**Wireless Denial of Service (WDoS) attack**

**Definition**

Today, a denial-of-service attack is considered an easy attack as the nature of wireless networks is that the medium is shared between the nodes in the network. The attacker achieves the denial of service (DOS) attack by blocking access to the medium by flooding the traffic with packets or by interfering with the network’s reception. The wireless DoS attacks can be classified into two categories [4]:

1. Physical layer attacks: these attacks target the reception process and the transmission communication of the network. It involves disturbing or interfering a legitimate communication. These are some examples of attacks that target the physical layer:

* Jamming attack:
* Deauthentication attack
* Beacon flooding attack

1. Protocol layer attacks: these attacks target the wireless network’s protocol layer. These attacks involve manipulating the communication between the client and the AP or disturbing the network communication. These are some examples that target the protocol layer of the network:

* Fragmentation attack
* ARP spoofing attack
* WPA/WPA2 cracking attack

**Mechanism**

A deauthentication attack is a kind of DoS attack that exploits the authentication WPA protocol by sending a forged de-authentication frame to the AP, causing the client to disconnect from the AP. This is the mechanism of the attack:

1. First, the attacker uses Airplay-ng tool to capture four-way handshake between the client and the AP.
2. Then attacker sends a series of forged de-authentication packets to the AP to end the communication session with the client (victim) and force the reauthentication process for the client.
3. The attacker impersonates the client and authenticates himself to the AP.

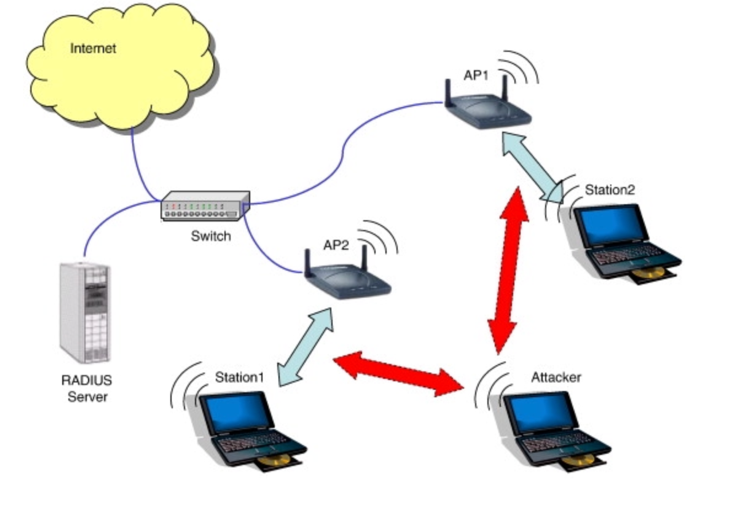
Denial of service can be achieved by the attacker when he continuously sends deauthentication packets, causing a DoS attack on the target network. A successful deauthentication attack denies the clients from accessing the network’s resources and causes them to lose connection to the network. In addition, this attack can be used to create further attacks like MITM attack or allow the attacker to crack the WPA encryption key.

**Tools**

These are the tools used to achieve different types of wireless DoS attacks [1][2]:

* Airmon-ng
* Airodump-ng
* Aireplay-ng
* mdk3: this tool is used to inject data into the wireless network. It’s usually used to exploit WIFI 802.11 vulnerabilities.

**Detection**

The following are detection techniques to detect deauthentication attack:

* Mac address spoof detection

This technique is used to analyze the sequence number pattern of the captured traffic to detect deauthentication attack. Detection systems showed that they were able to capture and detect MAC spoofing attacks traffic to identify deauthentication attack.

* Wireless intrusion detection system

WIDS is used to monitor and capture malicious traffic that flows inside the network.

Figure : Generic DoS attack

* Wireless AP logs

In this detection technique, the AP maintains a log of the network’s traffic to identify suspicious or unusual activities that can initiate an attack on the network.

**Countermeasures**

Denial of service attack is a powerful attack that threatens the availability and the security of the network. However, there are defensive techniques to encounter it. The following are techniques to mitigate the risk of deauthentication attack on the wireless network:

* Upgrade to secure WIFI protocol

By upgrading the WIFI protocol to secure protocols like WPA2 or WPA3 this minimizes the chance of DoS attack to occur on the network.

* Configure AP to drop deauthentication packets that originate from outside the network.
* Implementing network access control (NAC).

**References**

1. <https://sudorealm.com/blog/deauthentication-attack-using-kali-linux>
2. <https://subscription.packtpub.com/book/networking-&-servers/9781785280856/6/ch06lvl1sec27/denial-of-service-attacks>
3. Pelechrinis, Konstantinos & Iliofotou, Marios & Krishnamurthy, Srikanth. (2011). Denial of Service Attacks in Wireless Networks: The Case of Jammers. Communications Surveys & Tutorials, IEEE. 13. 245 - 257. 10.1109/SURV.2011.041110.00022.
4. Kemal Bicakci, Bulent Tavli, Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks, Computer Standards & Interfaces, Volume 31, Issue 5, 2009, Pages 931-941, ISSN 0920-5489, https://doi.org/10.1016/j.csi.2008.09.038.