Computer Networks
Jacobs University Bremen
Dr. Jürgen Schönwälder

Course: 320301
Date: 2013-10-31
Deadline: 2013-11-06

Problem Sheet #4

Problem 4.1: *IEEE 802.11 wireless networks* (1+1+2+2+2+2 = 10 points)

Please read about IEEE 802.11 wireless networks and answer the following questions. Some questions refer to the packet trace available from http://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=get&target=mesh.pcap

a) What is the purpose of the RTS and CTS frames? When are they used?

b) Why are link-layer acknowledgements used in IEEE 802.11 wireless networks but not in IEEE 802.3 wired Ethernet networks?

c) The IEEE 802.11 frame format includes a `duration` field. What is the purpose of the `duration` field?

d) Explain the terms BSS, BSSID, SSID, ESS and ESSID (in infrastructure mode) and how they relate to each other.

e) How are IP packets encapsulated in IEEE 802.11 wireless frames? (You may look into the packet trace to find the answer.)

f) Load the packet trace into `wireshark`. How can you filter out all beacon management frames? How many wireless BSSs are sending beacons? What are their BSSIDs and SSIDs? Which wireless channels are used?

Solution:

a) The Request to Send (RTS) and Clear To Send (CTS) frames can be used to reduce collisions. A station wishing to send data first sends an RTS frame. The receiver replies with a CTS frame before the data frame transmission starts. An RTS / CTS exchange makes sense in order to guard a transmission of a "long" data frame; it is not useful for small data frames. The RTSThreshold parameter controls what a "long" frame is.

b) The likelihood to loose a frame is significantly higher in wireless networks due to the changing properties of the wireless channel and the fact that stations may be mobile. Hence, it is essential to be able to deal with frame losses at the link-layer in order to be efficient. In wired networks, frame losses are rare events and hence the handling of frame losses can be deferred to higher protocol layers.

c) The duration field reserves the channel for the transmission of a data frame and its acknowledgement. The sender first calculates the time needed for the whole exchange and sends the duration as part of the RTS request. If the access point sends a CTS, the duration included determines the time during which the channel is reserved. Upon receiving the CTS, the sender sends the data frame which may be followed by an acknowledgement.

d) The Basic Service Set (BSS) is a single access point and all associated stations. The Basic Service Set Identification (BSSID) (in infrastructure mode) is essentially the MAC address of the access point and uniquely identifying the BSS. The Service Set Identifier (SSID) is a human readable string identifying a BSS. A Extended Service Set (ESS) is a collection of interconnected BSSs sharing the same SSID. The common SSID used by an ESS is also called an ESSID.

e) IP packets are encapsulated in a Logical Link Control (LLC) header. More precisely, the IEEE 802.11 frame header header is followed by an LLC header which is followup by a SNAP header. The LLC header contains the Service Access Point (SAP) of the source and the destination (each one octet) and the LLC control octet. The SNAP header contains on Organizational Unit Identifier (OUI) (3 octets) and a Type field (2 octets). The Type field value 0x0800 for the OUI value 0x000000 indicates that the following header is an IPv4 header.

f) Beacon frames can be selected by using the filter `wlan.fc.type_subtype == 0x08`.

	Access Point #1	Access Point #2
BSSID	06:03:7f:07:a0:16	00:00:00:00:00:00
SSID	freebsd-ap	Broadcast
Channel	36	36
Frequency	5180 MHz	5180 MHz