RP2 - Availability analysis of SURFwireless

Kasper van Brakel

July 4th, 2019

Universiteit van Amsterdam

SURF NET

Introduction

- SURFwireless: Wi-Fi-as-a-Service since 2016
- Aerohive, Hivemanager
- Investigate potential attacks that threaten the availability for clients of SURFwireless

Research questions

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

  Sub-questions:

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

Scope

- Potential attacks must be applicable on 802.11 with WPA2-Enterprise
- The general security of eduroam is out of scope, only investigating attacks on availability
- Only detection and prevention methods of the attacks that can be configured from the Hivemanager were investigated

Related work

- Type of DoS attacks (Bicakci et al.):
  - Radio Frequency(RF) jamming
  - MAC layer attacks
  - Above MAC layer attacks (protocol based i.e. ARP, ICMP, TCP)

- MAC layer Denial-of-Service(DoS) attacks:
  - Deauthentication attack (Bellardo et al.)
  - Channel Switch attack (Könings et al.)
  - Quiet attack (Könings et al.)

Experiments

Parameters:

- iPerf3 and ping
- Experiments performed 30 times for 60 seconds
- Scapy

Experiments:

- Basetest
- Deauthentication attack
- Channel Switch attack
- Quiet attack

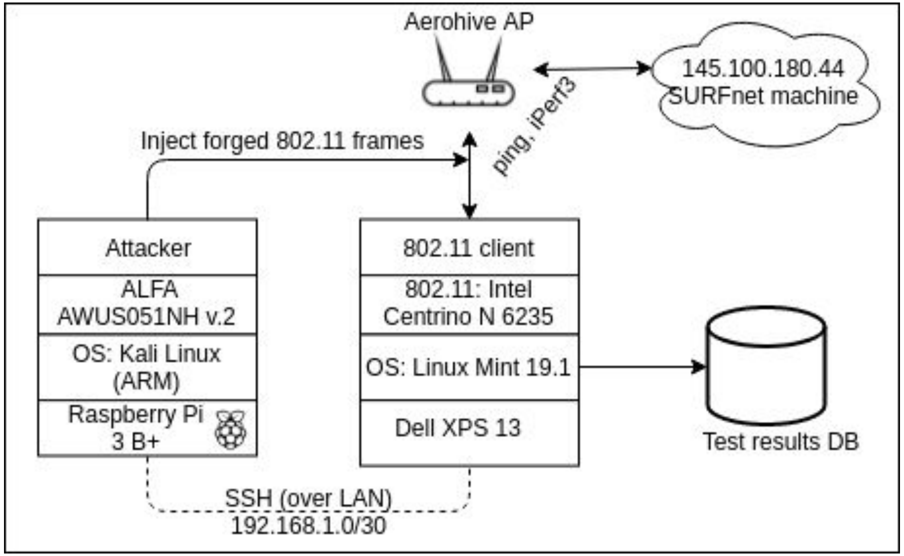


Figure 4: Testbed setup

Deauthentication attack

- Abuses deauth frames

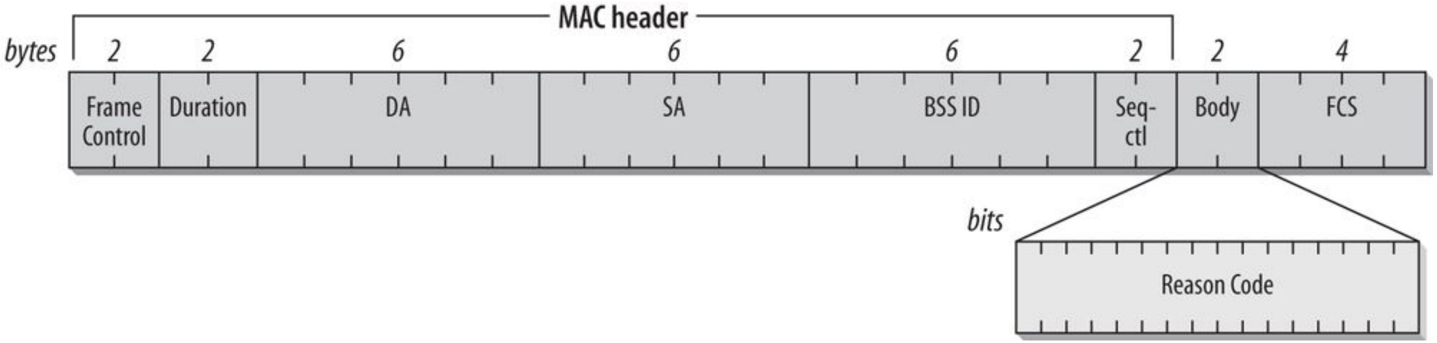
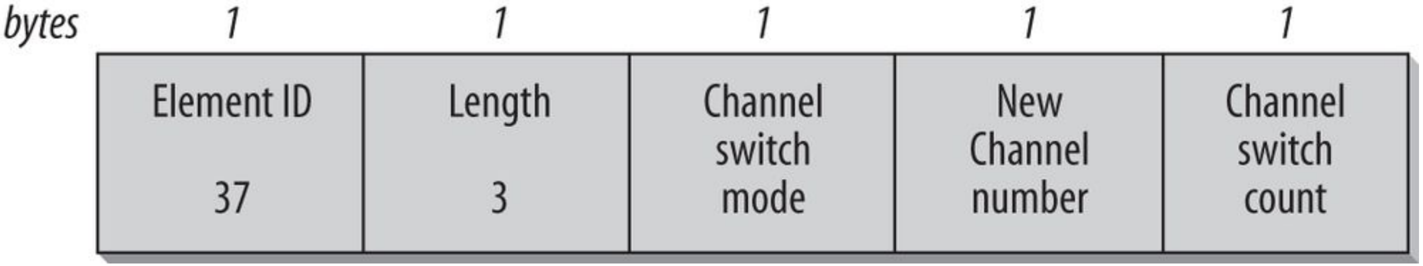


Figure 1: Generic Deauthentication frame. Source: 802.11 Wireless Networks: The Definitive Guide, Oreilly

Channel Switch attack

- Abuses 802.11h amendment
- Transmitted in Beacon, Probe response or action frame

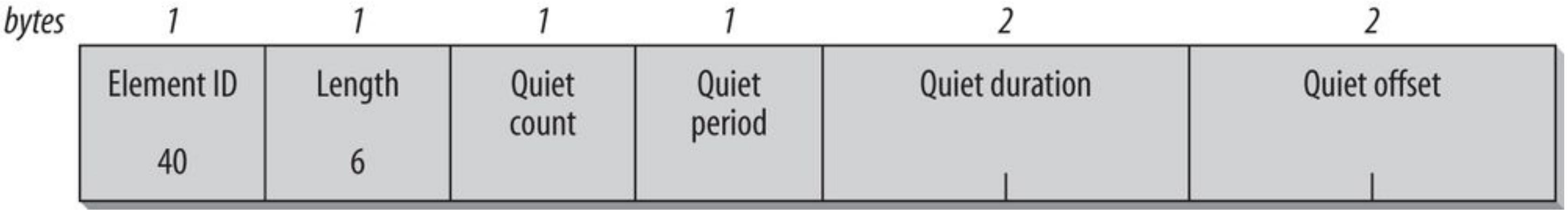


bytes	1	1	1	1	1
	Element ID 37	Length 3	Channel switch mode	New Channel number	Channel switch count

Figure 2: Generic Channel Switch element. Source: 802.11 Wireless Networks: The Definitive Guide, Oreilly

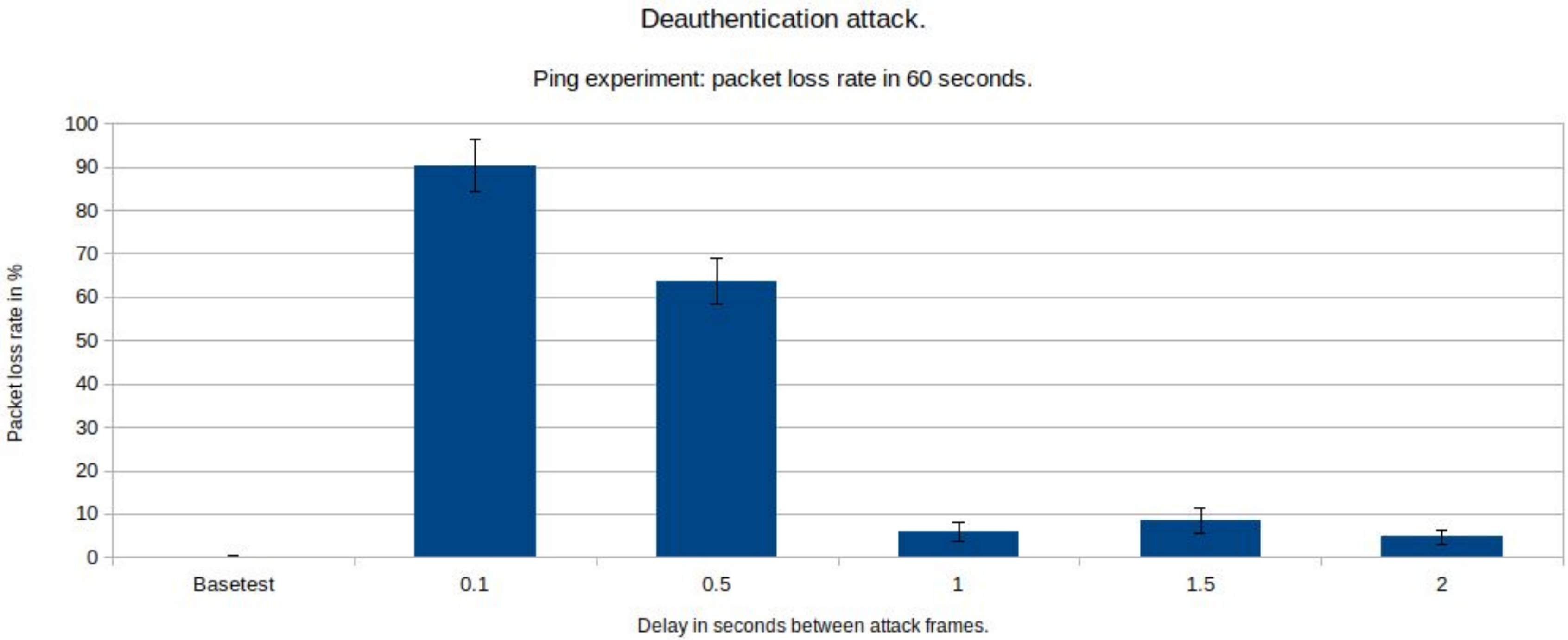
Quiet attack

- 802.11h amendment
- Transmitted in Beacons, Probe response
- Depending on driver implementation clients can be silenced for up to 65535 Time Units



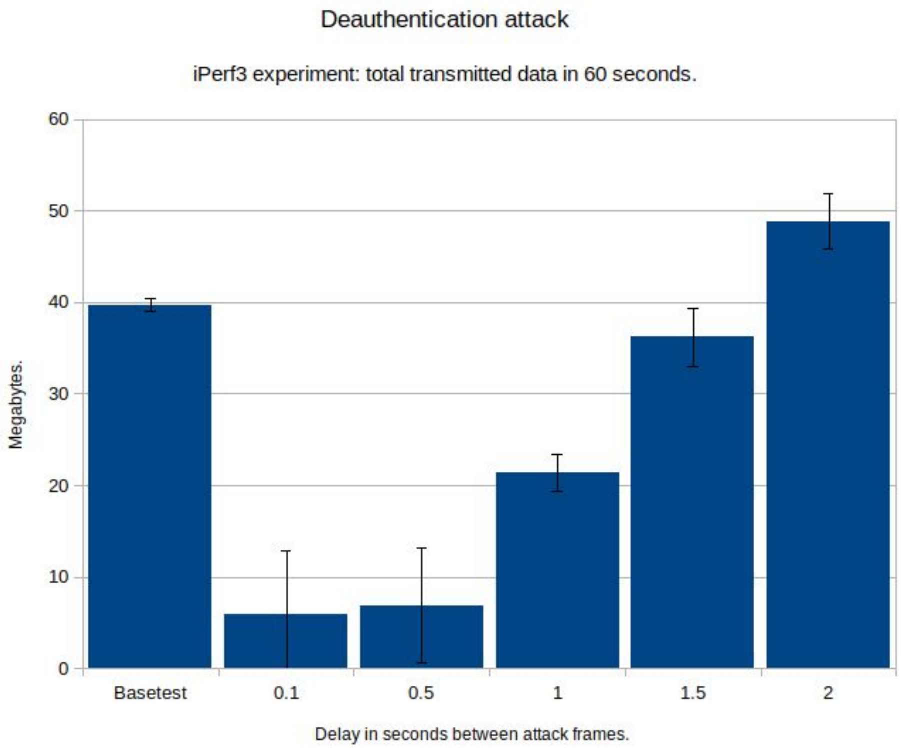
bytes	*1*	*1*	*1*	*1*	*2*	*2*
	Element ID 40	Length 6	Quiet count	Quiet period	Quiet duration	Quiet offset

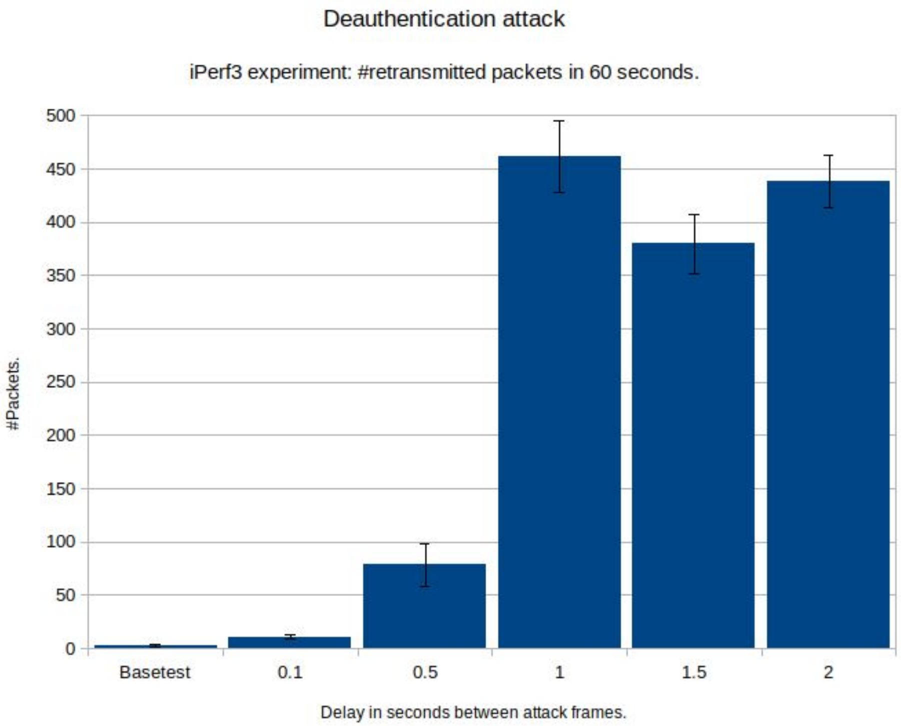
Figure 3: Quiet element. Source: 802.11 Wireless Networks: The Definitive Guide, Oreilly

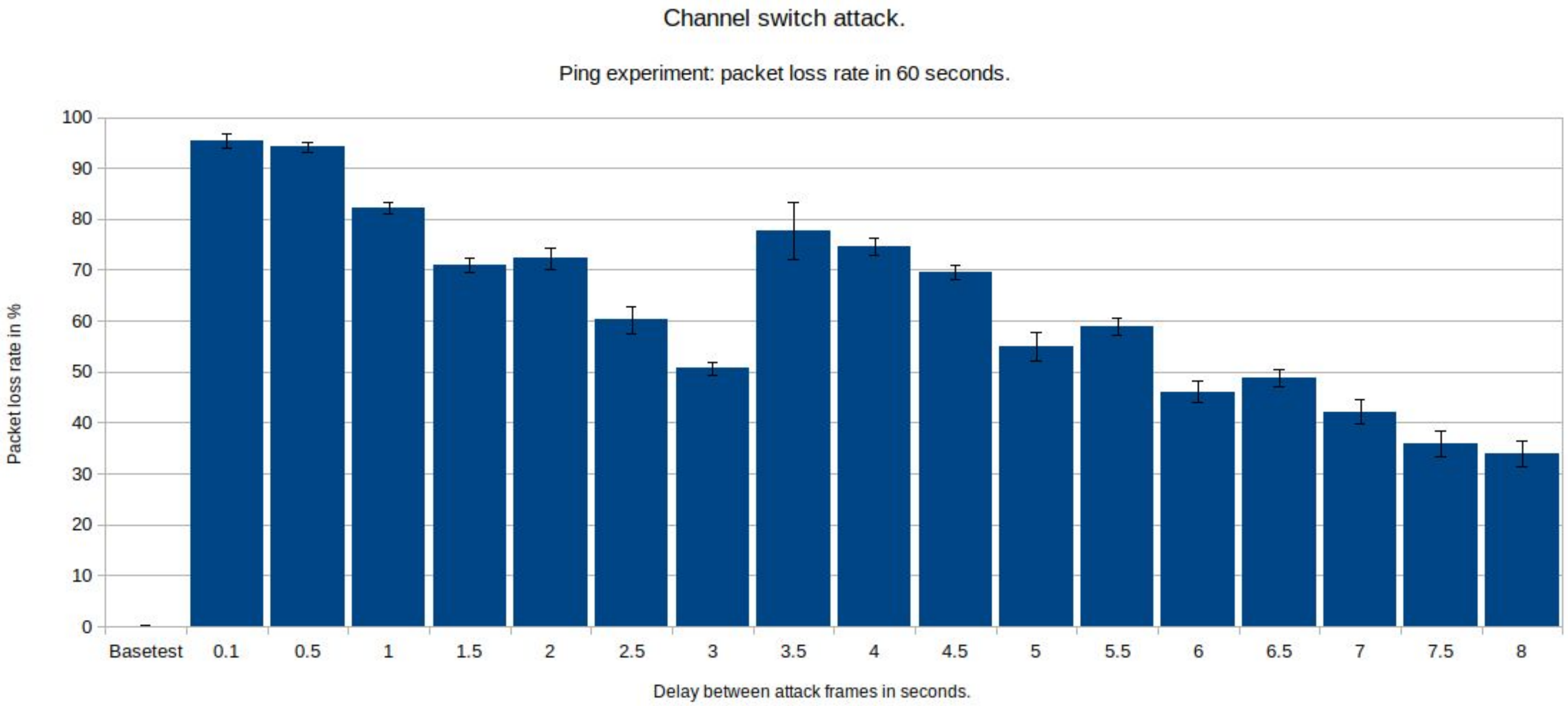


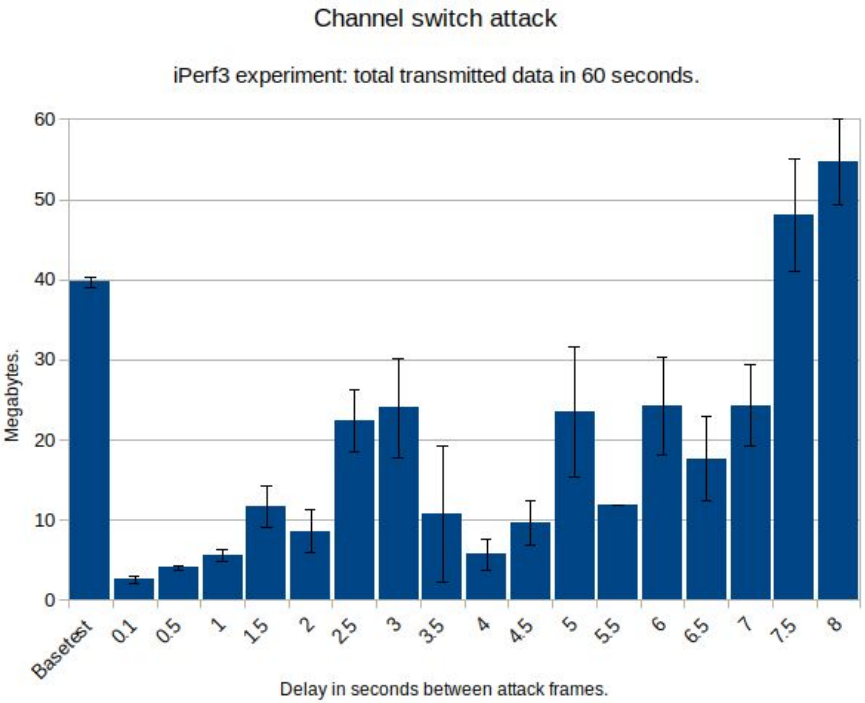
Deauthentication attack.

Ping experiment: packet loss rate in 60 seconds.


Deauthentication attack
iPerf3 experiment: total transmitted data in 60 seconds.
Megabytes.
60
50
40
30
20
10
0
Basetest
0.1
0.5
1
1.5
2
Delay in seconds between attack frames.

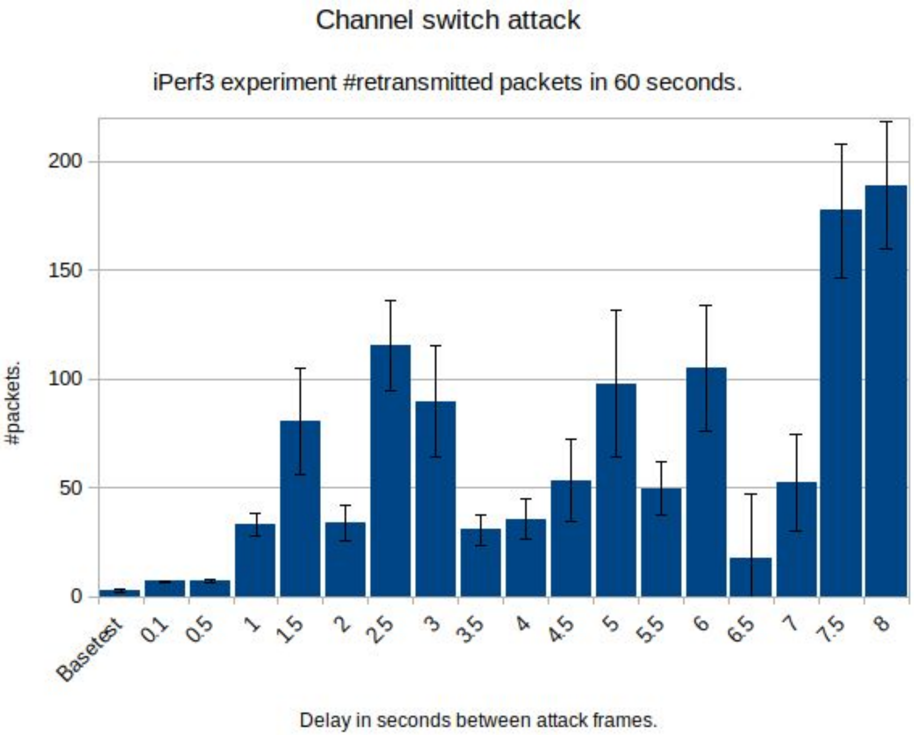

Deauthentication attack
iPerf3 experiment: #retransmitted packets in 60 seconds.
#Packets.
500
450
400
350
300
250
200
150
100
50
0
Basetest
0.1
0.5
1
1.5
2
Delay in seconds between attack frames.


Channel switch attack.
Ping experiment: packet loss rate in 60 seconds.
Packet loss rate in %
100
90
80
70
60
50
40
30
20
10
0
Basetest
0.1
0.5
1
1.5
2
2.5
3
3.5
4
4.5
5
5.5
6
6.5
7
7.5
8
Delay between attack frames in seconds.



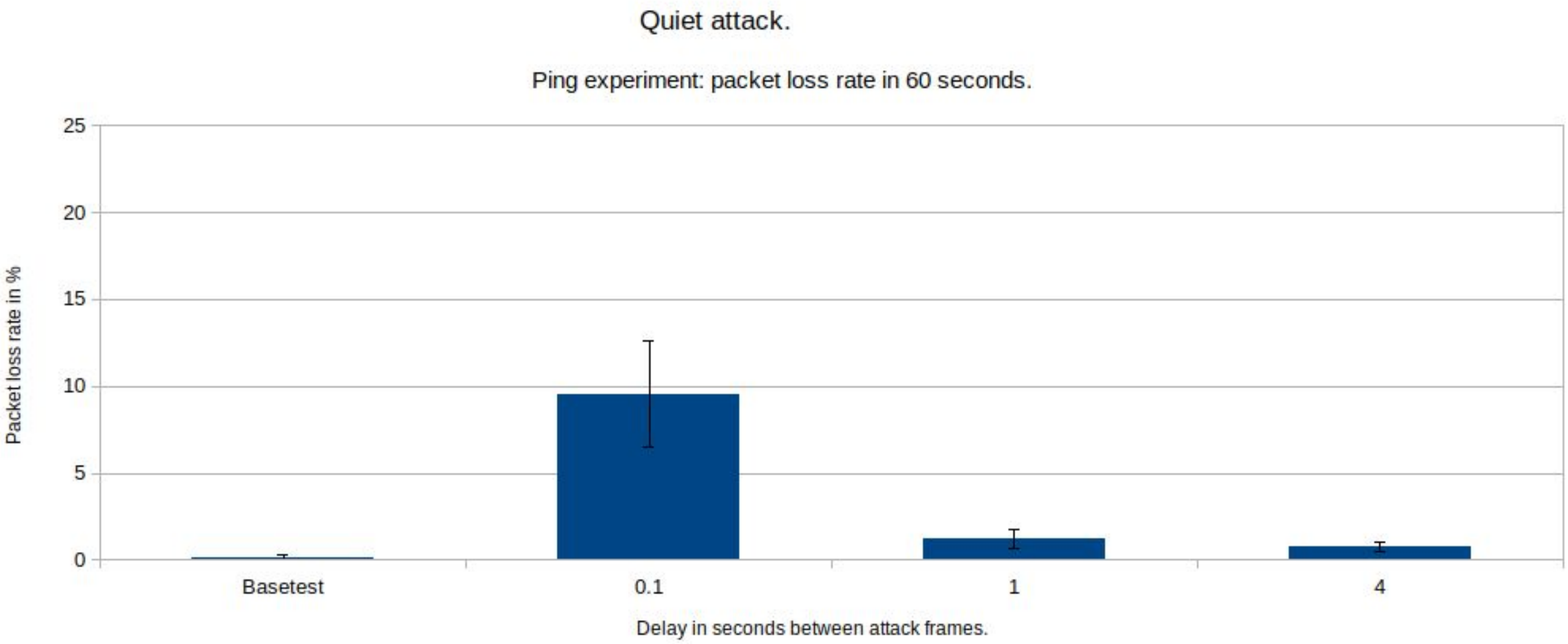
Channel switch attack

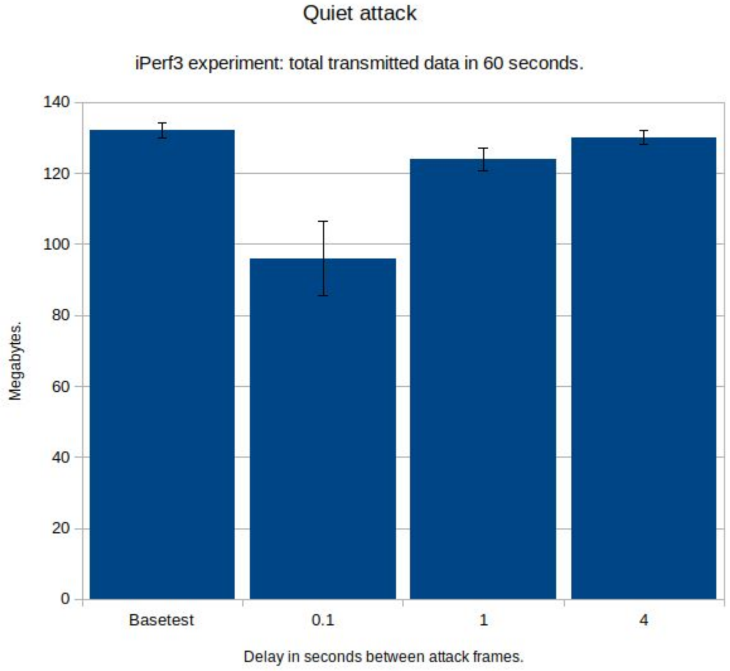
iPerf3 experiment: total transmitted data in 60 seconds.

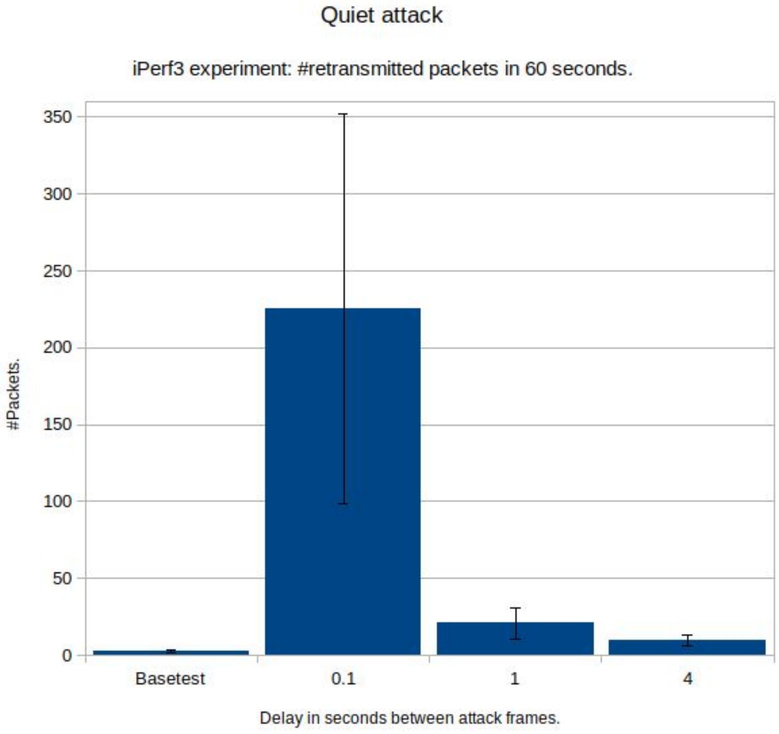


Channel switch attack

iPerf3 experiment #retransmitted packets in 60 seconds.


Quiet attack.
Ping experiment: packet loss rate in 60 seconds.
Packet loss rate in %
25
20
15
10
5
0
Basetest
0.1
1
4
Delay in seconds between attack frames.


Quiet attack
iPerf3 experiment: total transmitted data in 60 seconds.
Megabytes.
140
120
100
80
60
40
20
0
Basetest
0.1
1
4
Delay in seconds between attack frames.


Quiet attack
iPerf3 experiment: #retransmitted packets in 60 seconds.
#Packets.
350
300
250
200
150
100
50
0
Basetest
0.1
1
4
Delay in seconds between attack frames.

Vulnerable devices

- Vulnerable against Deauthentication and Channel Switch attack

Device	**802.11 chip**	**OS**
Dell XPS 13	Intel 6235-N	Linux mint 2019.1
Macbook pro (2017)	Airport card	MacOS 10.14.5
Samsung S10	Broadcom	Android 9
One Plus 6T	Qualcomm	Android 9

Detection

- DoS protection by Aerohive
- Only deauthentication attack was detected

DoS Detection Type	**Alarm Threshold Client** (frames per minute)	**Alarm Threshold SSID** (frames per minute)
Probe Request	1200	12000
Probe Response	2400	24000
(Re) Association Request	600	6000
Association	240	2400
Disassociation	120	1200
Authentication	600	6000
Deauthentication	120	1200
EAP Over LAN (EAPol)	600	6000

Table 1: Overview of default threshold values Hivemanager.

Detection

- Formula:

$$time/attackFrameRate * connectedClients$$

Clients	Attack frame rate															
	0.1	0.5	1	1.5	2	2.5	3	3.5	4	4.5	5	5.5	6	6.5	7	7.5
1	600	120	60	40	30	24	20	17.1	15	13.3	12	10.9	10	9.2	8.6	8
10	6000	1200	600	400	300	240	200	171	150	133	120	109	100	92	86	80

Table 2: Overview of threshold values for Hivemanager per investigated attack frame rate.

Prevention

- 802.11w protects:
  - Robust action frames
  - Deauthentication frames
  - Dissasociation frames

- Channel switch and Quiet attack can both abuse beacon and probe response frames ← not protected

Code:	Action type:
0	Spectrum management
1	QoS
2	DLS
3	Block Ack
5	Radio
6	Fast BSS Transition
8	SA Query
9	Protected Dual of Public Action
126	Vendor-specific Protected

Table 3: Overview of robust action frames from 802.11 specification Source

Discussion

- SSID threshold not variable based on client count
- Quiet attack may potentially work on other devices
- More sophisticated detection methods to determine MAC address spoofing based attacks i.e. by sequence number exists (Guo et al). Source
- For 802.11w protection both client and AP must support it
- Attacks were conducted on a single access point environment

Conclusion

- Deauthentication attack and Channel Switch attack both succeeded
- Impact on the wireless clients depend on used attack frame rate
- Only the deauthentication attack was detected by Aerohive WiPs
- 802.11w protects against deauthentication attack, channel switch and quiet attack remain unaddressed

Future work

- Locate attacker, combining 802.11-based positioning and frame thresholds per AP

- Investigate other relevant attacks that potentially threaten the availability of SURFwireless and determine the threshold value for Aerohive WiPs.

- Investigate the possibility to extend the current 802.11w amendment to support all frames if client is authenticated.

Questions?