Channel Switch and Quiet Attack: New DoS Attacks exploiting the 802.11 Standard (Demo Proposal)

Bastian Koenings, Florian Schaub, Frank Kargl – Ulm University, Germany
{firstname}.{lastname}@uni-ulm.de

I. Introduction

IEEE 802.11-based wireless networks are being deployed in large numbers in home, business, and public environments but also in critical environments like hospitals or production plants where reliance on their availability is crucial.

Despite security mechanisms having been introduced to the standard to ensure confidentiality, integrity, and authenticity, availability remains a particular challenge. RF jamming is a well known Denial-of-Service (DoS) attack. Advanced jamming methods have been proposed being more energy efficient and less detectable. Intelligent DoS attacks exploit vulnerabilities in the MAC layer of the 802.11 standard. Especially newer amendments like IEEE 802.11h or n are less well analyzed. We propose and demonstrate the feasibility of two new DoS attacks on 802.11 that fall in exactly this category.

DoS attacks against the 802.11 MAC layer apply to all IEEE 802.11 networks and many have been proposed [1]. The majority of attacks are based on masquerading, i.e. forging the identity of other stations. In contrast, we focus on fabrication and injection of management messages. They can be easily forged because, unlike data messages, they are neither encrypted nor integrity protected by any part of the standard and require no authentication. The future amendment 802.11w [2] aims to change this, but until its release and implementation they are extremely vulnerable.

The following two new attacks are based on the fabrication of management information elements that have been introduced with amendment 802.11h [3] to enable dynamic frequency selection (DFS) in the 5 GHz band. In Europe, DFS is mandatory for 802.11 devices operating at 5,25-5,35 GHz and 5,47-5,725 GHz [4]. Stations have to monitor the current channel for other signals, e.g. military radar, and switch to a different channel if it is occupied.

II. Quiet Attack

To be able to monitor the current channel for other activities, an access point (AP) includes a *quiet element* in beacons or probe responses. The quiet element specifies a certain time interval for which receiving stations have to be silent, i.e. send no messages, to allow for channel measurement. An attacker can forge the *quiet element* with the result that stations that adhere to 802.11h will remain silent for the specified quiet period.

III. Channel Switch Attack

If an access point recognizes other activity on the current channel during measurement it has to advise all stations of the BSS to change to a different channel with a *channel switch announcement element*. An attacker can utilize this element to get other stations in the BSS to change to a different or invalid channel. Furthermore, stations can be forced to be silent for a certain time before switching to the specified channel. Only after waiting an additional timeout, stations would try to establish a connection on another channel.

IV. Demonstration Setup

Quiet attack and channel switch attack will be demonstrated with an AP, a test station, and an attacker station (Fig. 1). A ping station connected to the AP uses ICMP pings to generate constant data traffic to the wireless test station. A station with its NIC in monitor mode measures the attack effect on the replies. Ping interval is 0.1 seconds, ping payload 5,000 bytes. An Atheros AR5212 NIC with Linux and Madwifi drivers is used for the monitor and attacker stations, enabling tests of 802.11a/b/g devices.

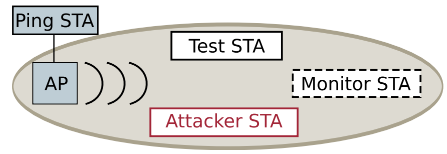

Fig. 1. Demonstration setup.

The success of an attack can be assessed in real-time by plotting traffic information at the monitor station. The effects of the attacks on different combinations of 802.11 devices, firmware versions, operating systems, and drivers can be easily tested using different test stations. Conference attendees can even connect their own mobile equipment to the WLAN and see if it is vulnerable.

The demonstration testbed consists of three laptops and one AP plus the test devices, and is therefore highly mobile. For attacks without measurements a single laptop is sufficient. The attack can be contained in its BSS and will not influence other WLANs.

V. Results

Both attacks were tested with 15 devices with varying drivers and operating systems. 5 devices recognize the quiet element and can be attacked successfully, the rest ignores it. A DoS effect of 67 s is achieved with a single message for an Intel 2200BG under Linux (ipw2200) and an Intel 4965AGN under Vista. These two examples show that older devices (802.11b) and current devices (802.11n) are susceptible to the *quiet attack*.

With *channel switch attacks*, DoS effects of 5-26 s are achieved with a single message. Most devices switch back to the original channel after 15 s. 9 devices ignore the channel switch announcement, because they only operate at 2.4 GHz. Surprisingly, the Intel 2200BG under Linux (ipw2200) can be silenced for 26 s, although the device operates only at 2.4 GHz. 5 devices supporting 802.11a were attackable even when operating on 802.11b/g channels.

VI. Conclusion

Channel switch and quiet attack are two new DoS attacks in 802.11 networks. They exploit management information elements introduced with 802.11h to enable the operation of 802.11a devices in the 5.2 GHz band in Europe and many other countries. By simply forging quiet period or channel information, a DoS effect up to 1 min. can be demonstrated caused by a single message. Thus, the presented attacks are very energy efficient and harder to detect due to few required messages. Interestingly, the attacks are also successful with devices operating at 2.4 GHz. However, some 802.11a/n devices ignore the channel switch announcements and quiet elements and are thus not standard compliant. These devices and drivers violate EN 301 893 [4], and must therefore not operate in Europe despite being sold publicly.

References

[1] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in *Proc. USENIX*, 2003, pp. 15–28.

[2] IEEE, "P802.11w/D6.0 - Part 11: Wireless LAN MAC and PHY Layer specifications - Amendment 4: Protected Management Frames," 2008.

[3] ——, "Std 802.11h – Part 11: Wireless LAN MAC and PHY Layer specifications – Amendment 5: Spectrum and Transmit Power Management Extensions in the 5 GHz band in Europe," 2003.

[4] ETSI, "EN 301 893 v1.5.1: Broadband Radio Access Networks (BRAN); 5 GHz High Performance RLAN," 2008.