Securing Wireless LANs: Part 7

Gaurav S. Kasbekar
Dept. of Electrical Engineering
IIT Bombay

References

- J. Edney, W.A. Arbaugh, "*Real 802.11 Security: Wi-Fi Protected Access and 802.11i*", Pearson Education, 2004.
- J. Bellardo, S. Savage, "802.11 Denial-Of-Service attacks: Real Vulnerabilities and Practical Solutions," In *Proceedings of the 12th conference on USENIX Security Symposium*– Volume12, Pages 15-28, 2003.
- M.S. Ahmad, S. Tadakamadla. "Short paper: security evaluation of IEEE 802.11 w specification", in *Proceedings of the fourth ACM conference on Wireless network security*, pp. 53-58, 2011.
- Wikipedia article on 802.11w:
  - https://en.wikipedia.org/wiki/IEEE_802.11w-2009

802.11w for Management Frame Security

Motivation

- Recall: 802.11i includes several mechanisms for achieving authentication, confidentiality and message integrity of data frames
- However, apart from data frames, other frames called "*management frames*" are exchanged, e.g.:
  - beacons, authentication request and response frames, association request and response frames, disassociation frames, deauthentication frames
- Traditionally, management frames did not contain sensitive information and did not need protection
  - so 802.11i did not provide encryption and message integrity for management frames
- However with the addition of new features to the 802.11 standard, new and highly sensitive information started being exchanged in management frames
  - e.g., new fast handoff, radio resource measurement, discovery and wireless network management schemes (provided in 802.11r, 802.11k and 802.11v)
  - details omitted
- Also, networks that used 802.11i were shown to be vulnerable to several Denial-of-Service (DoS) attacks, which were possible because management frames were not protected
  - such attacks prevent legitimate users from accessing the network
- For above reasons, a new amendment to the 802.11 standard was approved in 2009 to incorporate security mechanisms in its management frames
  - called *802.11w*

802.11 Management Frames

- E.g. of 802.11 management frames:
  - Beacon
  - Probe request and response
  - Authenticate request and response
  - Associate request and response
  - Disassociate
  - Deauthenticate
- Beacon:
  - periodically sent by an AP to communicate throughout its range, the characteristics of the connections it offers to its associated clients
  - one beacon is sent every 102.4 milliseconds
  - beacon contains list of data rates supported by AP, list of authentication, encryption and message integrity protocols supported by the AP and many other fields
- When a user arrives into an area and switches on his/ her mobile device with Wi-Fi:
  - it scans different channels and receives beacons sent by different APs present in the area
  - list of Wi-Fi networks present in the area provided to user, who can then select a network he/ she wants to connect to

802.11 Management Frames (contd.)

- Above described process of discovering the network by scanning all possible channels and listening to beacons (called *passive scanning*) is not considered to be very efficient
- To speed up the discovery process, stations often use what is called *active scanning*
- In active scanning:
  - stations still go through each channel in turn,
  - but instead of passively listening to the signals on that channel, station send a "*Probe Request*" management frame asking what networks are available on that channel
  - Probe Requests are broadcast packets
- When an AP receives a Probe Request packet from a station, it sends a *Probe Response* packet to the station, which contains the characteristics of the connections it offers to its associated devices
  - Probe Response similar to Beacon, but there are some differences
- Once a Probe Request is sent, station starts a ProbeTimer countdown and waits for answers
  - at the end of the timer, station processes the answers it has received

802.11 Management Frames (contd.)

- Authentication request/ response frames
  - after receiving beacon or probe response frame from AP, authentication request frame is sent by station to AP, which contains the station's MAC address
  - next, an authentication response is sent by AP to station, which contains a success or failure message
- Purpose of above initial authentication request/ response exchange is to allow the AP to verify that the station is a valid 802.11 device
  - *no security-related exchanges are done in the above authentication request/ response frames*
- 802.11 standard allows a client to be authenticated with multiple APs at once,
  - so the standard provides association messages to allow the client and AP to agree as to which AP shall have responsibility for forwarding packets to and from the wired network on the client's behalf
- Once the station determines which AP it would like to associate to, it sends an *association request* frame to that AP
  - contains chosen encryption type and other compatible 802.11 capabilities
- If the elements of association request match the capabilities of the AP, it creates an Association ID for the station and responds with an *association response* frame with a success message granting network access to the station
- After association response is sent, security validation takes place
  - at this stage, the EAP and the four-way handshake, which we discussed earlier, take place

802.11 Management Frames (contd.)

- Once a station is associated to an AP, either side can terminate the association at any time by sending a *disassociation frame*
  - a station often sends a disassociation frame when it leaves the current AP to roam to the range of another AP
  - an AP sends disassociation frame if station uses some invalid parameters
- Station or AP can send a *deauthentication frame* at any time
  - typically sent when all communications are terminated
  - note that even when disassociated, a station can be authenticated to the AP