Availability analysis of SURFwireless

K. van Brakel
Security and Network Engineering - University of Amsterdam

August 13, 2019

Abstract

This study investigates the impact of three Denial-of-Service(DoS) attacks: Deauthentication, Channel Switch, and Quiet Attack on 802.11 clients connected with the SURFwireless network. Potential detection and prevention methods for these three attacks are discussed. The impact of the attacks was determined by measuring the network performance, using iPerf3 and ping. First, while not under attack, a network performance basetest was conducted. Then, the network performance while under attack was measured and compared with the basetest. In this paper is demonstrated that depending on the used attack frame delay, both the Deauthentication attack and Channel Switch attack had a noticeable impact on the network performance of the target 802.11 clients. By enabling the 802.11w amendment, the Deauthentication could be prevented while the Channel Switch and Quiet attack were insusceptible for this counter measure. Only the Deauthentication attack was detected by the Wireless Intrusion Prevention System(WIPS) of Aerohive.

1 Introduction

SURF is the collaborative organisation for ICT in Dutch education and research. One of the services that SURF offers is network connectivity, which is part of the SURFnet department. SURFnet only connects institutions that belong to its target group: educational institutions, healthcare institutions, research institutions, and libraries. Since 2016, SURFnet offers SURFwireless, a Wi-Fi-as-a-service proposition. A broad variety of users, such as students, employees, and visitors expect a fast and secure network with high availability. The network has to support a wide range of devices, each with its own characteristics like 802.11 chipset, driver version, and operating system(OS). Furthermore, the

demand for innovative services like 802.11-based positioning systems and integration with the Internet of Things(IoT) increases. Each of these features rely on the 802.11 network of SURFwireless. According to SURFnet, users of SURFwireless assume that the network is secure and always available. Hence, some customers almost completely rely on the 802.11 network of SURFwireless for network connectivity. Therefore, availability of SURFwireless is very important for SURFnet.

For the 802.11 network of SURFwireless the equipment of Aerohive is used. The 802.11 solution of Aerohive is a controller-less architecture[1], meaning that the APs function as an independent device without the need for a controller. The configuration settings of the Aerohive APs are maintained from a central location, called the HiveManager.

Attacks that threaten the availability of 802.11 networks are better known as Denial-of-Service(DoS) attacks. DoS attacks threaten the availability of a network by attempting to prevent legitimate users to access the network[8]. This research was conducted for SURF to gain more insight about what potential DoS attacks threaten the availability of SURFwireless and what the impact of these attacks is. Researchers have already investigated and presented various attacks that threaten the availability of 802.11 networks[17, 8, 5, 11, 7]. Attacks where valid protocol frames are abused to attack one or more clients are also known as semantic attacks[11]. For Media Access Control(MAC) Layer DoS attacks management frames are exploited most often[8]. In September 2009, the 802.11w amendment was published. The main purpose of the amendment is to reduce the susceptibility of 802.11 systems to malicious attacks that impersonate legitimate 802.11 devices and forge their frames in attempt to disrupt the 802.11 system[4]. The 802.11w amendment protects against forging of disassociation, deauthentication, and robust action frames[4, 18].

In the HiveManager the Wireless Intrusion Prevention System(WIPS) environment can be configured. The WIPS environment from Aerohive is able to detect MAC layer based DoS attacks on 802.11 networks. This detection mechanism works on basis of a certain threshold per 802.11 frame type that are used for DoS attacks. The threshold value is expressed in packets per minute(PPM) in the Aerohive WIPS environment. For this study, known DoS attacks were implemented in Python with a library called Scapy and conducted on the SURFwireless network. The effectiveness of the attacks was measured by studying the network performance as experienced by clients. Each attack was conducted with varying delays(in seconds) between the attack frames, referred to as attack frame delay in the rest of this paper. The used attack frame delay can be expressed in PPM, the threshold values the Aerohive WIPS environment uses.

The rest of the paper is organized as follows: in Section 1.1 the research questions that were formulated for this research are presented. In Section 2, related work is described and in particular MAC layer DOS attacks. Section 3 describes the workings of the three investigated DoS attacks. Where Section 4 describes the methods that were used to perform the experiments. Next, in Section 5 the results of the conducted experiments are presented and discussed in Section 6. Finally, Section 7 summarizes the findings of this research followed

by potential future work in Section 8.

1.1 Research questions

The question central in this paper is as follows:

How can SURFnet detect that the availability of the SURFwireless service is under threat and determine its impact?

In order to answer the main research question the following sub-questions were composed:

- Which common attacks on 802.11 networks can be used to threaten the availability of SURFwireless?
- What impact do these attack cause on the wireless clients of SURFwireless?
- What measures can SURFnet take to defend SURFwireless against attacks on availability?

2 Related work

Previous studies have shown that various kind of attacks against wireless networks exist[20, 19, 25]. These attacks can be classified into two categories, active and passive attacks[9]. Examples of active attacks are DoS, message corruption/altering, and replay attacks. As the name suggests such attacks actively interfere with a client that is connected with the 802.11 network. In contrast to passive attacks, where the attacker stays hidden and is limited to monitoring and listening of the wireless channel. Examples of such attacks are eavesdropping, traffic analysis, and camouflage adversaries[19, 9]. In this study only attacks that potentially threaten the availability of SURFwireless were investigated, thus DoS attacks. According to Bicakci et al. DoS attacks on 802.11 networks can be categorized into three categories: physical layer, MAC layer, and above the MAC layer attacks in 802.11 networks[8]. For each of these categories multiple attacks exist[17, 8, 5, 11, 7]. Only MAC layer DoS attacks were investigated during this study because equipment that was used to perform the attacks with was limited to a RaspberryPi 3 and an Alfa 802.11 adapter.

MAC layer In [7, 11, 8, 5] several MAC layer attacks are discussed. From which the Deauthentication attack is the most common attack[7]. 802.11 frames can be classified into three different type of frames: management frames, control frames and data frames. Each of these frame types has its own subtypes. A more detailed overview of the 802.11 frames including their subtypes is given by Bicakci et al.[8].

3 Workings of the investigated DoS attacks

In this section, the three MAC layer DoS attacks that were investigated: Deauthentication, Channel Switch, and Quiet attack are described. The Deauthentication attack was chosen for this study because it is the most common MAC layer DoS attack on 802.11 networks[17]. The Channel Switch and the Quiet attack were chosen because according to Könings et al. both attacks cannot be mitigated even though the 802.11 network is protected by the 802.11w amendment[17]. The three investigated DoS attacks require unique fields to be forged. However, for all of them applies that the MAC layer has to be forged, which requires the attacker to forge at least the following fields:

- **DA**, Destination MAC address of the target;
- **SA**, Source MAC address of the impersonated device;
- **BSSID**, of the impersonated 802.11 network;

The tool Airodump-ng[1] was used to obtain the DA, SA, and BSSID of the target. The remaining fields in the MAC header, Frame Control, Duration, and Seq ctl were padded with zeros. Chapter 3 "802.11 Framing in Detail" from [12] gives detailed information about the 802.11 MAC header fields and their purpose.

3.1 Deauthentication attack

In the 802.11 standard a deauthentication frame is sent whenever the need to terminate the established connection between two 802.11 stations occurs. Figure 1 shows the 802.11 MAC header including the attributes of a deauthentication frame. With a Deauthentication attack, the attacker impersonates its target and transmits a deauthentication frame on the target's behalf. Causing the established connection between the two 802.11 devices to be terminated. Before the two devices can continue transmission again, the client has to follow the required steps of the authentication process again to restore the previously established connection. By continuously transmitting deauthentication frames the network becomes unavailable for the target[8, 7].

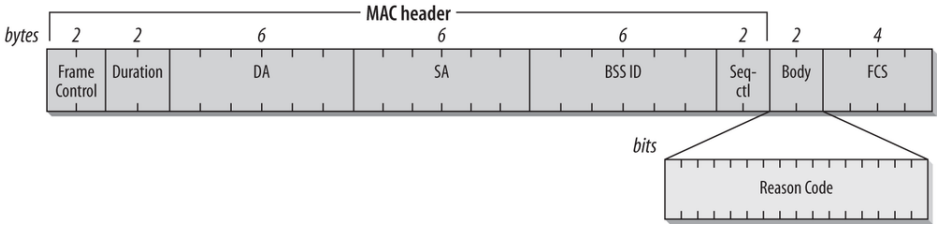


Figure 1: Generic deauthentication frame[12].

3.2 802.11h amendment

Both the Channel Switch and the Quiet attack, which are described in the Section 3.3 and 3.4, abuse the 802.11h amendment[3]. Radar equipment that also uses the 5 GHz frequency band has priority over 802.11 equipment on the shared frequencies in Europe. Therefore, it is mandatory that APs avoid interference with radars that operate at the 5 GHz frequency band. One of the components of the 802.11h amendment is Dynamic Frequency Selection(DFS). With DFS, APs actively listens for radar activity on its current working channel. When radar activity is detected, the AP is obligated to switch to another channel[15]. To prevent losing connection with the connected 802.11 clients, a channel switch announcement is transmitted to the connected 802.11 devices before the AP switches to the new channel. This announcement contains the channel the AP is going to switch to.

3.3 Channel Switch attack

The channel switch announcement element, that is abused by the Channel Switch attack can either be transmitted in a Beacon, Probe response, or in an Action frame as information element[17]. The Channel Switch attack abuses the channel switch announcement information element that is specified in 802.11h amendment[11, 17]. Various information elements can be attached to management frames[12]. Gupta et al. gives an overview of the existing information elements including their meaning that can be added to 802.11 management frames[14]. The Channel Switch Attack is not the only attack on 802.11 networks that abuses channel switch announcement. The Key Reinstallation Attack, which was presented by Vanhoef et al. also abused the channel switch annoucement[23]. With the Channel Switch attack the attacker creates forged frames containing a channel switch announcement. Figure 2 displays the generic fields of a channel switch announcement element, which consists of the following fields[17]:

- **Channel switch mode**, indicates whether the client can continue to transmit(value 0) until it switches channel or if it has to stop transmission immediately(value 1);
- **New channel number**, indicates the new channel the AP switches to when channel switch count is reached;
- **Channel switch count**, indicates the remaining Beacon intervals before the AP switches to the new channel;

3.4 Quiet attack

The Quiet attack described by Könings et al. abuses the quiet element that is specified in the 802.11h amendment[17]. The quiet element is used by APs to silence 802.11 devices that are on its channel to measure if there is radar activity

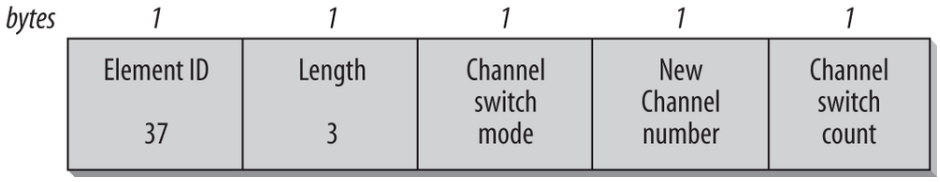


Figure 2: Generic Channel Switch frame[12].

on its current working channel. The quiet element, can either be included in Beacons or in Probe Responses[17]. The quiet element depicted in Figure 3, consists of the following four fields[12]:

- **Quiet count**, the number of Beacon transmission intervals until the 802.11 client has to stop transmission of frames for the specified quiet duration;
- **Quiet period**, a zero value indicates the quiet time is not scheduled. A non-zero value indicates the number of Beacon intervals between the scheduled quiet element;
- **Quiet duration**, indicates the duration in time units for which the 802.11 clients have to be quiet. 1 time unit equals 1024 μs;
- **Quiet offset**, a non-zero value indicates the number of time units after a Beacon interval the next quiet time will begin. Quiet offset has to be smaller than one Beacon interval.

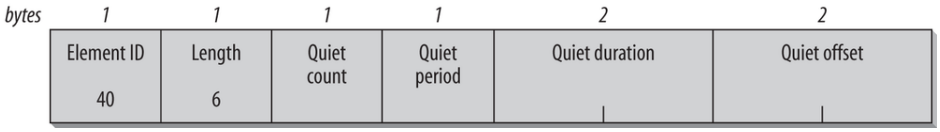


Figure 3: Generic Quiet frame[12].

4 Test environment and experiments

This section discusses the test environment that was used to perform the DoS attacks that are described in Section 3. Furthermore, the applied methods, the soft- and hardware, including the version that was used and its purpose for the experiments are discussed.

4.1 Test environment

The test environment consists of a single AP, which was configured on channel 11 from the 2.4 GHz frequency band, a Dell XPS13 which functions as 802.11

client/target, and a RaspberryPi 3 B+ was used to perform the attacks that are described in Section 3. More detailed information of the used devices can be found in Table 1 and a graphical overview of the test environment can be found in Figure 4.

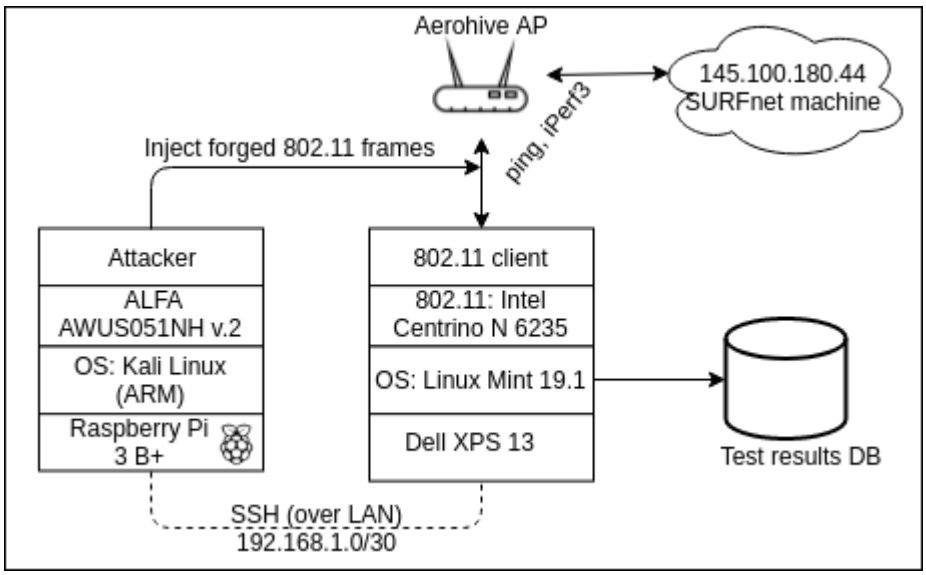


Figure 4: Overview of the test environment.

Device	**802.11**	**Software**	**Role**
Dell XPS13 Intel Centrino Advanced-N 6235	a/b/g/n	Linux mint 19.1 Cinnamon Kernel 4.15.0-51	Targeted client
Raspberry Pi 3 B+	b/g/n/ac	Kali Linux Kernel 4.19.29-Re4son-v8+	Attacker
Aerohive AP630	a/b/g/n/ac/ax	HiveOS 10.0r5	Access point
Alfa AWUS051NH	b/g/n	driver=rt2800usb	Monitor mode
Alfa AWUS036NEH	b/g/n	driver=rt2800usb	Monitor mode

Table 1: Detailed overview of devices that were used for the test environment including 802.11 capabilities and used software versions.

To conduct the attacks, monitor mode is required for frame injection[24]. The on-board 802.11 chip of the Raspberry Pi does not support monitor mode. Therefore, an Alfa AWUS051NH was used as 802.11 adapter instead. The test environment was located at the office of SURFnet in Utrecht. The test AP was not used by any of the employees of SURFnet for regular work activities. To prevent employees of SURFnet to accidentally connect with the test AP, the eduroam SSID was not broadcast by the test AP. Instead, a test network with the SSID "wips-test-802.1x" was configured. The test SSID was configured identically as the eduroam SSID in terms of configuration settings except for

the channel configuration to avoid interference with SURFwireless network. The SURFwireless network consists of various types of APs from the brand Aerohive. During this study, only AP model AP630 from the brand Aerohive was used during the experiments. This particular AP has support for 802.11ax. However, during the conducted experiments the AP was configured as 802.11n AP. To verify whether the forged frames were transmitted correctly, Wireshark was used to manually inspect the forged frames.

4.2 Experiments

To measure the impact on the network performance of each attack a Transmission Control Protocol(TCP) iPerf3 session and ping were started from the 802.11 client. The iPerf3 session was used to measure the data rate the 802.11 client was able to achieve. The ping session was used as second measurement to determine whether network communication with the targeted 802.11 client was possible. The ping packets were transmitted every second. Within the period of 1 month (14 July - 13 August) at least 86% of all traffic from a relatively large customer of SURFwireless (600+ APs) existed of TCP traffic, justifying the choice for measuring TCP traffic. Reduced TCP throughput results in longer waiting times of internet services (such as e.g., browsing, access via Secure Sockets Layer(SSL) and streaming media) as experienced by users of SURFwireless. Prior to performing the measurements during the attacks, a basetest which represents the baseline measurements where no attacks were performed while the iPerf3 and ping measurements were conducted, was held. To determine the impact of the investigated attacks, the results of the conducted experiments were compared with the basetest.

Before launching the iPerf3 and ping session, the attack was launched on the RaspberryPi. The three investigated attacks were implemented in Python3 with Scapy, a python library. The scripts that were created and used for this study can be found at [22]. Scapy enables the user to create, forge, or decode packets on a network, to capture and analyse them, and inject custom 802.11 frames. For the purpose of this study, Scapy was used to inject 802.11 frames. The 802.11 client and the RaspberryPi were connected with a Secure Shell(SSH) connection over a fixed link. The attack was launched from the 802.11 client by using the SSH connection with the RaspberryPi. After the attack was initiated, both the ping and iPerf3 session were started in separated threads. Each experiment lasted for 60 seconds and was repeated 30 times. To determine the impact of the attack with varying attack frame delays, each experiment was conducted with multiple attack frame delays. The attack frame delay represents the amount of seconds between each of the forged attack frames. The expectation was when the attack frame delay would be increased the impact of the attack on the 802.11 client would decrease. The used frame delay can be expressed in PPM, the threshold value per frame the AeroHive WIPS environment uses. The process of the experiments was completely automated in Python3 and the results of the measurements were stored in a MySQL database.

4.2.1 Deauthentication attack

While conducting the Deauthentication attack, reason code 7 was used. Which has the following value: "Class 3 frame received from nonassociated STA."[2]. The optional vendor specific field was not used because it is an optional field. The 802.11w field was not used either because 802.11w is disabled on the SURF-wireless network.

4.2.2 Channel Switch Attack

According to Könings et al. if the client switches to the new channel and does not receive any Beacon frames on that channel, the client will switch back and reconnect[17]. To decline traffic for the targeted 802.11 client completely, the attacker has to forge Beacon frames from the AP the client was connected to[17]. However, for this study another approach was used. Instead of forging Beacon frames on the new channel, channel switch announcements were repeatedly transmitted on the current working channel of the AP during the attack period. The reason for this change was because the RaspberryPi that was used for the experiments was equipped with one Alfa 802.11 adapter. Therefore, it was not possible to transmit forged Beacon frames with Channel Switch announcement and to transmit forged Beacon frames from the AP on the new channel simultaneously.

Used parameters Table 2 shows the parameters that were used while performing the Channel Switch attack. Value 0 was used for the channel switch count field, indicating that the targeted 802.11 client immediately had to switch to the channel specified in the new channel field. For the field channel switch mode, value 0 was used, indicating that the targeted 802.11 client immediately has to stop transmission on its current working channel. For the new channel field, the value 36 was specified during all the throughput measurement experiments. According to Könings et al. some 802.11 clients allow the input of invalid channels as well[17]. Another experiment was conducted where the attacker attempted to make the investigated devices listed in Table 4 switch to an invalid channel, namely channel 127.

Field	**Value**
Channel switch mode	0
New Channel	36, 127
Channel switch count	0

Table 2: Used parameters for Channel Switch attack.

4.2.3 Quiet attack

Targeted clients can be theoretically silenced for a maximum period of 65535 Time Units(TU) with a single forged frame. However, Könings et al. have

shown that it depends on the driver implementation whether clients comply with this maximum silent period[17].

Used parameters Table 3 shows the parameters that were used while performing the Quiet attack. For the field quiet count, value 0 was used. Which indicates that the targeted 802.11 client immediately had to stop transmission of any frames for the specified time which was indicated in the quiet duration field. For the quiet period field value 0 was used, meaning the quiet element is not scheduled repeatedly. Finally, the value 0 was used for the quiet offset field, meaning that the quiet element took effect immediately. The expectation when specifying a quiet duration of 4000 time units was that the targeted 802.11 client would be silenced completely when an attack frame delay of 4 seconds is used.

Field	**Value(decimal)**
Quiet count	0
Quiet period	0
Quiet duration	4000
Quiet offset	0

Table 3: Used parameters for Quiet attack.

4.3 Vulnerable devices

To determine whether only the Dell XPS13 was vulnerable to these attacks, five additional devices were attacked. Table 4 gives an overview of the additional investigated devices. On each of the devices an iPerf3 session was started. Both the Deauthentication and Channel Switch attack were conducted with an attack frame delay of 0.1 seconds. The expected result for the targeted 802.11 devices was to lose connectivity.

Device	**802.11 chipset**	**OS**
Dell XPS 13	Intel Centrino Advanced-N 6235	Linux Mint 2019.1
Macbook pro (2017)	Airport card	MacOS 10.14.5
Samsung S10	Broadcom	Android 9
OnePlus 6T	Qualcomm	Android 9
XNB W650EH	Intel AC 7265	Windows 10

Table 4: Overview of devices that were investigated whether they are vulnerable to the three investigated attacks.

5 Effects of the DoS attacks

In this section, the results of the performed experiments are presented. The results section is subdivided into two parts. First, the impact in terms of network throughput and packet loss rate for the Deauthentication, Channel Switch, and Quiet attack is presented. Secondly, an overview of devices that were investigated for this study is given. The graphs can be read as follows: the blue bar represents the mean value of the 30 experiments, the black error bar on top of the mean value depicts the range of the results with a 95% confidence level. In each graph the results per attack frame delay is compared with the basetest, which is labeled with the tag 'base' in the graphs.

5.1 Impact of the DoS attacks

5.1.1 Deauthentication attack

Figure 5 shows that when the attack frame delay increases, thus the delay in seconds between forged attack frames increases, the packet loss rate also decreases. When attack frame delay 0.1 and 0.5 seconds were used, a packet loss rate of 90% and 63% was achieved. When further increasing the attack frame delay to 1, 1.5, and 2 seconds the packet loss rate decreases below 10%. Figure 6(a) depicts the remaining throughput in megabytes(MB) per second while conducting the attack. As expected, an attack frame delay of 0.1 and 0.5 seconds have the most noticeable impact on the network throughput. Nevertheless, an attack frame delay of 1 second decreases network throughput by roughly half even though less than 10% packet loss rate was experienced. Figure 6(b), shows that 462 retranmissions occurred when an attack frame delay of 1 second was used, causing the decreased throughput. Another remarkable result occurred when an attack frame delay of 2 seconds was used. The data throughput while under attack, was higher than with the basetest. An assumption is, because the amount of retransmissions that occurred as a result of the attack, more traffic was transmitted resulting in a higher total bandwidth than compared with the basetest.

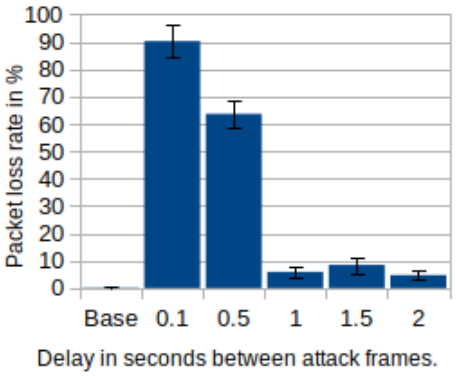
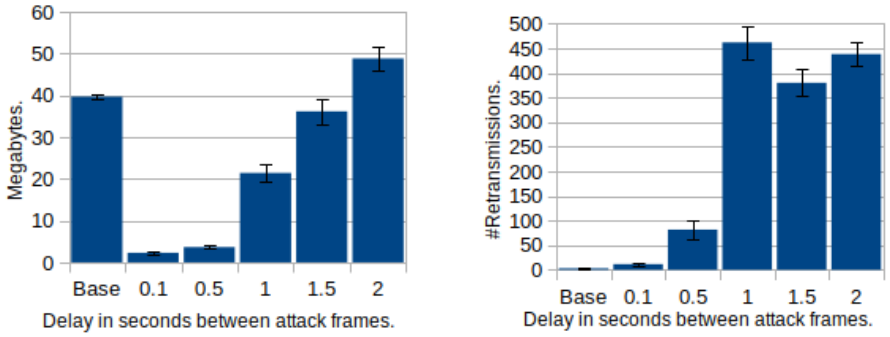


Figure 5: Deauthentication attack - ping: packet loss rate in 60 seconds.



(a) Transmitted data in 60 seconds

(b) Retransmissions in 60 seconds

Figure 6: Deauthentication attack: iPerf3.

5.1.2 Channel Switch attack

Figure 7 depicts the impact of the Channel Switch attack on the ping experiment of the targeted client. Figure 8 and 9 demonstrate the impact of the Channel Switch attack on the iPerf3 experiment. When the attack frame delay was increased to 8 seconds, noticeable impact was measured whereas the impact of the Deauthentication attack with an attack frame delay of 2 seconds was noticeably lower. As with the Deauthentication attack, a higher attack frame delay i.e. 7.5 and 8 seconds caused the packet loss rate to decrease but the number of retransmissions to increase remarkably. Which resulted into a higher amount of transmitted data than was observed during the basetest. For attack frame delays 1.5, 2.5, 3, 5, and 6 seconds a bigger than expected increase in the amount of transmitted traffic was observed. An assumption is that this was caused by the amount of retransmissions that occurred as a result of the attack.

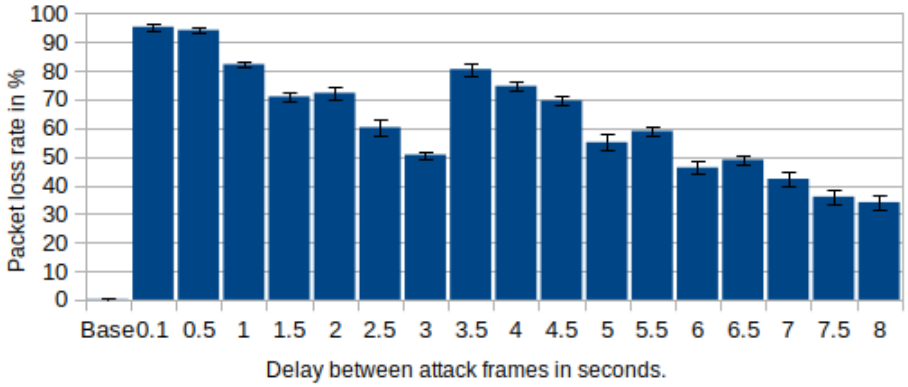


Figure 7: Channel Switch attack - ping: packet loss rate in 60 seconds.

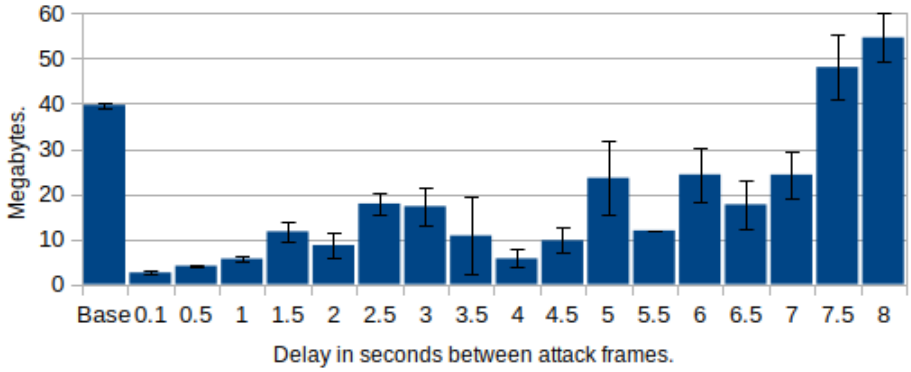


Figure 8: Channel Switch attack - iPerf3: transmitted data in 60 seconds.

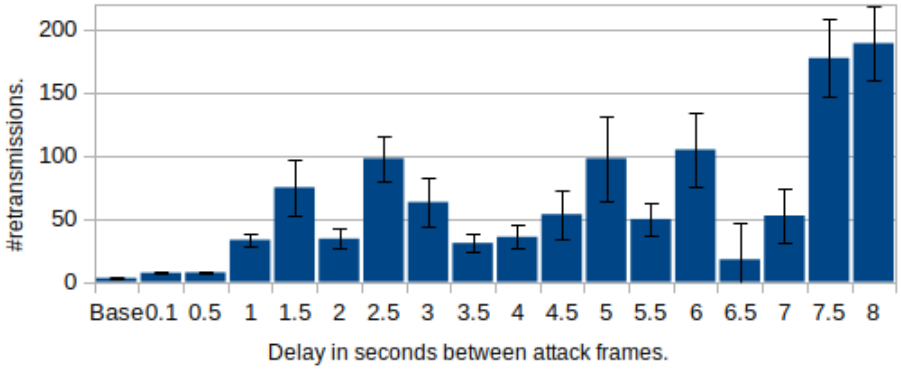


Figure 9: Channel Switch attack - iPerf3: retranmissions in 60 seconds.

5.1.3 Quiet attack

With the described parameters from Table 3, the Quiet attack did not affect the targeted client as expected. The expectation was no data would be transmitted when an attack frame delay of 4 seconds was used. However, Figure 10 shows that the impact of the Quiet attack with an attack frame delay of 1 and 4 seconds was negligible. When an attack frame delay of 0.1 seconds was used a packet loss rate of 9.5% was achieved. Figure 11(a, b) show that the transmitted data is decreased by approximately 30 MB compared with the basetest. While the amount of retransmission increased to 225 when an attack frame delay of 0.1 seconds was used.

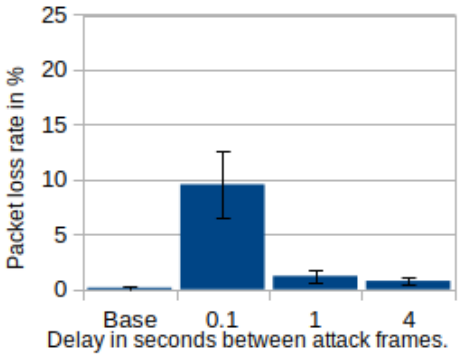
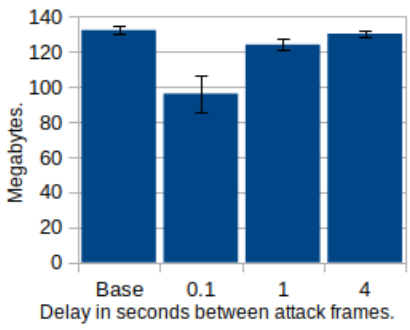
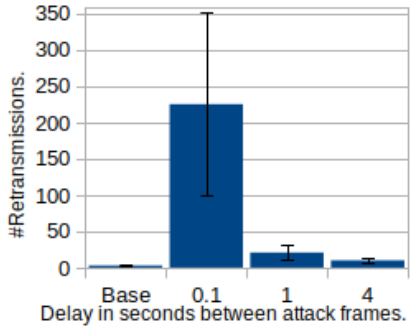


Figure 10: Quiet attack - ping: packet loss rate in 60 seconds.



(a) transmitted data in 60 seconds.



(b) Retransmissions in 60 seconds.

Figure 11: Quiet attack: iPerf3.

5.1.4 Vulnerable devices

In the previous subsections impact of the three investigated attacks on the Dell XPS13 was presented. In addition, it was found that the devices listed in

Table 4 are also susceptible to the Deauthentication and Channel Switch attack. Furthermore, it was found that only the Dell XPS13 was susceptible to Channel Switch attack when the invalid channel 127 was specified.

6 Discussion

This section is subdivided into three sections. First, potential prevention methods for the investigated attacks are discussed. Secondly, detection method that can be configured from the HiveManager and potential detection methods that are not implemented by Aerohive are discussed. Finally, the limitations of the results of the investigated attacks are discussed.

6.1 Prevention 802.11w Management Frame Protection

The 802.11w amendment, released by the Institute of Electrical and Electronics Engineers(IEEE) task force, extends the original 802.11 specification by protecting management frames. The purpose of the amendment is to defend 802.11 systems from malicious attacks that abuse unprotected management frames[4]. With the Aerohive equipment it is possible to enable 802.11w when Wi-Fi Protected Access II(WPA2) is used as security protocol. However, the 802.11w amendment has to be supported by both the 802.11 client and the AP in order for the protection mechanism to work. Within the HiveManager 802.11w it is possible to optionally enable 802.11w, meaning that the 802.11 clients that do support the amendment, make use of the protection mechanism. With the new security protocol, Wi-Fi Protected Access III(WPA3), the 802.11w amendment becomes mandatory[6]. WPA3 was released to the public on 25 June 2018 by the Wi-Fi Alliance[16]. The AP that was used for this study already supports WPA3. However, the SURFwireless network uses WPA2-enterprise as protection protocol. Therefore, WPA2-enterprise was also used for this study. As described in Section 3.3, the Channel Switch attack can be performed with Beacon, Probe Response and/or Action management frames. Enabling 802.11w did not protect against the Channel Switch attack because both Beacon and Probe Response frames are not protected by the 802.11w amendment[4, 17, 11]. Therefore, enabling 802.11w does not prevent against this attack. In contrast to the Deauthentication attack, which is countered by enabling this feature. Which makes it plausible when the security protocol of SURFwireless would be upgraded to WPA3 the network would still be vulnerable to the Channel Switch and Quiet attack. However, there was no WPA3 compliant 802.11 devices available for this study. Therefore, it was not verified whether this is actually the case.

6.2 Detection

The HiveManager from Aerohive has a build-in Wireless intrusion Prevention System(WiPS). This system is able to detect DoS attacks based on a threshold

for certain 802.11 frame types. These thresholds can either be specified on client or SSID basis. Table 5 shows for which 802.11 frames a threshold can be specified, including the values that were used for SURFwireless on client and SSID basis.

Frame type	**Threshold (PPM)**	**Threshold (PPM)**
Probe Request	1200	12000
Probe Response	2400	24000
(Re)Association Request	600	6000
Association Response	240	2400
Disassociation	120	1200
Authentication	600	6000
Deauthentication	120	1200
EAP Over Lan(EAPoL)	600	6000

Table 5: Overview of used alarm thresholds in packets per minute (PPM) per supported frame types.

Depending on the used attack frame delay, both the Deauthentication and the Channel Switch attack had a noticeable impact on the client while under attack. The used threshold for the deauthentication frame in the WIPS environment is 120 PPM on client basis. This would translate to an attack frame delay of 0.5 seconds. If an attack frame delay of more than 0.5 seconds was used, the attack was not detected by the WIPS, while Figure 6 shows that when an attack frame delay of 1 second was used the throughput was still reduced by roughly half. The Channel Switch attack was not detected by the WIPS because the Beacon Frame type was used to transmit the frames. In the WIPS it is not possible to specify a threshold for the Beacon Frame type. The WIPS environment does have a threshold for Probe Response frame, which can also be used for the Channel Switch attack. For SURFwireless this threshold is on 1200 PPM. Which translates to an attack frame delay of 0.05 seconds. Whereas Figure 7 shows that when an attack frame delay of 0.1 seconds was used the packet loss rate was approximately 90%. The WIPS of Aerohive fails to detect the Channel Switch attack and only detect the Deauthentication attack with an attack frame delay of 0.5 seconds or lower. Besides, more sophisticated detection methods to determine MAC address spoofing based attacks i.e. by sequence number[13] or collect the delay and throughput data and apply a change point detection algorithm to observe the change of distribution[10] exists, but are not implemented by Aerohive.

6.3 Limitations

According to Könings et al. only devices that support the 5 GHz frequency band are susceptible to the Channel Switch and Quiet attack[17]. According to SURFnet approximately 80% of the 802.11 devices that are connected with the SURFwireless use the 5 GHz frequency band. During this study only devices

that support both the 2.4 and 5 GHz frequency band were investigated while the access point was always configured on channel 11. Even though the 2.4 GHz frequency band was used the Channel Switch attack was still successful. The Channel Switch attack abuses the channel switch element which is used to announce the connected 802.11 clients that the AP will switch to a new channel because radar activity was detected by the AP on a 5 GHz DFS channel. The Quiet attack did not impact the network performance as expected. It could be that the Quiet attack only works on 802.11 networks that operate at the 5 GHz frequency band. However, the related work of Könings et al. have also shown that some devices were more sensitive than others to the Quiet attack i.e. the Windows Vista driver for the Intel 3945ABG limited the maximum quiet time to 8 seconds[17].

For the iPerf3 experiments only TCP throughput measurements were conducted. Therefore, the determined impact on 802.11 clients in terms of network throughput is only applicable to TCP traffic. It should be noted that TCP makes use of congestion control. A mechanism that controls the sending rate by manipulation the congestion window. When a TCP segment is lost, the congestion window will be decreased, thus decreasing the maximum achievable data rate[21]. When the targeted 802.11 client was under attack during the experiments 802.11 frames got lost. Causing the TCP congestion window to decrease because these frames also contain the TCP segments for the iPerf3 session. The impact of the attacks when different internet protocols like UDP would be used was not investigated during this study. Therefore, it is uncertain what the impact on the targeted 802.11 client would be when different internet protocols would be used.

In total five devices were investigated whether they are susceptible to the investigated attacks. It was found that the five devices are vulnerable for the Deauthentication and Channel Switch attack. However, the impact on network performance was only investigated for the Dell XPS13. It is possible that the performance impact differs per device. Furthermore, five devices do hardly represent the wide variety of different 802.11 client devices that are used on the SURFwireless network. Nevertheless, it is plausible that most devices are vulnerable to these attacks because the devices that were investigated are modern devices. In total four different OSs, Android, MacOS, Linux Mint, and Windows with the latest software updates installed were investigated. In all experiments, the availability of SURFwireless for a single client was under attack. To jeopardize the availability of SURFwireless for all connected clients, the attacks have to be applied to all individual clients connected.

During this study all the attacks were conducted on the 2.4 GHz frequency band. The expectation is that the attacks will have similar impact when the 5 GHz frequency band is used. However, this was not explicitly investigated during this study. Due to the fact that in general higher throughput is achieved when the 5 GHz frequency band is used, it is possible the attacks have a less noticeable impact on network throughput when the 5 GHz frequency band is used.

Finally, it should be noted that the experiments have been conducted in a

test environment which consisted of a single AP that was configured on a single 2.4 GHz channel. If multiple APs would be used in the environment, the impact on the 802.11 client of the Deauthentication and Channel Switch attack will most likely decrease. Because when the client is either deauthenticated from the AP or switched to an invalid channel, it is uncertain with which AP the client will attempt to reconnect. Furthermore, if the client would be disconnected on the 2.4 GHz channel, but environment consists of APs that are configured on both 2.4 GHz and 5 GHz channels, the attacker would be unsure whether the 802.11 client would reconnect with the 2.4 GHz or 5 GHz channel, assuming the 802.11 client supports both channels. Therefore, the attacker should continuously monitor to which AP and channel the client has switched to and adjust the attack parameters accordingly.

7 Conclusion

The tests described in this paper demonstrated that the five investigated 802.11 devices, the Dell XPS 13, MacBook pro, Samsung S10, OnePlus 6T, and XNB W650EH are susceptible to the Deauthentication and Channel Switch Attack. For the Dell XPS13 it has been shown that the network performance was impacted noticeable by both the Deauthentication and the Channel Switch attack, but not to the Quiet attack. For the Deauthentication and Channel Switch attack when an attack frame delay of 0.5 seconds was used, roughly 10% of the network throughput remained in comparison with the network throughput that was achieved during the basetest. The Aerohive WIPS was only able to detect the Deauthentication attack. The default threshold on client basis is 120 PPM and on SSID basis 12000 PPM. 120 PPM translates to an attack frame delay of 0.5 seconds, thus when a higher attack frame delay was used, the attack was not detected. The impact of the DoS attacks was dependent on the attack frame delay that was used and on the type of the attack. It was demonstrated that the Channel Switch attack had more impact with a higher attack frame delay than the Deauthentication attack. By enabling the 802.11w amendment on the 802.11 network of SURFwireless, the Deauthentication attack can be countered whereas the Channel Switch and Quiet attack remain unaddressed.

To conclude, the WIPS environment of Aerohive that is used by SURFwireless was able to detect the Deauthentication attack when an attack frame delay of 0.5 seconds or lower was used. Whereas the Channel Switch attack was not detected. The impact of the Deauthentication and Channel Switch attack depended on the used attack frame delay.

8 Future work

This study has demonstrated that five devices Listed in Table 4 are susceptible to the Deauthentication en Channel Switch attack when connected to the SURFwireless network. To determine whether more 802.11 devices are susceptible to

these attacks, expanding the list of investigated devices could be a next step. Furthermore, only three attacks were investigated. More DoS attacks on 802.11 networks exists. Therefore, this research could be repeated with other DoS attacks. As stated in the discussion, the impact on the 802.11 clients per attack potentially differentiates in a multi AP environment. Also, it could be interesting to investigate the overhead for the attacker what a multi AP environment brings. Furthermore, the impact on network throughput was only investigated when TCP was used. It could be interesting to investigate the impact of the investigated DoS attacks other internet protocols like UDP. Due to different characteristics of these protocols the results potentially vary. The WIPS of the HiveManager indicates on which AP the frame threshold was reached. Lastly, it could be useful to investigate the possibility to use 802.11-based positioning systems to locate the attacker to mitigate the attack.

References

[1] airodump-ng package description. `https://tools.kali.org/wireless-attacks/airodump-ng`. Online; accessed: 4-June-2019.

[2] Deauthentication reason code table. `https://www.cisco.com/assets/sol/sb/WAP371_Emulators/WAP371_Emulator_v1-0-1-5/help/Apx_ReasonCodes2.html`. Online; accessed: 8-July-2019.

[3] IEEE standard for information technology– local and metropolitan area networks– specific requirements– part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications - spectrum and transmit power management extensions in the 5 ghz band in europe. *IEEE Std 802.11h-2003 (Amendment to IEEE Std 802.11, 1999 Edn. (Reaff 2003))*, pages 1–75, Oct 2003.

[4] IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements. part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 4: Protected management frames. *IEEE Std 802.11w-2009 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, and IEEE Std 802.11y-2008)*, pages 1–111, Sep. 2009.

[5] Md Sohail Ahmad and Shashank Tadakamadla. Short paper: security evaluation of ieee 802.11 w specification. In *Proceedings of the fourth ACM conference on Wireless network security*, pages 53–58. ACM, 2011.

[6] Mariusz Bednarczyk and Zbigniew Piotrowski. Will wpa3 really provide wi-fi security at a higher level? In *XII Conference on Reconnaissance and Electronic Warfare Systems*, volume 11055, page 1105514. International Society for Optics and Photonics, 2019.

[7] John Bellardo and Stefan Savage. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In *USENIX security symposium*, volume 12, pages 2–2. Washington DC, 2003.

[8] Kemal Bicakci and Bulent Tavli. Denial-of-service attacks and countermeasures in ieee 802.11 wireless networks. *Computer Standards & Interfaces*, 31(5):931–941, 2009.

[9] Ismail Butun, Salvatore D Morgera, and Ravi Sankar. A survey of intrusion detection systems in wireless sensor networks. *IEEE communications surveys & tutorials*, 16(1):266–282, 2013.

[10] Mallesham Dasari. Real time detection of mac layer dos attacks in ieee 802.11 wireless networks. pages 939–944, 01 2017.

[11] Martin Eian and Stig F Mjølsnes. A formal analysis of ieee 802.11 w deadlock vulnerabilities. In *2012 Proceedings IEEE INFOCOM*, pages 918–926. IEEE, 2012.

[12] Matthew Gast. *802.11 wireless networks: the definitive guide. "* O'Reilly Media, Inc.", 2005.

[13] Fanglu Guo and Tzi-cker Chiueh. Sequence number-based mac address spoof detection. In *International Workshop on Recent Advances in Intrusion Detection*, pages 309–329. Springer, 2005.

[14] Vishal Gupta and Mukesh Kumar Rohil. Information embedding in ieee 802.11 beacon frame. In *National Conference on Communication Technologies & its impact on Next Generation Computing CTNGC*. sn, 2012.

[15] Guido R Hiertz, Dee Denteneer, Lothar Stibor, Yunpeng Zang, Xavier Pérez Costa, and Bernhard Walke. The ieee 802.11 universe. *IEEE Communications Magazine*, 48(1):62–70, 2010.

[16] Christopher Kohlios and Thaier Hayajneh. A comprehensive attack flow model and security analysis for wi-fi and wpa3. *Electronics*, 7(11):284, 2018.

[17] Bastian Könings, Florian Schaub, Frank Kargl, and Stefan Dietzel. Channel switch and quiet attack: New dos attacks exploiting the 802.11 standard. In *2009 IEEE 34th Conference on Local Computer Networks*, pages 14–21. IEEE, 2009.

[18] Thuc D Nguyen, Duc HM Nguyen, Bao N Tran, Hai Vu, and Neeraj Mittal. A lightweight solution for defending against deauthentication/disassociation attacks on 802.11 networks. In *2008 Proceedings of 17th International Conference on Computer Communications and Networks*, pages 1–6. IEEE, 2008.

[19] Dr G Padmavathi, Mrs Shanmugapriya, et al. A survey of attacks, security mechanisms and challenges in wireless sensor networks. *arXiv preprint arXiv:0909.0576*, 2009.

[20] Tanya Roosta, Shiuhpyng Shieh, and Shankar Sastry. Taxonomy of security attacks in sensor networks and countermeasures. In *The first IEEE international conference on system integration and reliability improvements*, volume 25, page 94, 2006.

[21] Stefan Savage, Neal Cardwell, David Wetherall, and Tom Anderson. Tcp congestion control with a misbehaving receiver. *ACM SIGCOMM Computer Communication Review*, 29(5):71–78, 1999.

[22] K. van Brakel. 802.11 availability attacker. `https://github.com/kaspertje100/802.11_Availability_Attacker/blob/master/attacker.py`.

[23] Mathy Vanhoef and Frank Piessens. Key reinstallation attacks: Forcing nonce reuse in WPA2. In *Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS)*. ACM, 2017.

[24] M Vipin and S Srikanth. Analysis of open source drivers for ieee 802.11 wlans. In *2010 International Conference on Wireless Communication and Sensor Computing (ICWCSC)*, pages 1–5. IEEE, 2010.

[25] Yong Wang, Garhan Attebury, and Byrav Ramamurthy. A survey of security issues in wireless sensor networks. *DigitalCommons@University of Nebraska - Lincoln*, 2006.