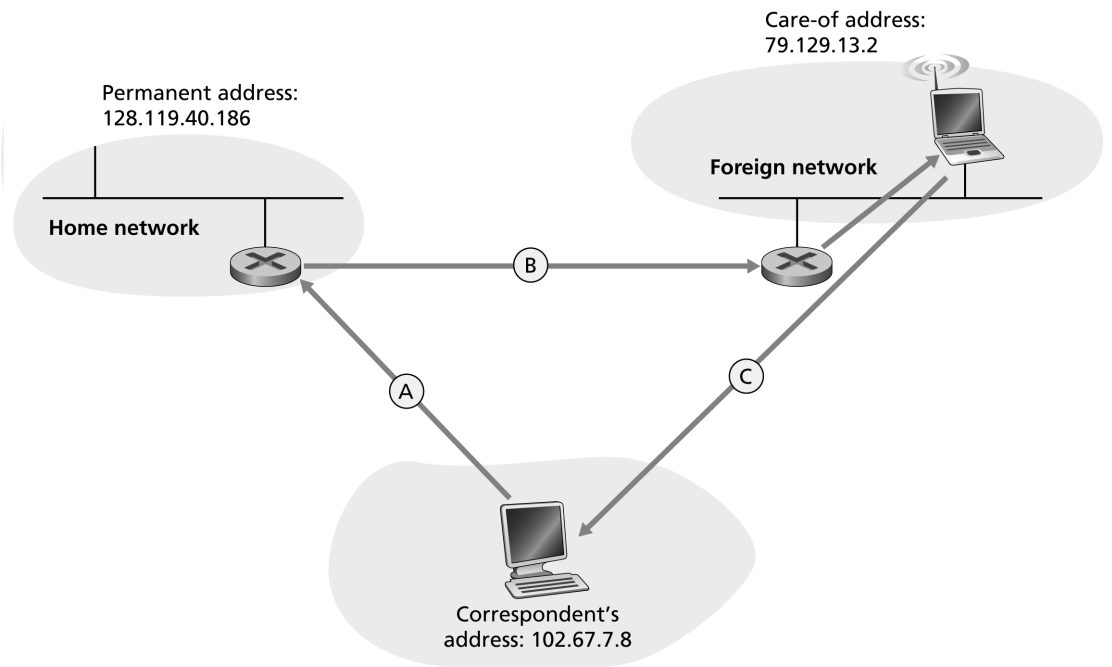
a. If node A were to begin transmitting to node B at some point after t_3, would A's transmission be successfully received at B?

b. If node A were to begin transmitting to node B at some point after t_3, would A's transmission interfere with the ongoing transmission from D-to-C?

c. At t_3, can B respond to A's RTS message with a CTS message? Why or why not?

8. **DIFS and SIFS timing in 802.11.** The SIFS is the amount of time that a node waits between receiving a DATA frame and sending an ACK. The DIFS is the amount of time that a node waits (sensing the medium) before sending a new DATA frame. Why do you think that the designers of 802.11 made the SIFS shorter than the DIFS?

9. **Mobile IP: indirection and encapsulation.** Consider the scenario below in which a mobile node whose permanent address in its home network is 128.119.40.186, is visiting a foreign network and has received a care-of-address of 79.129.13.2. A correspondent with address 102.67.7.8 sends a UDP segment to the mobile host using Mobile IP. Consider the IP datagrams A, B, and C. What are the source and destination IP addresses of these datagrams? Also, describe the contents of the payload (data) part of these IP datagrams.



10. **Packet loss during handoff.** Consider the mobile IP scenario in Review Question 9. The round trip time (RTT) between the correspondent and the home network is 1000 ms; the RTT between the home network and the foreign network is 120 ms. There is also a second foreign network (not shown in the figure above) that has an RTT from the home network of 160 ms. You may assume that all delays are fixed, and that the one-way delays between two points is equal to one-half the RTT. The correspondent is sending datagrams to the mobile hosts at a rate of one packet every 100 ms, periodically, and has been sending such datagrams for a long time (that is, long before $t = 0$). Suppose that the home network receives datagrams from the correspondent at $t = 0$, 100, 200, 300, and so on. At $t = 100$, the mobile node leaves the first foreign network and 500 msec later joins the second foreign network.

    a. Suppose that the mobile node leaves the first foreign network without signaling this to the foreign agent, and then joins the second foreign network, at which time the mobile IP registration process begins between the foreign agent in the new network and the home agent. Are any of the datagrams being relayed by the home agent to the mobile node lost during the mobile node's transition between foreign networks? Explain.

    b. Suppose now that the RTT delay between the home network and each of the foreign networks is doubled. How many datagram will be lost?

    c. Suppose that the RTTs between the home and foreign networks are the same as in the initial problem statement. Now suppose that the delay between the correspondent and the home network is doubled. How many datagrams will be lost?

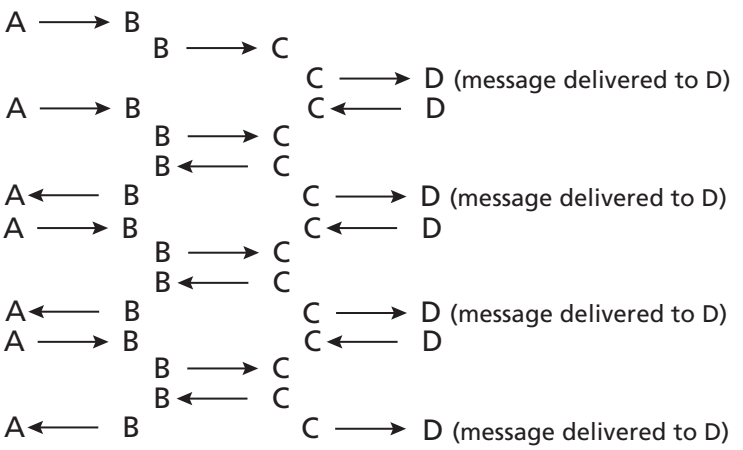
    d. Now suppose that when the mobile node leaves the initial foreign network at $t = 100$, it informs the foreign agent in this original foreign network. This foreign agent then informs the home agent that the mobile node is leaving the foreign network and that it (the home agent) should buffer any packets it receives from the correspondent until a registration is received from a new foreign agent, at which point the buffered packets can be sent to the mobile host in the new foreign network. In this scenario, (i) how many packets are lost, assuming that once a packet is sent, it can not be retransmitted, and (ii) how many packets are buffered at the home agent?

Answers to Review Questions

1. a. Note that A must send to B, B must send to C, and C must send to D. Also note that C's transmissions to D are heard by B, and thus B cannot receive from A (nor can B send to C) while C is transmitting to D, since A's and C's message would interfere at B. Similarly, neither A nor C can transmit when B is transmitting. Thus, only one node can ever be transmitting during a time slot. Since each message must be transmitted over three hops (A-B, B-C, and C-D), the maximum rate at which messages can be transmitted from A to D is one message every three time slots, or 0.3333 messages/slot.

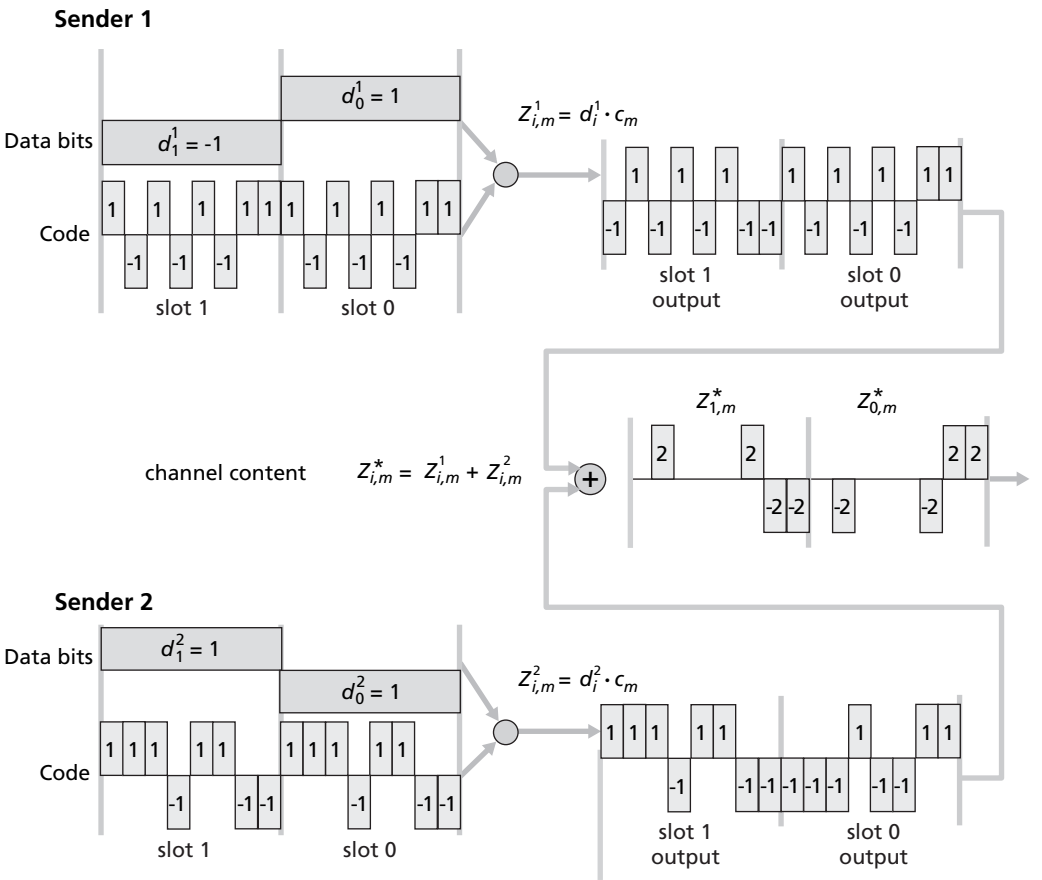
   b. Message transmissions can now be pipelined, while A is sending to B, B can be sending to C, and C can be sending to D. The maximum rate is thus one message/slot (three times the throughput of the wireless scenario!).

   c. Consider the following sequence of transmissions, in which data message flow from left to right, and ACK messages flow from right to left. Each line below shows the transmission activity during a time slot.

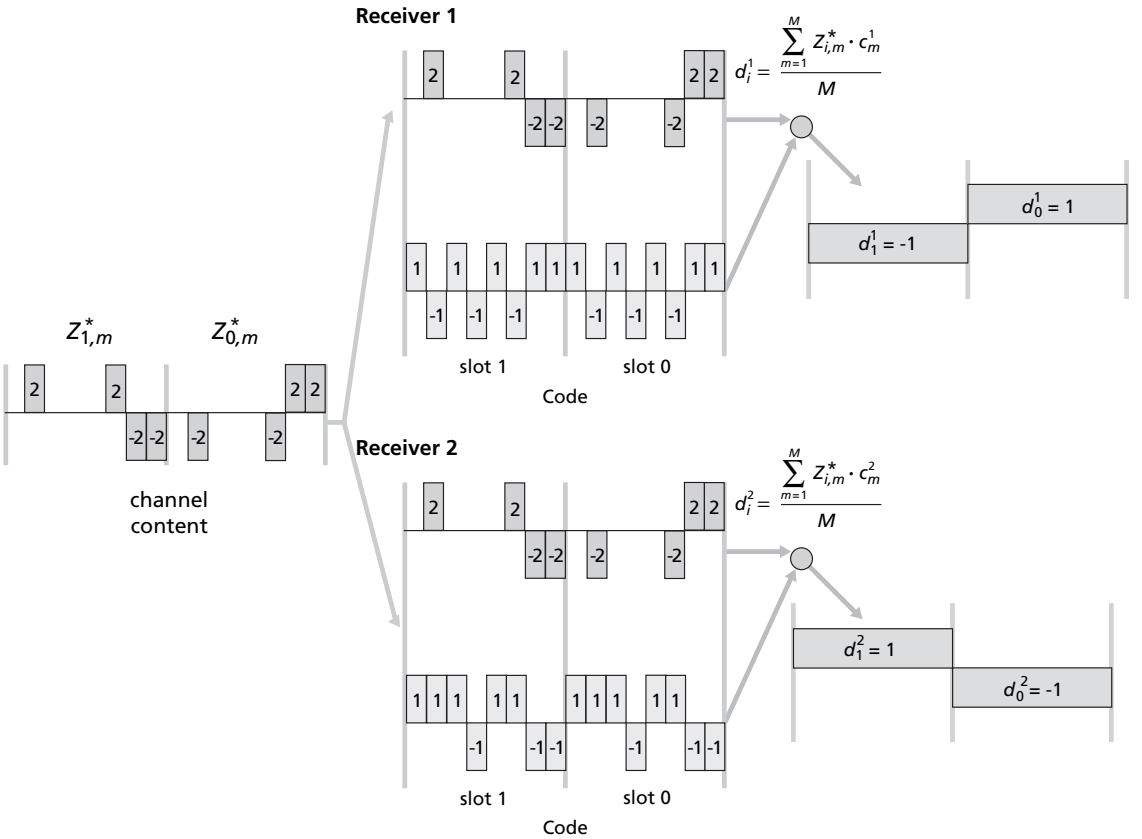


   Note that here we are able to take advantage of spatial reuse of the wireless channel: A can send a data message to B at the same time that an ACK is being sent to from D to C. Similarly, C can send a data message to D at the same time that B is sending an ACK message to A. The throughput is thus one message every four slots, or 0.25 messages/slot.

2.


Sender 1
Data bits
Code
slot 1
slot 0
slot 1 output
slot 0 output
channel content
Sender 2
Data bits
Code
slot 1
slot 0
slot 1 output
slot 0 output

3.



4. a. Recall that HTTP 1.0 Web transfers are transaction-oriented and non-persistent. Thus, as long as your link layer association does not change while you are downloading a page, the changing link-layer association will not be visible to your web browser application.

   b. If your laptop's link-layer association changes, your laptop will need an IP address in the network associated with the new access point. This network is likely to be different from the network associated with the old access point. Thus, your IP address is likely to change, and you will no longer be receiving datagrams sent to your old IP address. If a file transfer is in progress when your link-layer association changes, the file transfer will eventually abort because the underlying TCP sender will no longer receive ACKs from your laptop, once your laptop joins the new network and discards its old IP address.

5. Let us assign 802.11 channel 1 to node A, channel 6 to node B, and channel 11 to node C. Node A will send on channel 1; node B will receive on channel 1 and send on channel 6; node C will listen on channel 6, and send on channel 11; and node D will listen on channel 11. In this case, the channels do not interfere with each other, and messages can be transmitted simultaneously on any of the channels. In this case, the 802.11 network achieves the same throughput as in the wired case.
6. If the ACK timeout value is set too short, the sender will timeout prematurely, before an ACK has a chance to propagate back to the sender. In this case, the sender may retry its transmission (thereby interfering with the returning ACK), or simply ignore the late-arriving ACK. One of the authors actually learned this lesson the hard way, when working with a class of undergraduates on outdoor 802.11 networks. See http://madwifi.org/wiki/UserDocs/LongDistance for an interesting discussion of 802.11 issues over long distance links.
7. a. Yes. A's message would be received successfully at B since D's transmission does not reach B.
   b. No. A's transmission would not interfere with D's transmission at C, since A's transmission does not reach C.
   c. No. B cannot respond to A's RTS. When B receives the CTS from C, it (B) must defer its transmission until after the DATA frame sent by D and the ACK message (not shown) sent by C have been sent. Thus, B cannot respond to A's RTS and thus, A cannot send, even though its message transmission would be correctly received at B and would not interfere with the transmission from D to C.
8. Suppose at any given time, a node has a new DATA frame to send and begins waiting for DIFS time units. At the same time, a nearby node has just successfully received a DATA frame. In this case, the latter node will transmit its ACK after waiting only SIFS time units, that is, before the node with the new DATA frame begins its transmission of its DATA frame. Thus, the smaller value of SIFS gives priority to nodes wanting to send an ACK over nodes wanting to send a new DATA frame.
9. • Datagram A has source address of 102.67.7.8 and a destination address of 128.119.40.186. The payload of datagram A is the UDP segment being sent from the correspondent to the mobile host.
   • Datagram B has a source address of the IP address of the home agent, and a destination address of 79.129.13.2 The payload of datagram B is datagram A.
   • Datagram C has a source address of 79.129.13.2, and a destination address of 102.67.7.8. The payload of datagram C is whatever reply the mobile host sends to the correspondent.

10. a. The mobile arrives at the foreign network at t = 600 msec and immediately registers with the foreign agent who then immediately sends a new registration to the home agent. This registration arrives at the home agent at t = 680 msec. When the next datagram arrives from the correspondent at t = 700, the home agent will then relay this to the mobile in the new foreign network. The datagrams sent at t = 100, 200, 300, 400, 500, and 600 will have been sent to the original foreign network. The mobile node will have already left the foreign network when these datagrams arrive, and so these six datagrams will be lost.

    b. In this case, the registration message from the new foreign network arrives at the home agent at t = 760, and so seven messages will have been sent to the old foreign network, and hence, lost.

    c. Trick question! The answer is six, following exactly the same reasoning as in 10(a). Note that even with an increase in delay between the correspondent and the home network, datagrams will still be arriving at t = 100, 200, 300, 400, 500, 600, and so on.

    d. The de-registration message arrives at the home network at t = 180 msec, and so the datagram sent at t = 100 will be lost. The home agent will buffer the packets arriving from the correspondent at t = 200, 300, 400, 500, and 600 and forward these to the mobile host when it (the home agent) receives the new registration at t = 680 msec. Thus, one datagram is lost, and five are buffered and eventually sent.