Network Security

Professor Gaurav S. Kasbekar
Department of Electrical Engineering
Indian Institute of Technology, Bombay

Week - 07
Lecture - 41
Securing Wireless LANs : Part 7

Hello, in this lecture, we'll continue our discussion on securing wireless local area networks. So, in the previous lectures, we discussed how authentication is performed between an access point and a mobile station, and also how they can securely communicate data frames, including confidentiality and message integrity. We discussed TKIP and CCMP. CCMP is the protocol used in 802.11i, and it can be used to provide security for the data frames that are exchanged. There is another kind of frame in Wi-Fi, namely management frames.

So, now we'll discuss the security of management frames. So, there is a standard called 802.11w for management frame security. First, we'll discuss what is meant by management frames, and then we'll discuss 802.11w for securing these management frames. So, recall that 802.11i, which we discussed earlier, includes several mechanisms for achieving authentication between the access point and mobile device, as well as confidentiality and message integrity of data frames. However, data frames are not the only ones that are exchanged.

Apart from data frames, other frames called management frames are exchanged from time to time. Examples are beacons, authentication request and response, association request, association response, disassociation frames, and deauthentication frames. We'll discuss the functions of these different kinds of frames. So, all these are examples of management frames. They don't contain any data, but they perform different functions.

For example, associating a mobile device with an access point or disassociating a mobile device from an access point, and so on. So, traditionally, management frames did not contain any sensitive information and did not need protection. So, that was the reason that when 802.11i was introduced in 2004, it did not provide encryption and message integrity for management frames. It only provided encryption and message integrity for data frames.

But as new features were added to the 802.11 standard, new and highly sensitive information started being exchanged even in management frames.

Some examples are as follows: So, handoff is the function where a mobile device that is initially communicating with an access point. Later on, it can move to the range of another access point. In that case, the mobile device needs to be handed off from the first access point to the second access point. So, this is known as handoff.

There is a functionality called fast handoff. Other functionalities are radio resource measurement, discovery, and wireless network management schemes. So, these are provided in all these standards: 802.11r, 802.11k, and 802.11v. Recall that 802.11, which is the standard on which Wi-Fi is based, has several amendments and versions which are named by alphabets. For example, 802.11a, 802.11b, g, ac, and so on.

So, for example, 802.11n is the standard that introduced MIMO, multiple input, multiple output, which uses multiple antennas at the transmitter and receiver. 802.11ac is also known as Wi-Fi 5, and 802.11ax is also known as Wi-Fi 6. So, similarly, there are all these versions of Wi-Fi 802.11r, 802.11k, and 802.11v, which provide all these functions. New fast hand-off, radio resource management, and discovery and wireless network management schemes. So, with these features, highly sensitive information is exchanged even in management frames.

We omit the details because these are not related to security. But we just need to note that because of the introduction of these features, even in management frames, sensitive information was exchanged, and hence they need protection as well. Also, networks that used 802.11i were shown to be vulnerable to several Denial of Service (DoS) attacks, and these were possible because management frames were not protected. We'll discuss some examples of these DoS attacks. We'll show how these are possible when management frames are not protected.

Such DoS attacks prevent legitimate users from accessing the network. One example is an attacker may repeatedly send deauthentication frames, which deauthenticate the mobile from the access point. So, the legitimate mobile device is not able to communicate with the access point. So, that results in denial of service to the mobile. So, because of this vulnerability, management frames needed to be protected as well.

So, for all these reasons, a new amendment to the 802.11 standard was approved in 2009 to incorporate security mechanisms into its management frames. This new amendment

incorporated security mechanisms into its management frames. This was in addition to 802.11i, which already provided security mechanisms in the data frames. So, this new amendment was known as 802.11w. So, this amendment incorporated security mechanisms into the management frames of 802.11.

So, let's discuss several examples of management frames to understand what kind of functions they perform. So, some examples of 802.11 management frames are as follows. One example is the beacon, which is a very important kind of frame, then probe request and response, authenticate request, authenticate response, associate request, associate response, disassociate, and deauthenticate. All these are examples of management frames. So, let's discuss the beacon in some detail.

In every Wi-Fi network, the access point periodically sends beacon frames. These are communicated throughout the range of the access point. And this beacon contains the characteristics of the connections that the access point offers to its associated clients. So, for example, one beacon is sent every 102.4 milliseconds. So, roughly 10 beacons are sent every second.

And examples of the information that is contained in beacons are as follows: The beacon contains the list of data rates supported by the access point. For example, 11 Mbps or 300 Mbps, and so on. So, what are the data rates that are supported by the access point? And the list of the authentication, encryption, and message integrity protocols that are supported by the access point, and many other fields.

Another example is the name of the network. So, the name of the network is also included in the beacon. This beacon contains all this information about the characteristics of the connections that the access point offers to its associated clients. And when a user arrives in an area and switches on his or her mobile device with Wi-Fi, the mobile device scans different channels and receives beacons sent by different access points present in the area. So, consider a user who moves into a particular campus.

So, the user arrives in a campus, and there are many access points in the campus network. So, when the user switches on their mobile device, the mobile device scans different channels. What is meant by scanning? So, Wi-Fi access points can operate on one of many possible frequency channels. By scanning, we mean that the mobile device first tunes to the first of these channels and receives frames on that channel for some time.

So, the mobile device listens on the channel for some time and gathers all the beacon frames that are transmitted on the channel. So, after scanning a particular channel for about 100 milliseconds, or slightly more than 100 milliseconds, it gathers all the beacons that are sent on the channel. And then it moves to the next channel and again receives frames on that next channel for about 100 milliseconds or so, gathering all the beacons that are sent on that channel, and so on and so forth. So, one by one, it tunes to every channel on which an access point may be present and gathers the beacons that are sent by access points on different channels. So, this way, the mobile device gets a list of all the access points that are present in the area.

This list is inferred from the beacons that are sent by the access points. So, notice that since one beacon is sent every 102.4 milliseconds, if a mobile device listens on a particular channel for slightly more than 102.4 milliseconds, then it will get at least one beacon. So, this way, it can get beacons from all the access points that are operating in that area. So, after scanning, this list of Wi-Fi networks that are present in the area is provided to the user. This process is familiar to us.

So, as soon as we switch on Wi-Fi, the mobile device scans the area for the available networks and shows us a list of Wi-Fi networks that are present in the area. And then the user can select the network that they want to connect to. So, this scanning is possible because beacons are sent periodically by access points. So, we see the function of one kind of management frame, namely beacons. It is useful for scanning and finding networks, as well as what are the characteristics of the network of this particular access point.

So, the process that we just described of discovering the network by scanning all possible channels and listening to beacons, this is called passive scanning, and this is not considered to be very efficient because a mobile device has to listen to a channel for a long time before it can get beacons. There is also a more efficient process for discovering networks, and that is known as active scanning. So, to speed up the discovery process, stations often use what is called active scanning. So, in active scanning, stations still go through each channel in turn. So, they first tune to the first channel and then tune to the second channel, and so on.

But on a particular channel, a mobile device doesn't just listen to the channel. Instead of passively listening to the signals on that channel, the station sends a management frame called a probe request management frame. And this frame is used to ask what networks are available on that channel. And these probe requests are broadcast packets, meaning they are sent to all the nodes that are tuned to that channel. So, this probe request packet sent by

a mobile device has the function of asking access points in the vicinity which networks are present on that channel.

When an access point receives a probe request packet from a station, the access point sends a probe response packet to the station, which contains the characteristics of the connections that it offers to its associated devices. So, this probe response packet is similar to a beacon in the sense that it contains the characteristics of the connections that the access point offers to its associated devices, such as a list of data rates, types of authentication, encryption, and message integrity that are supported, and so on. But there are some differences between a probe response and a beacon. So, this process of active scanning is faster than the process of passive scanning because a mobile device can tune to a particular channel and just directly send the probe request frame, and immediately it will get probe responses from all the access points that are tuned to that channel, and these probe responses have all the information about the characteristics of the connections that these access points offer to their clients. So, the mobile device does not have to wait for the next beacon; instead, it can immediately send the probe request management frame and get probe response packets.

Once a probe request is sent, the station starts a timer called the probe timer, counts down, and waits for responses. So, at the end of the timer, when the timer expires, the station stops listening to the channel and stores the list of networks it has found from the probe response frames it has gathered. So, at the end of the timer, the station processes the responses it has received, that is, the probe response packets it has received. So, from these probe response packets, as we said, the station gets to know which networks are present in the area and what are the characteristics. So, probe request and probe response packets are other examples of management frames.

So, we have discussed three examples of management frames: beacons, probe requests, and probe responses. Another set of management frames is authentication request and authentication response frames. After receiving a beacon or a probe response frame from an access point, an authentication request frame is sent by the station to the access point, and this authentication request frame contains the station's MAC address. Next, an authentication response is sent by the access point to the station, which contains a success or failure message. So, what is the purpose of these frames—authentication request and authentication response frames?

The purpose of this initial authentication request-response exchange is to allow the access point to verify that the station is a valid 802.11 device. For example, it sends packets

correctly with the correct format and with the correct timing requirements. For example, the amount of time it must wait before sending a packet and the format of the packet it sends, and so on. So, these are correct, and they conform to the 802.11 standard. So, that is what these authentication request and response exchanges verify.

It is important to note that no security-related exchanges are done in these authentication request and response frames. This is not the same authentication that we discussed earlier. So, in the security sense, authentication means that if Alice and Bob authenticate, then it means that Alice conveys to Bob that she is indeed Alice, and Bob conveys to Alice that he is indeed Bob. So, here we do not mean that authentication. So, here it is different; it has a different meaning.

It is just used to verify that the station is a valid 802.11 device. So, that is the function provided by the authentication request and response frames. And the 802.11 standard allows the client to be authenticated with multiple access points at once. So, apart from authentication, the standard provides association messages to allow the client and access point to agree on which access point shall have the responsibility for forwarding packets to and from the wired network on the client's behalf. So, consider an access point.

It is connected to the wired network. For example, the internet is over here. So, this is the internet. And a mobile device communicates with this access point. And there may be other access points in the area which are also connected to the internet.

So, out of these access points, which access point is responsible for forwarding the packets of the mobile device to the internet and sending packets from the internet to the mobile device? So, one of these access points is responsible for these functions, and that is the access point with which the mobile device is associated. So, suppose, for example, that the mobile device associates with this access point. In that case, the mobile device will communicate wirelessly with this access point, and this access point has the functions of forwarding the packets of this mobile device to the internet and sending packets from the internet to the mobile device. So, at any time, the mobile device is associated with only one access point.

Now, once the station determines which access point it would like to associate with, it sends an association request frame to that access point. So, this association request frame contains the chosen encryption type and other compatible 802.11 capabilities. If the elements of the association request match the capabilities of the access point, then the access point creates an association ID for the station and responds with an association

response frame with a success message granting network access to the station. So, for example, this access point may send an association response frame to this mobile. Subsequently, this mobile is associated with this access point.

After the association response is sent, security validation takes place. At this stage, the EAP and the four-way handshake, which we discussed earlier, take place at this stage. Authentication in the security sense is performed only at this point, after the association takes place. So, we have discussed four types of management frames on this slide. Authentication request, authentication response, association request, and association response.

So, to summarize, after a mobile device performs scanning, it authenticates itself with an access point. This is done through authentication request and authentication response frames. A mobile device may remain authenticated with multiple access points simultaneously. And it associates with only one of these access points. This association is done through the exchange of association request and association response frames.

All these are management frames. Once a station is associated to an access point, either side, that is, either the station or the access point, can terminate the association at any time by sending this association frame. This ends the process of association between the station and the access point. A station often sends a disassociation frame when it leaves the current AP to roam to the range of another access point. For example, the station may be earlier communicating with an access point A, say, then it moves outside the range of access point A, and then it moves to the range of another access point B. So while it is about to move out of the range of access point A, it sends a dissociation frame to access point A to end its association with access point A, and it associates with the other access point, access point B.

That is the function of the disassociation frame. An access point can also send a disassociation frame to the station. This typically happens when the station uses invalid parameters to communicate. In that case, the access point disassociates the station. This is another type of management frame, the disassociation frame, used to end the process of association.

The station or access point can send a deauthentication frame at any time, and this ends authentication as well. So, it is typically sent when all communications are terminated and the authentication has to be ended. Note that even when disassociated, a station can be

authenticated to the access point. So, first authentication takes place, and then association takes place. Consider a mobile device that is associated with an access point.

If a disassociation frame is sent by one of these parties, then the association will end, but the station will still remain authenticated. To end authentication, the station or the access point has to send a deauthentication frame. So, these two are other examples of management frames. One is a disassociation frame, and another is a deauthentication frame. So, in summary, we discussed management frames in 802.11.

We discussed different kinds of management frames which perform different functions. Examples are beacon frames, probe request, probe response, association request and association response, authentication request, authentication response, and disassociation and deauthenticate. So, we discussed the functions that these different frames perform. In the next lecture, we'll discuss the security aspects of management frames. In particular, how 802.11w provides security to management frames.

Thank you.