

Security Topics in Networking and Distributed Systems

CS 590D

Lecture 15: 802.11 Denial of Service

Department of Computer Sciences
Purdue University

References

- 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions John Bellardo and Stefan Savage. USENIX 2003



802.11 Services

- Station Services – similar to those in a wired network.
 - Data Delivery
 - Authentication
 - Privacy
- Distribution Services – enables a node to roam between several base stations
 - Association
 - Reassociation
 - Disassociation
 - Integration

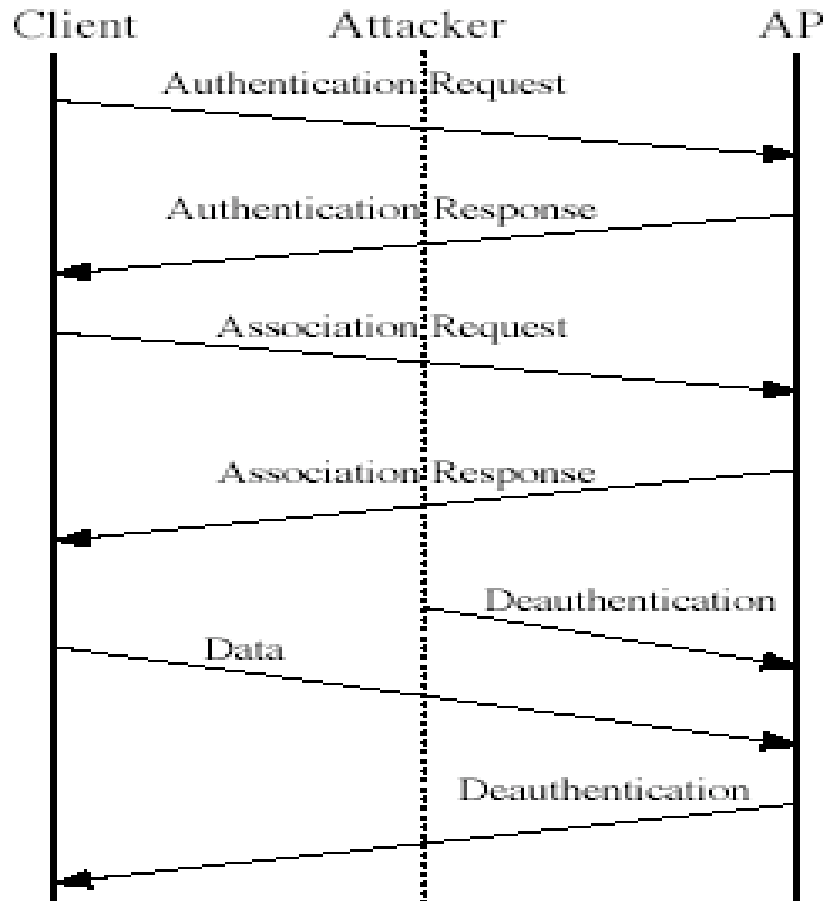
802.11 Type of Frames

- Management frame:
 - authentication of a wireless client to a base station (authentication/deauthentication)
 - when more than one base station present the station authenticates itself to all of them, but only one base station will forward packets to/from wired network (association/disassociation)
- Control frames:
 - power save: TIM, Poll
 - RTS/CTS (reserve the channel)
- Data frames

Authentication/Deauthentication Association/Dissociation

- Clients can explicitly ask for deauthentication from a base station
- Base station can send an deauthentication message to a client
- Similarly a client can ask for dissociation from a base station
- All these messages are not authenticated, so anybody can inject packets
- Question: How easy is to do that?

Deauthentication Attack



- An attacker can deny access to individual clients, or rate limit their access

Figure 1: Graphical depiction of the deauthentication attack. Note that the attacker needs only generate one packet for every six exchanged between the client and access point.

Association/Dissociation Attacks

- Similar with deauthentication, an attacker can pretend that he is a base station and send a disassociation message.
- Less impact than the deauthentication attack because for a client is less costly to associate again with a base station as opposed to authenticate again

Countermeasures?

- Non-cryptographic, non-invasive methods (WHY?)
- For a successful attack, deauthentication message must be sent after authentication was established (monitor for authentication message)
- Delay the effects of deauthentication/dissociation requests (queuing), then observe traffic from the client; if data comes, then the request must have been spoofed

Power Management

- Allow idle station to go to sleep (save battery)
- Wireless station announces when it goes to sleep
- Base station starts buffering packets for the sleeping node
- Periodically the base station broadcasts (traffic indication map) TIM indicating that there are buffered packets
- Wireless station can also wake up and poll the base station to see if there are buffered packets
- Relies on time synchronization mechanisms between the base station and the wireless stations (TIM period and timestamp also sent in clear)

Power Management (cont.)

- Broadcast/multicast frames are also buffered at the base station and sent at a different time calls DTIM (delivery traffic indication map) also periodically broadcast
- Power Saving stations wake up prior to expected DTIM
- If TIM indicates frame buffered the wireless station sends PS-Poll and stays awake to receive data else the station sleeps again

Power Saving Attacks

- An attacker impersonates a wireless station that is asleep and pretends that is awake
- The base station will send all the buffered frames, that will be lost
- An attacker impersonates a base station and sends spoofed TIM making it believe that there are no packets buffered for it
- An attacker can send corrupted TIM period to the wireless station making it keep sleeping or desynchronized.
- Countermeasures?

802.11 Medium Access

- Two mechanisms for channel access
 - Distributed Coordination Function (DCF), mandatory
 - Point Coordination Function (PCF), optional, used only in infrastructure mode
- DCF is a Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol
- Why “collision avoidance” ?

Collision Detection

- Every node listens, if channel free, then send
- If “collide”, they retransmit at random times (exponential back-off)
- Collisions may still exist, since two stations may sense the channel idle at the same time
- In case of collision, the entire packet transmission time is wasted
- Random access MAC protocols: ALOHA, SLOTTED ALOHA, CSMA and CSMA/CD (used by Ethernet)

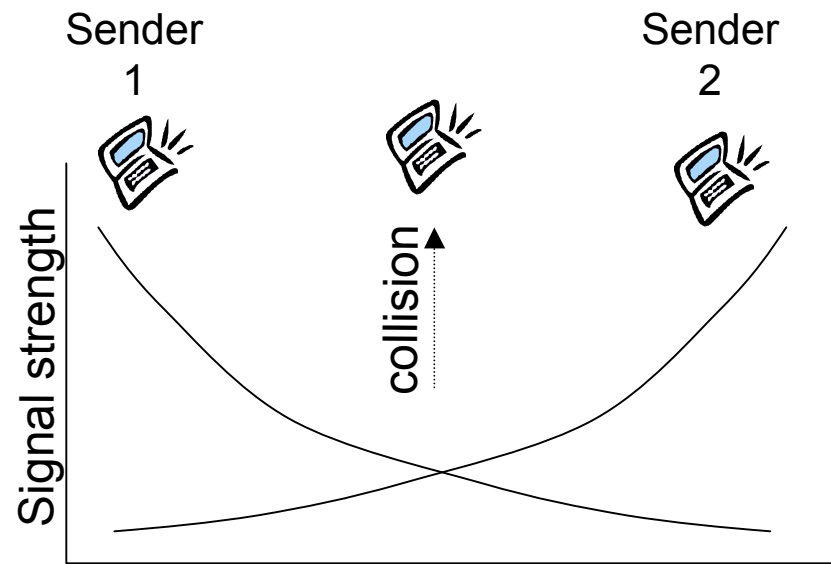
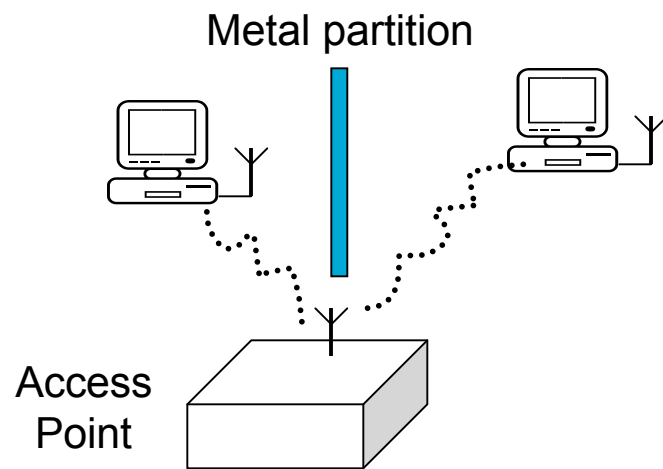
Collision Avoidance

- Collision detection is very difficult (in some cases impossible) in wireless. Transmitters don't reliably know if there is a collision at the receiver.
- Collision detection does not work well for wireless
 - multipath fading of a radio signal: small time delays can occur in radio signals, as results the quality of the signal at the receiver will be degraded (weaker).
 - Hidden terminal: Two or more senders might not receive from each other.

COLLISION AVOIDANCE !

Hidden Terminal

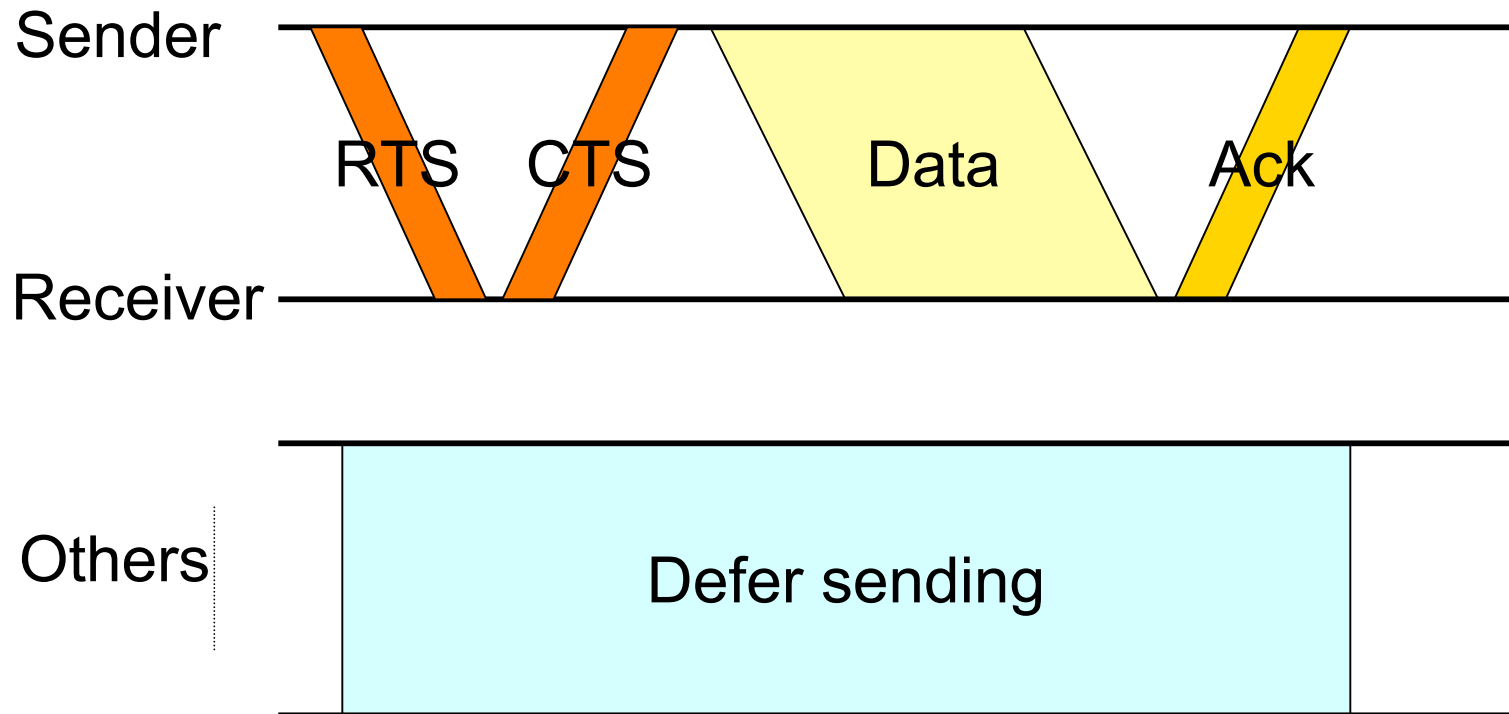
Hidden Terminal:



CSMA/CA: Collision Avoidance

- Listens to see if medium is idle (“carrier sense”).
- If idle, wait an *additional* random backoff time.
- If line is still idle, transmit.
- Wait for receiver acknowledgement.
- Retransmit if necessary.
- Additional RTS/CTS to reserve the channel, and the size of the data to let other know how long the channel will be busy

RTS/CTS Mechanism



RTS/CTS is optional in 802.11b

Virtual Carrier Sensing

- RTS/CTS contain duration of data transfer + Ack
- Virtual Carrier Sensing: Nodes overhearing RTS/CTS stay silent for specified duration (stored in Network Allocation Vector NAV)
- Interframe intervals used as a priority mechanism: four types SIFS, PIFS, DIFS, EIFS; Attack can exploit SIFS/DIFS



Media Access Attacks

- Packet sending to the media is not authenticated in 802.11.
- Sending packet within each SIFS (20 microseconds) to compete for the media; requires the attacker to “work hard” to block the channel: sending 50,000 packets/second,
- Virtual Carrier-Sense attack: Sending out packets with large NAV, since maximum value for NAV is 32 milliseconds, attacker needs to send 30 times/second to block the channel

Practicality of the Attacks

- A wide variety of 802.11 cards do not typically allow the generation of any control frames, permit other key fields (such as NAV) to be specified by the host, or allow reserved or illegal field values to be transmitted.
- Software-based method to modify headers of frames by exploiting a debugging feature (auxiliary port)

Defense to Virtual Carrier-Sense Attack

- For four key frame types contains NAV:
 - ACK and Data frame: ignore NAV since there is no fragmentation.
 - RTS frame NAV: respected until such time as a data frame should be sent.
 - CTS frame NAV: specify some threshold (30%) if such time is used by CTS frame then ignore NAV.

Summary

- Authentication/Deauthentication and association/disassociation packets not authenticated, anybody can inject
- Software-based attack was successfully conducted
- Exploit the RTS/CTS mechanism to conduct carrier sense attack
- Low-overhead, non-cryptographic
- countermeasures are suggested

