The IEE 802.11 standard comes with a type of packet called a deauthentication frame. This frame is used specifically to terminate a wireless connection using this standard. This frame can be sent both from the client and from the access point. One interesting thing about this frame is that the access point nor the client can refuse this frame. This means that by forcing an access point to send these frames to certain or all clients connected they will disconnect once received.

There is such a term called disassociation which would essentially leverage the exact same process as deauthentication. However, in a disassociation the client would be kicked off one access point, but another access point on the same network would pick up your client again. Essentially disassociating you from your current access point.

Demonstrated in labs and with tools that exist out there today spoofing these types of attacks is not difficult. The IEEE 802.11w standard was designed to include a feature called PMF or Protected Management Frames, which helps guard against deauthentication attacks. However, there are a great number of devices without this protection. Given the cost of upgrading a router with the newest standards and security features isn’t always affordable it’s up to vendors to get in touch with the users of devices and provide a path to upgrading and enabling these security features on older devices.

Protected Management Frames do more than protect against deauthentication and disassociation attacks. This also protects against ACK Request/Responses, Radio Measurement, Spectrum Management, and more. In addition, it will protect from Channel Switch Announcement directed at a client. This is done with several encryption mechanisms such as using the same PTK as for data frames, Separate Receive Sequence Counter (RSC), new algorithm for the broadcast integrity protocol, and more.

If an attacker attempts to associate with a spoofed MAC address of a client connected to an access point, then the access point will start a process called Security Association Query. This query is sent to the actual client which can return the correct response, so it ignores the spoofed associate attack.

From the research I’ve completed there is no similar attack against access points that have PMF enabled. Meaning there is a mitigation path forward for those devices susceptible to these attacks. I think the conclusion here is that this is a good way to protect against this type of attack now. However, as attackers evolve and so do the methods PMF may have flaws.

References

<https://www.itpro.com/security/cyber-attacks/wifi-network-attacks-the-risk-to-businesses>

<https://wlan1nde.wordpress.com/2014/10/21/protected-management-frames-802-11w/>

<https://blog.spacehuhn.com/wifi-deauthentication-frame>

<https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack>