ulm university universität
uulm

University of Ulm | 89069 Ulm | Germany

Faculty of
Engineering
and Computer Science
Institute of Media Informatics

Evaluation of the 802.11w Amendment for existing DoS attacks

Bachelor thesis at the University of Ulm

Submitted by: Dominik Lang
dominik.lang@uni-ulm.de

Supervisor:
Prof. Dr.-Ing. Michael Weber

Advisor:
Bastian Könings

2011

Version November 6, 2012

Satz: PDF-LaTeX 2$_\varepsilon$

Contents

1 Introduction

In our current society information is equivalent to power and money. The recent events regarding WikiLeaks show what impact information can have. The basis of our information society is the progress in digital technology and networking. Information lies digitally encoded on computers and these computers are joined to a massive network which forms the internet. This enables information sharing all over the world and defines our everyday life. Today these computers are not just stationary desktop computers; smartphones, PDA's and recently tablets are everywhere. To connect these kinds of devices, traditional wired technology is impracticable. Therefore several wireless network technologies have emerged.

Humans prefer comfort. We want to connect to the internet everywhere we go, without having to carry cables with us. Wireless networks have become very popular, and are extensively used at universities, offices and homes. Furthermore many shops, restaurants and most airports offer hotspots. The heavy employment of wireless networks has the effect that the hardware has become cheap and affordable. As a consequence wireless networks are also used to bring connectivity to the developing world[1].

In a time of increasing cybercrime, infrastructure and connectivity are critical resources. The ubiquity of wireless networks makes them a worthwhile target. Attacking the availability of networks can have major effects. Hence, the security of wireless networks is an important aspect. Unfortunately, the by far most used wireless networking standard 802.11 is subject to critical security vulnerabilities. Enhanced data frame protection was introduced with the 802.11i amendment which offers good authentication as well as increased integrity and confidentiality. But *Denial of Service* (DoS) attacks remain an issue, especially through the unprotected management frames. A new amendment, 802.11w, intends to protect management frames and prohibit DoS attacks. This bachelor thesis analyses and evaluates the 802.11w amendment on existing DoS attacks.

[1] http://www.wndw.net

This thesis is structured into two main parts: Section 2 to Section 5 describe the theoretical part containing an overview of the standards and the attacks, whereas Section 6 to Section 8 describe the practical part including implementation, testing and evaluation.
Section 2 describes some basic formats and structures of the IEEE 802.11 standard. Section 3 moves on to presenting how the standard itself may be exploited to launch DoS attacks on *wireless local area networks* (WLAN). Section 4 then shows how the 802.11w amendment adds protection against DoS attacks. The following Section 5 describes attacks on 802.11w which remain feasible after the amendment as well as those introduced subsequently to it.
Section 6 offers an overview of the implemented tools. While Section 7 gives an overview of the attacks which were tested and the test setup in general, Section 8 shows and evaluates the results of the tests. Finally Section 9 gives a conclusion to the work done in the course of this thesis.

2 Standards Overview

This section explains basic concepts of 802.11 [17] which are integral to understanding the DoS attacks.

The IEEE 802.11 standard is in its core similar to IEEE 802.3 (Ethernet). However, due to the openness and unreliability of the underlying radio medium, it is much more complex and specifies a wide range of management functionality. Consequently 802.11 distinguishes between three different types of frames: Data frames, Control frames and Management frames.
Data frames carry the actual data from higher layers; Control frames help to insure service's reliability; Management frames compensate for the openness of the radio medium, by providing additional mandatory and optional services such as authentication and association.

As the characteristics of the wireless medium suggest, everyone with an appropriate device can transmit and receive signals, contrary to the wired medium, where only those plugged into a jack can do so. Therefore a cryptorphic algorithm termed *Wired Equivalent Privacy* (WEP) was introduced to protect Data frames. Due to flaws in WEP [23, 12, 3, 6, 22, 4, 7] the 802.11i [18] amendment established features to achieve enhanced protection of Data frames. However, the designers left the Management frames unprotected. As a result, wireless networks are still vulnerable to DoS attacks.

Throughout this thesis the term *Robust Security Network* (RSN) refers to the *CTR*[1] *with CBC-Mac Protocol*[2] (CCMP) - one of the two data confidentiality protocols introduced by 802.11i [18] - unless otherwise specified.

[1] counter mode
[2] cipher-block chaining message authentication code

2.1 Spectrum Management

Originally IEEE 802.11 operated solely in the 2.4 GHz frequency spectrum, with 1.0 Mb/s and 2.0 Mb/s data rates. In 1999 the 802.11b [15] amendment allowed data rates of 5.5 Mb/s and 11Mb/s in the 2.4 GHz frequency spectrum. In the same year the 802.11a [14] amendment added additional channels in the 5 GHz spectrum. 802.11a allows data rates of up to 54 Mbit/s. However, in Europe the 5 GHz frequency spectrum is also used for aeronautical, satellite and military services. The *European Conference of Postal and Telecommunications Administrations* (CEPT) therefore decided in ERC/DEC/(99)23 [10], now replaced by ECC/DEC/(04)08 [9], that certain conditions must be met to transmit in the 5 GHz frequency spectrum. The specific requirements are defined in the *European Telecommunications Standards Institute's* (ETSI) EN 301 893 [11] and consist of *Transmit Power Control* (TPC) and *Dynamic Frequency Selection* (DFS), which are described in the following subsections. Because 802.11a does not comply with these conditions, another amendment was needed. In 2003 802.11h [16] was ratified which incorporates these two necessary mechanisms. TPC and DFS are now mandated by WRC-03 [9].

Dynamic Frequency Selection

DFS provides support for testing channels for the presence of radar and reacts appropriately, for example by switching the channel to one without radar interference.

Transmit Power Control

TPC provides support for regulating the transmit power. At first TPC was used to utilize regulatory requirements. However, TPC can be used to adapt to certain conditions: transmit power can be boosted when high path losses are detected. Whereas it can be reduced when less power is needed, which is very convenient for mobile devices.

2.2 Authentication and Association State machine

The Authentication and Association State machine consists of three states, as seen in Figure 2.1.

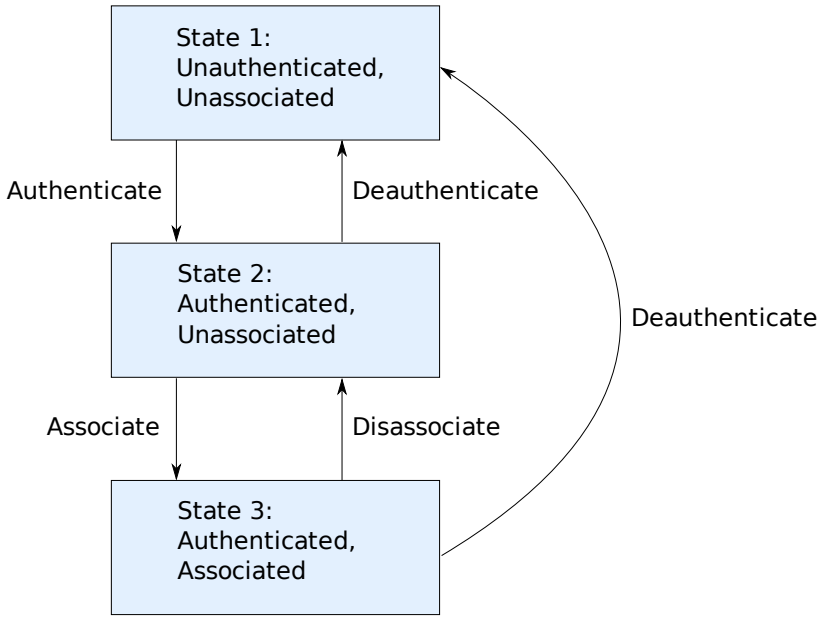

Figure 2.1: Authentication and Association State machine

A *wireless station* (STA) entering a wireless network starts off in State 1. The first step is to authenticate itself to the *access point* (AP). After a successful authentication, the STA's state is set to State 2. The STA will then associate itself with the AP and, if successful, can move on to State 3. In an RSN, RSN authentication and key exchange take place next.
After performing all these steps the STA is connected to a wireless network and can begin transmitting Data frames. Data frames can only be transmitted in State 3.

When moving in the opposite direction through the state machine, there are two possible operations: disassociation and deauthentication. Disassociation moves the state machine from State 3 to State 2, whereas deauthentication changes the state from State 2 or 3 to State 1. Because authentication is a prerequisite of association, deauthentication automatically disassociates an STA.
Deauthentication and disassociation take place without a response. The sending STA changes its state accordingly immediately. Consequently receiving STAs have no other

choice than to accept Deauthentication and Disassociation frames. Therefore 802.11 specifies that deauthentication and disassociation are notifications, not requests [17].

2.3 Frame formats

2.3.1 General frame format

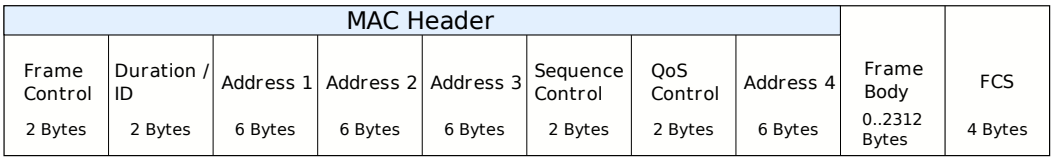

Figure 2.2: General frame format

Figure 2.2 depicts the general structure of IEEE 802.11 MAC frames. A frame begins with a MAC Header, which consists of the fields *Frame Control* (FC), Duration / ID, Address 1, Address 2, Address 3, Sequence Control, *Quality of Service* (QoS) Control, Address 4, Frame body and *frame check sequence* (FCS). Not all frames have all of these fields, merely the first three and the FCS fields are mandatory.
Two fields of the Frame Control field are of interest here, namely To DS[3] and From DS. They specify in which direction the frame is to be sent, from a STA to an AP, or from an AP to a STA respectively.

The following sections describe in more detail the format of some particular Management frames which are of heightend importance for the purpose of this bachelor thesis, as well as the *information elements* (IE) which are one of the basic components of these frames[4].

2.3.2 Information elements

Future changes have always been considered likely in the IEEE 802.11 standard and there already have been a number of amendments. To make things easier the frame body was designed for extensibility. All management information is stored in so-called information

[3] distribution system
[4] For more information see the IEEE 802.11 Standard [17].

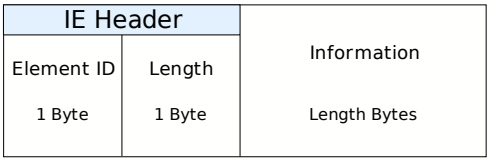

Figure 2.3: Information element format

elements, Figure 2.3. IEs consist of two header fields and a body. The header fields specify the type of IE and the length of the IE body. With this structure, a management frame can have as many IEs as are needed. IEs may also be defined as optional and amendments can add IEs to management frames.

Quiet IE

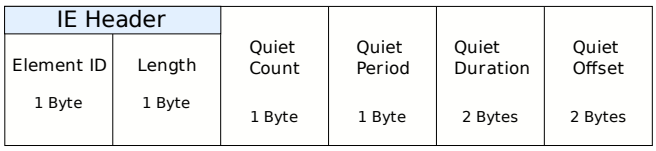

Figure 2.4: Quiet IE

The Quiet IE is used to silence the channel for measurement purposes.
Its Length field is 6.
The Quiet count field defines the number of *target beacon transmission times* (TBTT), which is the interval at which the AP sends its beacon frame, up until the beacon interval during which the quiet interval begins.
The Quiet Period field defines a periodic interval of quiet intervals.
The Quiet Duration field defines the length of the quiet interval.
While the Quiet Offset field defines at what point during a beacon interval the quiet interval will begin.

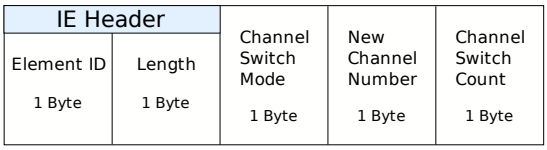

Figure 2.5: Channel Switch Announcement IE

Channel Switch Announcement IE

The Channel Switch Announcement IE is used to announce that the AP and therefore the WLAN is going to change the channel and when this switch will occur.
Its Length field is 3.
The Channel Switch Mode defines if STAs are allowed to transmit until the channel switch or if they shall be quiet.
Additionally the New Channel Number specifies the new channel to which a STA shall move to.
The Channel Switch Count field defines the number of TBTTs until the channel should be switched.

Supported Rates IE

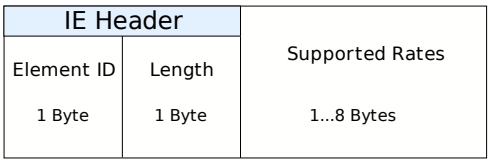

Figure 2.6: Supported Rates IE

Up to eight supported rates may be specified in the frame body of the Supported Rates IE. Each rate is defined in one byte and at least one supported rate must be given. The rates are encoded in 500 kb/s units and rounded up if necessary.

IEs used by DFS

DFS is based on the following IEs:

- Supported Channels
- Channel Switch Announcement
- Measurement Request
- Measurement Report
- Quiet
- IBSS DFS

When measuring a channel, the channel can be quieted by the AP with the Quiet IE. An AP can request other STAs to conduct a test by sending a Measurement Request to them. After finishing a test, an STA responds with a Measurement Report. If the tests yield the presence of radar the channel can be switched with the Channel Switch Announcement.
In addition, associations from STAs can be accepted or rejected based on the Supported Channels.

IEs used by TPC

TPC is based on the following IEs:

- Power Constraint
- Power Capability
- TPC Request
- TPC Report

An AP can advertise the regulatory maximum transmit power in its Beacon frame with a Power Constraint IE. It may also reject an STA's association based on the advertised Power Capability of the STA.
A STA can dynamically adapt its transmit power by observing the path loss and estimating the link margin. Furthermore it can send a TPC Request IE to ask for another STA's path loss and link margin values which will then receive a TPC Report IE in return.

2.3.3 Management frame formats

MAC Header						Frame Body	FCS
Frame Control	Duration / ID	Destination Address	Source Address	BSSID	Sequence Control		
2 Bytes	2 Bytes	6 Bytes	6 Bytes	6 Bytes	2 Bytes	0...2312 Bytes	4 Bytes

Figure 2.7: Management frame format

In Management frames there are no Quality of Service and Address 4 fields. Address 1 field contains the *Destination Address* (DA), the Address 2 field contains the *Source Address* (SA) and Address 3 contains the *Basic Service Set Identifier* (BSSID) which indicates the specific WLAN the frame belongs to.

All further described frames have the MAC Header in common and only their frame body is depicted in the following figures.

Deauthentication and Disassociation frame formats

2 Bytes	Reason Code
0...2310 Bytes	Vendor Specific

Figure 2.8: Deauthentication frame format

Deauthentication and Disassociation frames primarily contain one field in their body: Reason Code. The Reason Code field states the reason for the deauthentication or disassociation.
Multiple Vendor Specific IEs may follow.

Association Request frame format

For this bachelor thesis the Supported Rates and the RSN IEs are worth noting. The Supported Rates field specifies up to eight of the data rates supported by the associating

Capability	Listen interval	SSID	Supported Rates	Extended Supported Rates	Power Capability	Supported Channles	RSN	QoS Capability	Vendor Specific

Figure 2.9: Association Request frame format

STA. More rates can be added in the Extended Supported Rates IE if necessary.
RSN Capabilities, such as supported cipher suites and *authentication and key management* (AKM) suites are specified in the RSN IE.

Action frame format

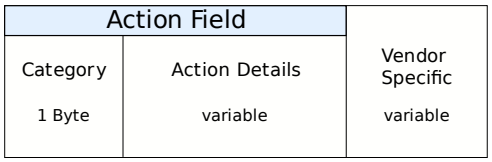

Figure 2.10: Action frame format

Action frames were introduced by the 802.11h amendment [16]. The idea is to allow management functionality other than connection management, such as authentication and association or discovery services. 802.11h specifies five different Action frames:

- Measurement Request
- Measurement Report
- TPC Request
- TPC Report
- Channel Switch Announcement

The Category field specifies the type of Action frame and therefore the meaning of the subsequent bytes. Whereas the Action Details field contains the actual data specific to the Action frame type. Multiple Vendor Specific IEs may follow at the end.

3 Attacks

Denial of Service attacks on 802.11 can be categorized into two sections: *Radiofrequency-Jamming* (RF-Jamming) and *Medium-Access-Control-Layer* (MAC-Layer) attacks. Since the transmission medium of wireless networks consists of the radiofrequency spectrum, jamming a network can be done by continuously transmitting random data to increase the noise on the given channel. The medium is then jammed and no more useful data can be sent or received. These kind of attacks are called RF-Jamming attacks and require nothing but a transmitter. These attacks are easy to perform, usually have a high impact and are difficult to defend against. However, there are a few countermeasures and the probability of detection is high. Furthermore, a lot of power is needed to transmit continuously.

Attacks aimed at the MAC-Layer of 802.11 are more subtle. Instead of jamming they attack the state machine of the 802.11 MAC-Layer protocol. A common goal is to set an STA into the deauthenticated state at either the AP or the STA. Other attacks make use of the DFS and TPC mechanisms.

The focus of this thesis lies on the DoS attacks at the MAC-Layer[1].

3.1 Deauthentication attack

The Deauthentication attack is the most widely known DoS attack on 802.11. As described in Section 2.2, an STA new to a network starts off in the unauthenticated state. After authenticating itself it moves on to the authenticated state. If the network is an RSN the RSN authentication procedure can now start.
When leaving a network an STA sends a Deauthentication frame and sets the state back to the unauthenticated state at both its own state machine and the AP's state machine. Deauthentication frames are Management frames and are therefore sent in the clear without any

[1] See Könings [21] for a complete discussion of DoS attacks on 802.11.

protection. By forging a Deauthentication frame an attacker can deauthenticate a targetted STA. This can be done in both directions: from DS and to DS.

A similar attack is the Disassociation attack. The difference is that a Dissasociation frame is sent instead of a Deauthentication frame. However, the recovery is faster because the state machine is still in the authenticated state.

Although these attacks have been long known, Bellardo et al. [5] were the first to describe and analyse these attacks in a technical paper in 2003. However, they also note that these attacks are not novel and reference three existing implementations.

3.2 Association Request attack

Ahmad et al. [2] describe vulnerabilities which they term the Autoimmunity Disorder of WLANs. This name derives from the fact that APs try to handle inacceptable packets appropriately by rejecting STAs that do not possess the capability of operating in the WLAN. Frames containing capability information are however management frames and can therefore be forged.

802.11 specifies that an AP may reject associations from STAs with unacceptable capabilities such as Basic Rate Set or inappropriate RSN IE. Thus if an STA is authenticated and sends an Association Request frame with invalid Supported Rates values the AP may reject the association and change the state to unauthenticated for that STA.
Therefore an attacker could forge an invalid Association Request frame and deauthenticate a target STA.

3.3 Quiet attack

As described in Section 2.3.2, DFS provides the mechanism to silence the channel for measurement, by using the Quiet IE. An AP may send a Quiet IE in its periodic Beacon frame to announce the quiet interval.
Könings [21] showed that an attacker can forge a Beacon frame containing a Quiet IE to silence the WLAN for up to 67 seconds. However, very few drivers implement the Quiet functionality.

3.4 Channel Switch attack

Similar to the Quiet attack, Channel Switch Announcements can be sent in a Beacon Frame. Könings [21] showed that an attacker can forge a Beacon Frame containing a Channel Switch Announcement and direct STAs to change the channel. Furthermore, by setting the Channel Switch Mode to 1 the attacker can force the STAs to be silent until the channel switch occurs.
By changing to a channel which is out of reach of the AP's channel the AP and the targetted STAs are not able to communicate, resulting in an effective DoS state.

4 802.11w

As noted above, the 802.11i [18] amendment does not include protection for Management frames. The purpose of 802.11i is to provide confidentiality of user information. It was very quickly discovered that WEP does not provide the services it guarantees [23, 12, 3, 6, 22, 4, 7]. Consequently a fast amendment was needed to supercede WEP; thus 802.11i emerged.
User data is protected by 802.11i, but as described earlier, vulnerabilities based on management frames and control frames remain.
It is a difficult task to protect management and control frames which are used to guarantee the correct functioning of a wireless network. For example:

- It must be possible for Deauthentication frames to be sent in order to reject non-authorized STAs before any *security association* (SA) is completed.
- Certain management and control frames need to be received by every STA on the channel in range, as well as by STAs in different WLANs.

Originally management frames did not carry any interesting data. However, the amendments 802.11k Radio Ressource Measurement, 802.11r Fast Basic Service Set Transition and 802.11y 3650-3700 MHz Operation in USA transfer more and more information into Management frames. This makes Management frames a worthwhile target. See Appendix A for a short overview of the aforementioned amendments.

In 2005 a project planning to develop an amendment providing management frame protection was approved. The resulting amendment was titled 802.11w [19] and was finally approved in 2009.
The novelty of 802.11w is that it provides protection for certain Management frames. These protected Management frames are called Robust Management Frames.

A 802.11w STA possesses two new flags to express their Management Frame Protection Capability:

- Management Frame Protection Capable (MFPC)
- Management Frame Protection Required (MFPR)

If an AP sets both MFPC and MFPR, only STAs with at least MFPC set can connect to the WLAN.

Depending on whether the frames are unicast or multicast frames, Robust Management Frames provide different kinds of protection.
Deauthentication, Disassociation, certain Action and Public Action Frames all are Robust Management Frames.

4.1 Unicast Protection

Unicast Robust Management Frames are protected by CCMP in the same manner as unicast Data frames. Therefore data confidentiality, authentication, integrity, and replay protection is guaranteed.

4.1.1 SA Query

To protect against the Association Request attack, 802.11w specifies the SA Query procedure, as seen in Figure 4.1. When receiving an Association Request frame from an STA for which it holds an SA, the AP rejects the association with the Status Code field set to ”Association request rejected temporarily; try again later”. Additionally, a new field called ”Association Comeback time” is defined in the *Timeout Interval information element* (TIE) and set accordingly in the Association Response. This field specifies how long the associating STA shall wait until it may reattempt to establish an association. During this time the AP tries to detect whether an SA is in place with the apparently associating STA by issuing the following described procedure.
The AP begins the SA Query procedure by sending a protected SA Query Request to the STA. If the STA does not answer with a correct SA Query Response the AP sets its state with the STA to unauthenticated, deletes its SA and accepts the next Association Request as a valid request.
Otherwise the SA Query procedure is restarted upon receiving the next Association Request.

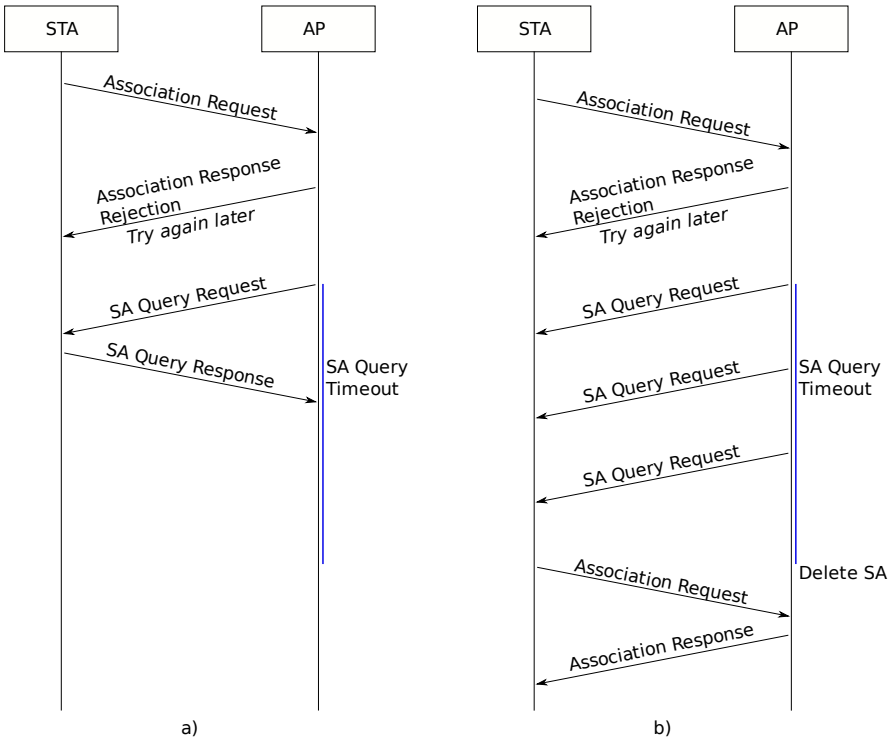

Figure 4.1: SA Query Procedure: a) STA confirms the SA; b) no response from STA, the AP therefore assumes the SA is invalid and deletes it.

4.2 Multicast Protection

For Broadcast Robust Management Frames 802.11w specifies a new integrity protocol called *Broadcast Integrity Protocol* (BIP). In order to realize BIP, a new *Management MIC IE* (MMIE) was introduced. The MMIE contains a KeyID, *Integrity Packet Number* (IPN) and a *Message Integrity Code* (MIC) as depicted in Figure 4.2.

IE Header		KeyID	IPN	MIC
Element ID	Length			
1 Byte	1 Byte	2 Bytes	6 Bytes	8 Bytes

Figure 4.2: Management MIC IE (MMIE)

4.2.1 Broadcast Integrity Protocol

BIP adds replay and integrity protection to broadcast management frames.

Replay protection uses the IPN in the MMIE as a sequence counter. If the received IPN is less than or equal to the locally saved current IPN, the frame was replayed and therefore must be discarded. The IPN is also protected by the integrity protection.

Integrity protection is conducted by adding a MIC created by using AES-128 in *Cipher-based Message Authentication Code* (CMAC) Mode [20] over *Additional Authenticated Data* (AAD) and the Management frame body. It is then stored in the MMIE MIC field. Upon receival of each broadcasted Robust Management Frame the MIC is recomputed and checked against the received MIC. If they are not identical the received frame is discarded. The Key for the MIC computation is called *Integrity Group Temporal Key* (IGTK) and is distributed during the 4-Way Handshake or the Group Key Handshake.

The AAD extends the integrity protection to the frame header. The header cannot be included into the MIC computation as is, because it contains fields that may change with retransmissions. Particularly it is a copy of the FC, Address 1, Address 2 and Address 3 fields of the frame header, with the exceptions of the Retry, Power Management and More Data bits in the FC field masked to zero.

4.3 Cisco CCXv5 MFP

A proprietary version of an early draft of 802.11w was implemented by Cisco and added to the Cisco Compatibility Extensions program CCXv5. The MFP capability is advertised with a Vendor Specific IE. An RSN is required; either *Temporal Key Integrity Protocol* (TKIP) or CCMP. Deauthentication, Disassociation and QoS Action frames are protected with the same protection as Data frames [8]. To protect against broadcast attacks, Cisco MFP forbids broadcast Deauthentication, Disassociation and Action frames and specifies that these must be dropped on receival [8]. However, Cisco MFP does not protect against Association Request attacks. Given that the Channel Switch and Quiet functionalities are implemented, the respective attacks should also be possible in theory. This was however not tested and therefore cannot be verified in the scope of this thesis.

5 Attacks against 802.11w

Channel Switch and Quiet attacks

The same Quiet and Channel Switch attacks, as described in Section 3.3 and Section 3.4 respectively, still work in 802.11w protected networks when launched in Beacon frames. Furthermore, some drivers fail to switch back to the correct channel without disconnecting; others do not switch back at all. As a result the STA's state is set back to the unauthenticated State 1. In this state an STA is vulnerable to all the attacks 802.11w protects against, because the protection can only be guaranteed after the RSN 4-Way Handshake in State 3. A Channel Switch attack could thus be used as an opener attack.

SA Query attack

Ahmad et al. [1] describe how the SA Query procedure can be circumvented by jamming the target STA during the SA Query procedure. If successful, the STA is set into the unauthenticated state at the AP and without an SA in place the target STA is vulnerable to conventional DoS attacks without 802.11w protection. Furthermore, the AP deletes the SA state with the target STA and therefore cannot decrypt frames sent by the target STA. However, the target STA keeps sending encrypted frames. Hence the AP answers with an unprotected Deauthentication frame, which the STA discards because it is not protected. The AP and the STA are now in a Deadlock situation.

BIP insider attack

Due to the fact that every authorized STA in an 802.11w protected WLAN possesses the IGTK, an insider can launch multicast attacks such as a broadcast Deauthentication attack against STAs in the WLAN.

Association Starvation attack

As described in Section 4.1.1 an Association Request may be rejected with the Association Comeback Time field set. Ahmad et al. [1] show that an attacker can forge such an Association Response with the maximum value set in response to an Association Request by the target STA.

EAPOL-Logoff attack

By forging *Exentsible Authentication Protocol over LANs Logoff* (EAPOL-Logoff) frames an attacker can delete the target's 802.1X state [1].

6 Implementation

This section gives an overview of the implementation of several chosen attacks.
The attacks were selected by weighing two factors; how renown and easy an attack is and whether Cisco CCXv5 MFP or 802.11w provide protections against them.
The Deauthentication attack was chosen because of its simplicity and due to being widely known. Cisco CCXv5 MFP does not protect against the invalid Association Request attacks [2] whereas 802.11w does, so this attack, too, was implemented. Additionally, neither 802.11w nor Cisco CCXv5 MFP provide protection against Channel Switch and Quiet attacks, therefore they were both also implemented.
The tests were conducted to verify the aforementioned assumptions as well as also test the actual implementations and the possible impact of the attacks.

Two tasks must be accomplished to successfully implement the attacks: frame capturing and injection. Frame capturing is necessary in order to inspect and analyse the network.
To capture frames, a way of obtaining raw input packets from the kernel is necessary. *Berkeley Software Distribution* (BSD) platforms provide the *BSD Packet Filter* (BPF) kernel interface with which the userland can access, filter and inject raw packets. Libpcap provides an easier-to-use abstract C interface to these mechanisms on BSD platforms. BPF and libpcap were originally designed with tcpdump in mind, however BPF has become a standard in BSD platforms and libpcap has been ported to various other platforms. There has also been a lot of effort in writing wrapper libraries to libpcap for many common programming languages. Libpcap was used for both tasks, capturing and injection, in all implementations realized over the course of this bachelor thesis.
To inject a packet it must first be constructed. After handing it over to libpcap it is passed on to BPF. BPF then hands the packet through the network stack to the specific *Network Interface Card* (NIC) driver, which injects the packet.

6.1 Attack tools

Several tools were implemented as part of this thesis to test and analyse 802.11 networks.

deauthattack

This tool performs Deauthentication attacks. The behaviour of the attack can be altered in the following ways:

- Reason Code can be set
- The direction of the attack
- The interval at which Deauthentication Frames are sent
- The number of Deauthentication frames which should be sent
- Monitor the channel and only reinject Deauthentication frames when the target STA tries to reconnect

assocreqattack

This tool performs Association Request attacks. The behaviour of the attack can be altered in the following ways:

- The direction of the attack
- The interval at which Association Request Frames are sent
- The number of Association Request Frames which should be sent
- Adding RSN IE without 802.11w
- Adding RSN IE with 802.11w

beaconattack

This tool performs Quiet and Channel Switch attacks. It does this by monitoring the network until a Beacon frame of the target WLAN is found and then modifies it by adding a Quiet or Channel Switch IE.

6.2 Monitor and analysis tools

This subsection briefly outlines the tools implemented to monitor the network.

framecap

The framecap tool monitors the channel the interface is set on and breaks down Association Request, Association Response, Deauthentication and Beacon Frames into their basic elements.

monitor

The monitor tool monitors the channel the interface is set on and prints in order what kind of frames are sent over the air, similar to tcpdump but specialised in 802.11 frames.

wlstat

Wlstat takes an interval as its parameter and analysis a pcapdump[1] file. It outputs how many packets and how many bytes have been transmitted during each interval, similar to tcpstat.

6.3 Other tools

Attack tools

Additionally to the tools described above, an attack tool by Könings [21] was also used. Könings 802.11 DoS attack tool implements the Channel Switch attack using Action Frames.

Monitor tools

The well-known tcpdump tool was employed to capture sniffed data for later analysis.

[1] Data captured by libpcap and saved to a file.

7 Testing

A frame can be received by an STA or by an AP. APs and STAs receive different kinds of frames, therefore they are open to various kinds of attacks.
The attacks have been categorized into whether an AP or an STA receives the attackframe.

In this thesis the Association Request, Deauthentication, Quiet and Channel Switch attacks were tested and analysed, the first of which is an AP attack with the rest of them being STA attacks.

7.1 Test Setup

7.1.1 802.11w Implementations

Although 802.11w has been ratified in 2009 the support it received ranges from very poor to nonexistent. During an extensive market research for 802.11w capable products within the scope of this thesis no vendor was found to have implemented 802.11w.

In contrast, the Open Source world is ahead in this respect. Various BSD systems have already implemented 802.11w in their network stack. The OpenBSD[1] operating system was used for a reference implementation on a BSD system.
Multiple Linux drivers support 802.11w, especially drivers using mac80211[2] framework in combination with Jouni Malinens' wpa_supplicant for STAs and hostapd[3] for APs, which implement the client STA and AP RSN functionality respectively.
However, it is not a trivial task to get 802.11w up and running.

Although OpenBSD has implemented 802.11w in their network stack the drivers do not yet use it. To get an OpenBSD STA to use the 802.11w code, modifications had to be

[1] http://www.openbsd.org/
[2] http://wireless.kernel.org/en/developers/Documentation/mac80211
[3] http://hostap.epitest.fi/

made to the network stack and to the drivers used for testing as a prerequisite for the test setup created for this thesis. Following a comprehensive driver source code review the modifications to the drivers comprised of setting an MFPC flag in the drivers attach-routine. The network stack kernel code review was more elaborate; the necessary modifications amounted to setting MFP flags after the IGTK was received in message three of the 4-Way Handshake.

The Linux ath9k driver already supports 802.11w management frame protection. However, some older NICs supported by ath9k are not capable of MFP hardware encryption and the drivers needed to be loaded with software encryption, as seen below, in order to establish the STAs 802.11w capability. This warranted an extensive examination of the documentation and several mailing lists in order to find the following command:

```
# modprobe ath9k nohwcrypt=1
```

OpenWrt [4] is an open source project with a directive of running Linux on embedded devices, mainly routers. It is capable of 802.11w in combination with the ath9k driver and hostapd and was found to need no further modifications for the test setup.

7.1.2 802.11w Stations

A total of four systems were used in two different setups for 802.11w testing. The systems are:

- OpenWrt Backfire 10.03.1[5] with hostapd v0.8.x on top of an ath9k driver as an AP.
- Linux Ubuntu 10.04 with hostapd v0.7.3 on top of an ath9k driver snapshot 2011-06-01 as an AP.
- Modified OpenBSD 4.8 with an iwn driver as an STA.
- Linux Ubuntu 10.04 with wpa_supplicant v0.7.3 on top of an ath9k driver snapshot 2011-06-01 as an STA.

The first setup consists of the OpenWrt AP, the OpenBSD STA and the Ubuntu STA, while for the second setup a different AP was chosen with the Ubuntu AP and the OpenBSD STA.

[4] https://openwrt.org/
[5] http://wiki.openwrt.org/toh/tp-link/tl-wr941nd

7.1.3 General Setup

The test scenario is constituted of an AP, an Attacker STA, a Ping STA, a Monitor STA and the Target STAs, as shown in Figure 7.1. All tests where conducted on channel 1 in the 2.4 GHz frequency spectrum.

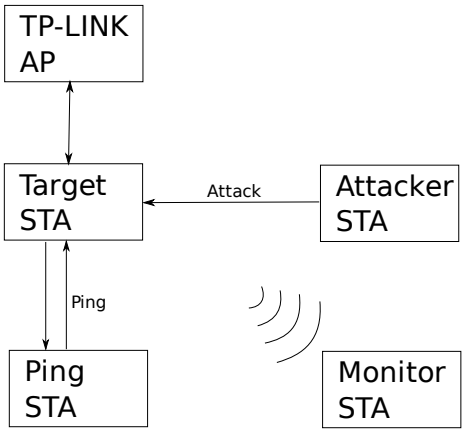

Figure 7.1: Test Setup

Access point

For STA testing the AP was implemented as an OpenWrt TPLink router as described in Section 7.1.2. In the 802.11w setup an OpenWrt and an Ubuntu AP were used, as described in Section 7.1.2.

Ping Station

The Ping STA was directly connected to the AP via cable and employed Linux Ubuntu 10.04. The aim of the Ping STA is to generate traffic to visualize the impact of DoS attacks. The specific command executed to achieve this was:

```
# ping -i 0.1 -s 5000 <target address>
```

This generates ten 5000 Bytes ping packets per second.

Monitor Station

The Monitor STA was combined with the Ping STA into one device. An Atheros AR5212 NIC with the madwifi driver in monitor mode was used to capture all packets during a DoS attack for later analysis. A wireless interface can be directly loaded into monitor mode:

```
# modprobe ath_pci autocreate=monitor
```

The following command in particular was utilised to capture traffic:

```
# tcpdump -i <interface> -w <file.cap> wlan src <target address>
```

This focuses solely on saving traffic generated by the Target STA.

Attacker Station

OpenBSD 4.8 with a Ralink AWUS036NH NIC and the OpenBSD run driver constituted the attacker STA. The interface was set into monitor mode with the following commands:

```
# ifconfig <interface> -nwid -bssid -wpa -wpapsk -nwkey
# ifconfig <interface> chan 1 media autoselect mediaopt monitor
```

The first command resets the interface and the second puts it into monitor mode on channel 1.

7.2 Access point attack tests

Association Request attacks were tested against APs in three different variations:

- invalid Supported Rates IE (without RSN IE and therefore also without 802.11w)
- invalid Supported Rates IE + RSN IE without 802.11w
- invalid Supported Rates IE + RSN IE with 802.11w

The reason the attack was tested with and without RSN IEs is, because some APs ignore Association Requests without RSN IEs in an RSN WLAN. Others react differently depending on the existence of an RSN IE. All three Association Request attacks have the following

basic frame structure, as described in Section 2.3.3 and as seen here in the following framecap tool dump:

```
Frame Control (FC):                00 00
Duration:                          3a 01
Address 1 (DA):                    <target AP MAC address>
Address 2 (SA):                    <target STA MAC address>
Address 3 (BSSID):                 <target AP MAC address>
Sequence Control (SC):             00 00
1 Capability:                      31 05
2 Listen interval:                 64 00
3 SSID:                            <ESSID>
4 Supported Rates:                 ee
```

The variants with pre-802.11w RSN IE and 802.11w RSN IE append an RSN IE with or without 802.11w capability at the end of the frame respectively. The interesting part is the Supported Rates IE set to 0xEE, a rate which is not included in any Basic Rate Set. Hereby the forged frame claims that the Target STA is not capable of transmitting in the Basic Rate Set of the AP.
All APs were set to an RSN CCMP configuration and additionally to an 802.11w configuration if capable.

The test procedure consisted of transmitting a single forged Association Request and then observing the impact of the attack.

7.3 Station attack tests

While the previous Association Request attack was directed towards APs, the Deauthentication, Quiet and Channel Switch attacks were tested against STAs. An Association Request attack directed to STAs does not exist, because only APs receive Association Requests and an STA therefore ignores these frames.
The testing of the Deauthentication attack consisted of two variants; one with the Target STA MAC address and another with the Broadcast Address as the Destination Address.

7.3.1 Test Procedure

The test procedure was composed of the following steps repeated in a loop:

- Five seconds of capturing traffic for comparison
- Attack
- Capturing of attack effect and recovery

The attack step iterated through variants of Deauthentication, Channel Switch and Quiet attacks.
Deauthentication attacks performed are:

- Ten Unicast Deauthentication frames per second directed to the target STA.
- Ten Broadcast Deauthentication frames per second directed from AP to STAs.

All of these Deauthentication attacks were launched for a duration of ten seconds.
In the next step, two Channel Switch attacks were launched:

- Channel Switch to a valid channel.
- Channel Switch to an invalid channel.

In both variants the Channel Switch Mode field was set to 0 and the Channel Switch Count field set to 1. These values were chosen based on Könings test results [21].

And lastly, two Quiet attacks were issued:

- Quiet with duration field set to 1000.
- Quiet with duration field set to the maximum of 65535.

In both Quiet variants the Quiet Count field was set to 1, the Quiet Period field set to 0 and the Quiet Offset field also set to 0. These values were again chosen based on Könings test results [21].

This process was carried out twice for 802.11w non-capable devices: in an RSN secured WLAN and in an Open WLAN.
In the 802.11w setup it was carried out once with 802.11w MFP enabled.

8 Evaluation

In this section the results of the tests described in Section 7 and observations made during this thesis will be described and evaluated. Before the results are discussed an example of how DoS attacks could be used as part of a more complex attack is given.

8.1 IE ordering

The IEEE 802.11 standard clearly specifies the order in which IEs may be set in frames. During the implementation of this thesis's beaconattack tool it was found that many APs do not set the correct order of IEs. This has no negative impact whatsoever, but violates the compliance with the IEEE 802.11 standard advertised by the vendors.

8.2 Accesspoint attacks

8.2.1 Pre-802.11w

Airport Express

The three Association Request attacks all trigger the same reaction at the Airport Express AP. After launching the attack the connection between target STA and Airport Express was interrupted for approximately six seconds.

OpenWrt

The configuration of the OpenWrt is described in Section 7.1.2.
The Association Request without any RSN IE attack had no impact. However, when a

pre-RSN IE or an 802.11w RSN IE was added the attack triggered a reboot of the AP. This attack with a single frame brought down the whole WLAN and also affected STAs connected by cable. These STAs attached by cable were disconnected for 25 to 30 seconds and wireless STAs were disconnected for 40 to 45 seconds.
The reboot was only triggered if the source address was associated with the AP. If a random address is used, the AP answered with a Deauthentication frame destined to the random address. By setting the source address to the broadcast address, this can also be used to generate broadcast Deauthentication frames from the AP itself.

Vodafone DSL-EasyBox 602

The Association Request frame without any RSN IE triggered a state change to the unauthenticated State 1 at the AP. However, the AP did not send a Deauthentication frame in order to notify the Target STA that the state machine had changed. Thus the Target STAs state machine remained in State 3. The AP silently discarded all incoming Data frames by the STA. This is particularly dangerous because the Target STA thought it was still connected and its User Interface therefore claimed to be connected. The only possible recovery is by reconnecting manually.

Adding a pre-802.11w RSN IE triggered the AP to send a Deauthentication frame. A madwifi based Target STA as described in Section 7.1.3 showed the same effects as without any RSN IE. However, a Mac2.1 OS X 10.6.7 reconnected right away. This is due to the Deauthentication frame sent by the AP which triggered a reconnect to the AP.

In contrast, by adding an 802.11w RSN IE the madwifi based Target STA reconnected by itself after the connection was interrupted for a while. The Mac2.1 STA completely disconnected. For recovery a reconnection attempt had to be initiated twice and the password had to be retyped.

Netgear DGND330B

All three variants of the Association Request attack caused the Netgear AP to react in the same manner by leading to one of three possible outcomes in a seemingly random order.

In the first outcome the Netgear AP reboots and thereby takes down the whole network, both wired and wireless. On average the attack resulted in approximately 24 seconds of cable, 48 seconds of WLAN and over 2 minutes of internet connectivity downtime.

The second outcome is similar to the first, but far more severe. In these cases solely the cable LAN was brought up. However, it was not possible to reconnect to the WLAN at all and the internet connectivity was never reset until the test was eventually aborted.

No AP reboot at all was triggered in the third and last outcome. The Netgear AP froze and did not respond, thus bringing down the whole wired and wireless network. For recovery the Netgear device needed to be rebooted manually with the hardware switch.

8.2.2 802.11w

OpenWrt

In this case the AP is an OpenWrt AP as described in Section 7.1.2.
The observations show the same behaviour as in the pre-802.11w mode, that was described in Section 8.2.1, with the exception that an Association Request with a pre-802.11w RSN IE was also discarded.
This behaviour is not compliant to the 802.11w specification and is due to bugs in the OpenWrt implementation.

8.3 Station attacks

All tested STAs were divided into two categories: laptops and mobile devices. The following list comprises the tested laptops:

- Broadcom BCM4322 with Windows 7
- Atheros 5008X with Windows 7
- Broadcom BCM4322 with Mac5.1 OS X 10.6.7
- Atheros AR5416 with Mac3.1 OS X 10.6.7
- Broadcom BCM4322 with Linux Ubuntu 10.04
- Intel iwl 5100 with OpenBSD 4.8

Additionally, the following mobile devices were tested:

- HTC Desire with Android 2.3.4
- Nexus S with Android 2.3.4
- iPhone 3gs with iOS 4.3.3
- iPod Touch 2 with iOS 4.3.3
- iPad with iOS 4.3.3

In the following section the evaluation appraises both the laptop and mobile device results for each tested attack.

8.3.1 Pre-802.11w

Deauthentication attack

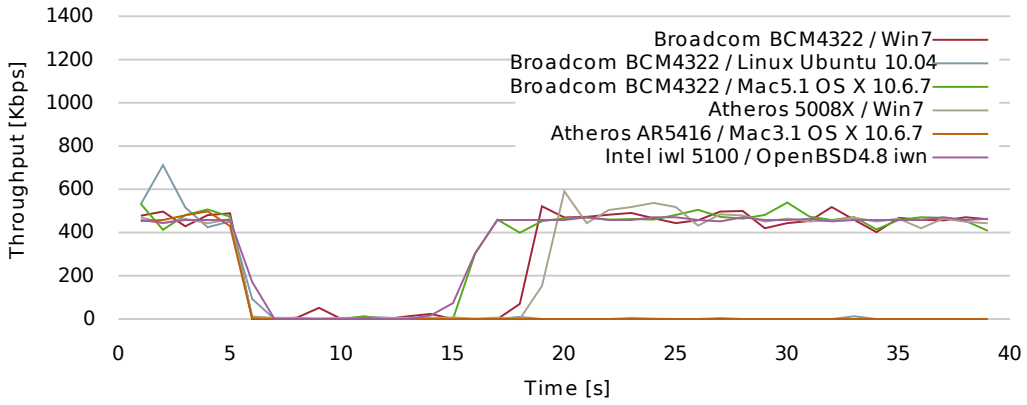

Figure 8.1: Unicast Deauthentication attack impact on laptops

Figures 8.1 and 8.2 show the vulnerability of STAs against unicast Deauthentication attacks. A DoS effect is achieved at every STA. This is no surprise, the STAs have no other choice but to deauthenticate, because there is no possibility in differentiating between legitimate and spoofed Deauthentication frames.

As depicted in Figure 8.1, all STAs except the Ubuntu 10.04 STA with a Broadcom NIC and a Mac third generation Intel with an Atheros NIC recovered quickly from the attack. In the

case of the Ubuntu STA, the NetworkManager[1] tool needed to be restarted to reconnect to the network.
The above-mentioned Mac STA was very persistent in remaining in a disconnected status. The WLAN module needed to be turned off and on twice and the password had to be retyped.

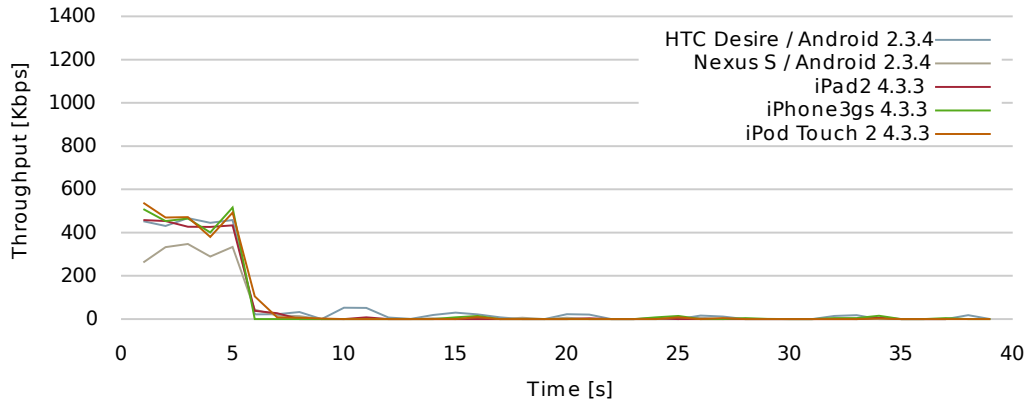

Figure 8.2: Unicast Deauthentication attack impact on mobile devices

The mobile devices yielded more quickly. This is likely due to the limited processing capabilities. In all cases the devices did not reconnect automatically. In most cases it sufficed to reconnect to the WLAN. However to reconnect the HTC Desire device, the wireless module had to be restarted.

Almost all tested devices experienced a DoS condition as an effect of the broadcast Deauthentication attack, as depicted in Figure 8.3, with the exception of the Windows 7 STA with an Atheros NIC. This STA ignored the broadcast Deauthentication frame.
Once again a restart of NetworkManager was needed to reconnect the Ubuntu 10.04 STA. The other STAs performed an automatic reconnect more quickly than after the unicast Deauthentication attack.

Figure 8.4 shows the impact of the broadcast Deauthentication attack on mobile devices. Solely the Nexus S reconnected automatically. The iOS devices had to be reconnected manually to the WLAN. Whereas a restart of the wireless module was once more necessary to reconnect the HTC Desire.

[1] http://projects.gnome.org/NetworkManager/

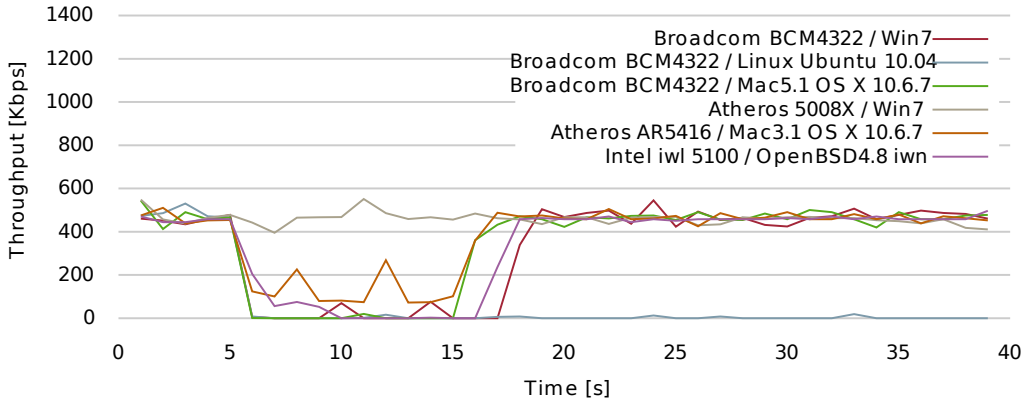

Figure 8.3: Broadcast Deauthentication attack impact on laptops

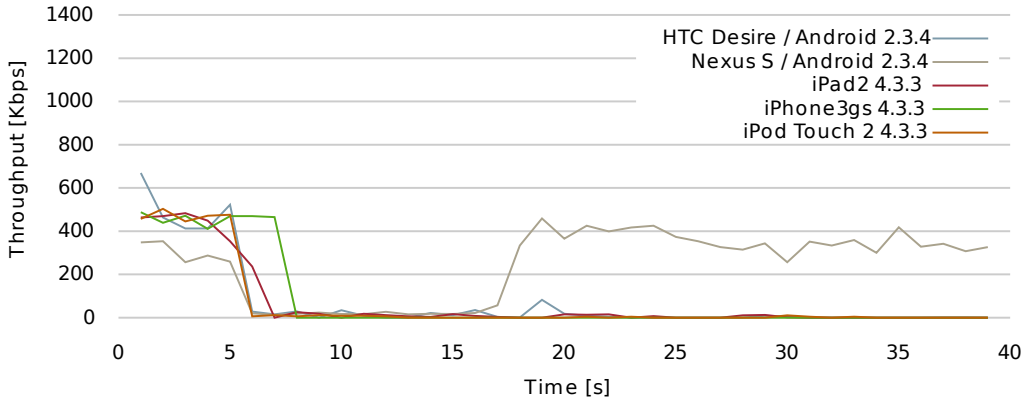

Figure 8.4: Broadcast Deauthentication attack impact on mobile devices

Channel Switch attack

The Channel Switch attack to a valid channel on laptops is depicted in Figure 8.5. In contrast to the Deauthentication attack where the STAs behaved similarly, the Channel Switch attack provokes different kinds of reactions.

As with the broadcast Deauthentication attack, the Atheros Windows 7 STA is resilient to the Channel Switch attack in the 2.4 GHz frequency spectrum.

Both Mac STAs honored the request but recovered with similar speed.

The Broadcom Ubuntu STA lingered on the false channel for about 24 seconds and then switched back automatically. However, it did not fully recover. It continually switched back

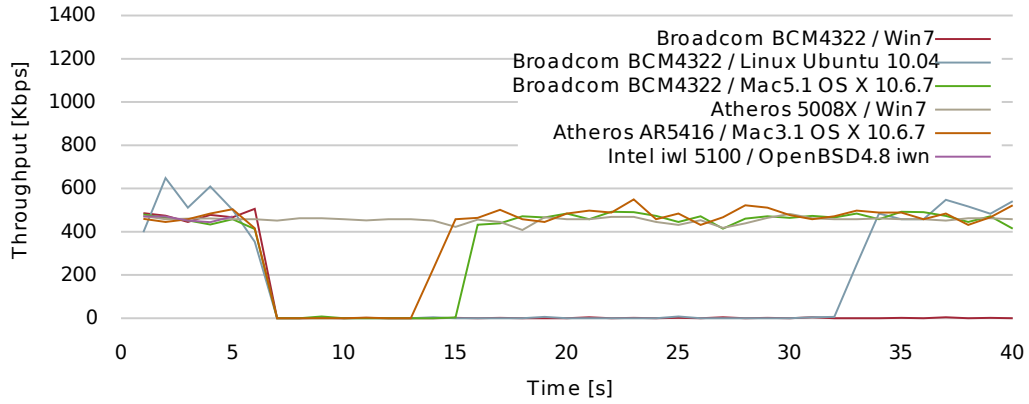

Figure 8.5: Channel Switch attack to a valid channel impact on laptops

and forth between the two channels, resulting in 30 to 40 times less throughput. A restart of the NetworkManager did not change this behaviour.
The OpenBSD STA completely switched over to the spoofed channel and did not switch back. A reconnect had to be done manually.

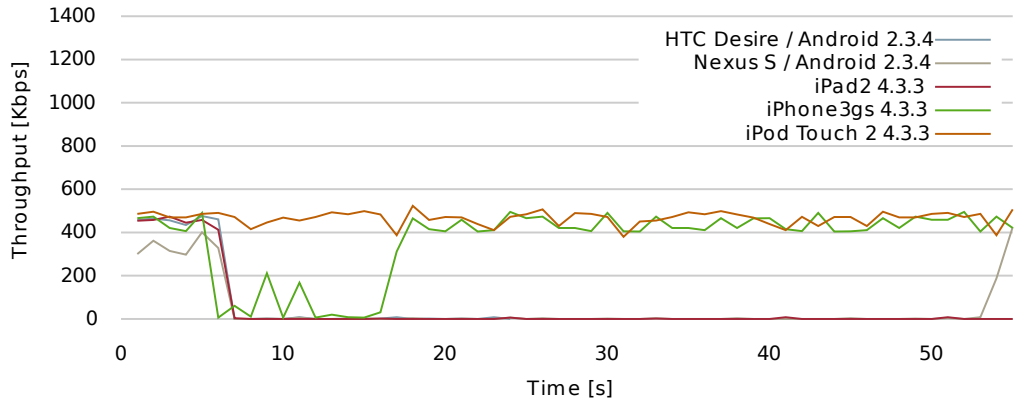

Figure 8.6: Channel Switch attack to a valid channel impact on mobile devices

Figure 8.6 depicts the effects of the Channel Switch attack to a valid channel on mobile devices. As with the Atheros Windows 7 STA, the Channel Switch attack has no effect on the iPod Touch 2.
The iPhone 3gs also recovered quickly, whereas the Nexus S lost connectivity for about 53 seconds before it switched back automatically. During this time the device claimed to the

user that it was connected.
On the other hand, the iPad2 and HTC Desire needed to be set back manually.

When changing the Channel Switch attack to an invalid channel only the OpenBSD STA honoured the request and had to be brought back manually. All the other STAs ignored the request.

Quiet attacks

None of the tested STAs showed an effect to the Quiet attack. It must be noted that all tests were conducted in the 2.4 GHz frequency spectrum. DFS and TPC are, however, only obligatory in the 5 GHz frequency spectrum.

The following Table 8.7 gives an overview over the vulnerabilities to the tested attacks.

	Unicast Deauth.	Broadcast Deauth.	Channel Switch	Quiet
Broadcom BCM4322 / Win7	●	●	●	
Broadcom BCM4322 / Linux Ubuntu 10.04	●	●	●	
Broadcom BCM4322 / Mac5.1 OS X 10.6.7	●	●	●	
Atheros 5008X / Win7	●			
Atheros AR5416 / Mac3.1 OS X 10.6.7	●	●	●	
Intel iwl 5100 / OpenBSD 4.8	●	●	●	
HTC Desire / Android 2.3.4	●	●	●	
Nexus S / Android 2.3.4	●	●	●	
iPad 2 4.3.3	●	●	●	
iPhone 3gs 4.3.3	●	●	●	
iPod Touch 2 4.3.3	●	●		

Figure 8.7: Summary of the test results

8.3.2 802.11w

All STAs were tested if they are able to connect to a WLAN requiring 802.11w, in order to check if a vendor might have implemented the functionality without advertising it, the result being that none of the STAs were able to connect.

The following results are based on the 802.11w implementations and setup as described in Section 7.

Deauthentication attack

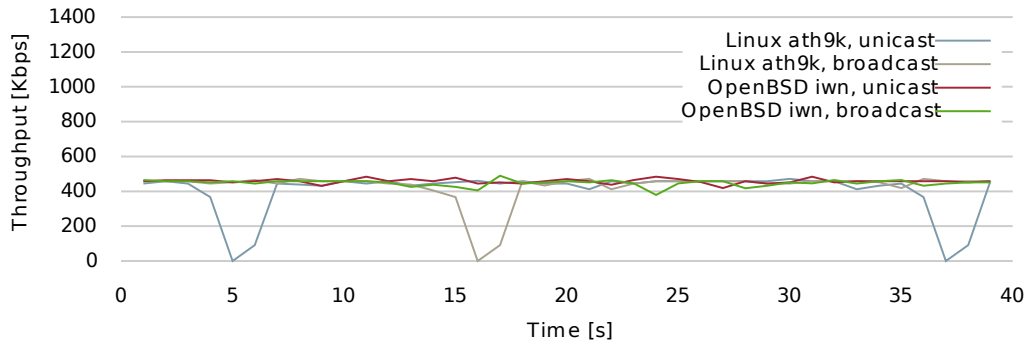

Figure 8.8: Deauthentication attack impact on 802.11w

As depicted in Figure 8.8, 802.11w STAs are resilient against Deauthentication attacks. Both STAs discard the attack frames, because the frames are not correct Robust Management Frames.
The sudden drops by the Linux ath9k STA are not triggered by the attack. They are possibly the effect of the STA scanning for networks.

However, 802.11w STAs are just as vulnerable to Channel Switch attacks as pre-802.11w STAs, as can be seen in Figure 8.9. Both STAs needed to be set back manually.

As in the pre-802.11w setup, the OpenBSD STA also switched to the invalid channel and needed to be set back manually.

This shows that, if an STA is vulnerable to the Channel Switch attack without 802.11w protection, the same still applies to 802.11w protection.

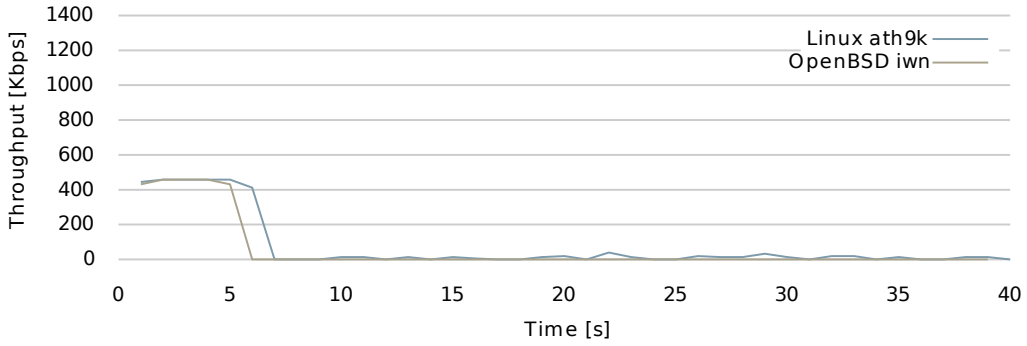

Figure 8.9: Channel Switch attack impact on 802.11w

Note that 802.11w protects Channel Switch Announcements in Action frames. However, all of the STAs tested ignored these frames.

The following Table 8.10 gives an overview over the vulnerabilities to the tested attacks.

	Unicast Deauth.	Broadcast Deauth.	Channel Switch	Quiet
Linux ath9k			●	
OpenBSD iwn			●	

Figure 8.10: Summary of the test results

8.3.3 Attack utilisation example

An STA usually prefers and chooses APs with the highest signal quality. This can be used to conduct man-in-the-middle attacks. For example, an attacker may want to attack an STA when the target is already connected to a WLAN. The attacker can then set up an AP with the same settings directed to the target so that the signal quality is higher than the AP it is connected to. By launching a DoS attack against the WLAN, the target STA disconnects from the real AP and reconnects to the rogue AP which the attacker has set up. This can be

done without the target user noticing anything. The STA merely notices a small glitch but can reconnect right away, which could happen in normal WLAN utilisation and is nothing unusual.
This can also be done in a larger scale. By launching the DoS attack against the whole network - for example a Deauthentication attack with the Destination Address set to Broadcast Address, or a Channel Switch attack - an attacker could take over a whole WLAN.

The attack was tested using an OpenBSD 4.8 STA as an AP and attacker. Target STAs were comprised of:

- iPad 1g with iOS 4.3.2
- iPod touch 1g with iOS 2.2.1
- Windows 7

After launching a broadcast Deauthentication attack, all STAs reconnected to the AP, set up by the attacker without the user noticing.

Note that the attacker has to set up an AP with the same configuration, meaning that in an RSN with *preshared key* (PSK) authentication the PSK must be known by the attacker.
Another possibility would be to set up a known network. Mobile devices in particular often have the default setting to connect to known networks.

8.4 Discussion

As expected, Deauthentication attacks are still very effective. The primary reason why these tests were conducted is to stress the magnitude of the attack after a century of awareness thereof, which has not improved at all.

An interesting observation is that many STAs implement the Channel Switch functionality, but do not implement the Quiet functionality in the 2.4 GHz frequency spectrum. Neither is obligatory in the 2.4 GHz frequency spectrum; yet Channel Switch is realised while Quiet is not. An assumption could be that the developers outweighed the possible positive and negative effects of these functionalities with the conclusion, that the potential for malicious use of the Quiet functionality is far too great and that the functionality is not used in widespread deployment, therefore ruling out its implementation.
Furthermore, all STAs do not react to the Channel Switch Announcement sent in Action

frames, just to those sent in Beacon frames. 802.11w protects Channel Switch Announcement in Action frames. By switching the implementation around in such a manner, that Channel Switch Announcements in Beacon frames are ignored and those in Action frames are reacted to, Channel Switch attacks could be eradicated within 802.11w. This only applies to unicast Action frames, with broadcast Action frames an insider Channel Switch attack would still be possible.

A frightening outcome is that two out of four access points crashed as a result of a single Association Request frame, affecting all devices connected to that particular AP. In many cases, especially in the private home sector, the AP is simultaneously a router and a modem. Therefore not only the WLAN is experiencing a DoS effect; the entire internet connection is down and unavailable. In modern times with intelligent houses and where everything is controlled and connected over the internet, this could have a greater impact than at first glance.

The attack utilisation example shows how DoS attacks can be used in combination with other attacks. Denial of Service is often not the ultimate objective of these attacks, but are an indispensable part of a more complex attack.
Another example would be to force a valid STA to reenter the network by deauthenticating the STA and thereby replay the handshakes taking place when entering the network. This would result in the generation of known encrypted byte sequences during the handshakes, which then can be used by an attacker to help crack the PSK.

9 Conclusion

Wireless LANs are subject to critical DoS attacks. Modern systems are just as vulnerable to these attacks as two years ago. Deauthentication and Channel Switch attacks can be launched effectively against current systems. Often one has to go to great lengths to recover from an attack. Moreover, many products are poorly designed and implemented. Some to the extent that a system crash is triggered upon receiving specific packets.
The outcomes in Section 8 reflect this. It is critical that WLANs become more robust against DoS attacks.
802.11w protects against a few of the MAC layer attacks, such as Deauthentication and Association Request attacks. Currently no vendor support exists and the Open Source support is still rare. Furthermore, 802.11w does not protect against Channel Switch and Quiet attacks.

The protection 802.11w provides is a beginning and a step in a promising direction. The vendors are now called for to start shipping their products with 802.11w support. A standard is not useful, if it is not implemented and used.

But even a full implementation of the 802.11w amendment will not yet be enough protection. As noted in the attacks overview on 802.11w in Section 5 and as seen in the evaluation in Section 8, an 802.11w amended WLAN is still open to DoS attacks. As soon as at least one attack exists which is able to disconnect a target STA from a WLAN or delete its SA, 802.11w protection can be removed and the target STA can be succesfully attacked with attacks which 802.11w would have protected against.

DoS attack protection still has a long way to go in 802.11. Difficult obstacles must be overcome to get a working design. It is arguably unlikely that 802.11 will ever provide the same level of protection for Management and Control frames as for Data frames. Flexibility, adaptability and interoperability would likely have to suffer as a side-effect of getting the same level of protection. Management and Control functionality would have to be limited mainly to intra WLAN functionalities. As soon as inter WLAN functionality is provided - which affects

the internal operation of a WLAN - the possibility of DoS attacks rises. In this scenario functionalities such as Quality of Service, optimal bandwidth usage and radar detection would be very difficult to realise. For Quality of Service and optimal bandwidth usage WLANs and STAs must ideally be evenly divided over the channels. The lack of inter WLAN communication complicates the matter; by introducing functionalities such as switching the channel, a potential for attacks similar to Channel Switch attacks could emerge.
All in all it is a difficult and complex task to design and implement DoS protection for protocols based on the wireless medium. 802.11w provides some basic protection, yet it is far from being satisfactory and will require much labor and attention in the future.

A Amendments

A.1 802.11k Amendment 1: Radio Ressource Measurement of Wireless LANs

- Radio Measurement to extend following properties:
  - capability
  - reliability
  - maintainability
- Mechanisms:
  - request and report:
    - Beacon
    - Frame
    - Channel Load
    - Noise Histogramm
    - STA Statistics
    - Location Configuration Information (LCI)
    - Neighbor Report
    - Link Measurement
    - Transmit Stream/Category Measurment
  - request only:
    - Measurement Pause

  - report only:
    - Measurement Pilot
- Public Action Frames:
  - Inter-BSS
  - AP to unassociated-STA
  - Measurement Pilot

A.2 802.11r Amendment 2: Fast Basic Service Set (BSS) Transition

- Faster Transition between BSSs
- Timeout Interval Information Element (TIE)
- Fast BSS Transition (FT) Protocols
  - FT Protocol / FT Resource Request Protocol
  - Over-the-Air / Over-the-DS

A.3 802.11y Amendment 3: 3650-3700 MHz Operation in USA

- Licenced band
- Cooperative
- Fixed and Enabled STAs
  - Fixed is allowed to transmit
  - Enabled STA coordinates unregistered STAs use of the licenced band
- Adds:
  - Dynamic STA Enablement (DSE)

    - Uses Public Action Frames
    - Enable STA
    - Deenable STA
    - Solves conflicts with other licencees
- Extended Channel Switch
- Regulatory Classes

B CD contents

- dominiklang_ba_11w.pdf
  This thesis as pdf
- images/
  All images in this thesis as pdf and inkscape svg
- src/
  - attack_tools-and-framecap/
    Source code of deauthattack, assocreqattack, beaconattack and framecap
  - wlstat-and-monitor/
    Source code of monitor and wlstat
- captures/
  The tcpdump pcap files from the attack tests

Bibliography

[1] M. S. Ahmad and S. Tadakmadla. Security evaluation of ieee 802.11w specification. In *WiSec'11*, 2011.

[2] S. Ahmad, J. V. R. Murthy, and A. Vartak. *Autoimmunity Disorder in Wireless LANs*. DEF CON 16, 2008.

[3] W. Arbaugh. *An Inductive Chosen Plaintext Attack against WEP/WEP2*. IEEE, 2001.

[4] W. Arbaugh, N. Shankar, Y. Wan, and K. Zhang. Your 802.11 wireless network has no clothes. In *Wireless Communications*. IEEE 9, 2002.

[5] J. Bellardo and S. Savage. 802.11 denail-of-service attacks: Real vulnerabilities and practical solutions. In *12th USENIX Security Symposium*, 2003. http://www.usenix.org/events/sec03/tech/full_papers/bellardo/bellardo_html/index.html.

[6] N. Borisov, I. Goldberg, and D. Wagner. Intercepting mobile communications: the insecurity of 802.11. In *Proceedings of the 7th annual international conference on Mobile computing and networking*. ACM, 2001.

[7] N. Cam-Winget, F. Housley, D. Wagner, and J. Walker. Security flaws in 802.11 data link protocols. In *Communications of the ACM*. ACM, 2003.

[8] Cisco. *Infrastructure Management Frame Protection (MFP) with WLC and LAP Configuration Example*, 2008. http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008080dc8c.shtml.

[9] ECC. *ECC Decision of 09 July 2004 on the harmonised use of the 5 GHz frequency bands for the implementation of Wireless Access Systems including Radio Local Area Networks (WAS/RLANs)*, 2004.

[10] ERC. *ERC Decision of 29 November 1999 on the harmonised frequency bands to be designated for the introduction of High Performance Radio Local Area Networks (HIPERLANs)*, 1999.

[11] ETSI. *EN 301 893: Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering the essential requirements of article 3.2 of the RT&TTE Directive*, 2008.

[12] S. R. Fluhrer, I. Mantin, and A. Shamir. Weaknesses in the key scheduling algorithm of rc4. In *Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography*. Springer-Verlag, 2001.

[13] M. S. Gast. *802.11 Wireless Networks*. O'Reilly, 2005.

[14] IEEE. *802.11a-1999 (R 2003): High-speed Physical Layer in the 5 GHz Band*, 1999. http://standards.ieee.org/getieee802/download/802.11a-1999.pdf.

[15] IEEE. *802.11b-1999 (R 2003): Higher-Speed Physical Layer Extension in the 2.4 GHz Band*, 1999. http://standards.ieee.org/getieee802/download/802.11b-1999.pdf.

[16] IEEE. *802.11h-2003, Amendment 5: Spectrum and Transmit Power Mangement Extensions in the 5 GHz band in Europe*, 2003. http://standards.ieee.org/getieee802/download/802.11h-2003.pdf.

[17] IEEE. *802.11-2007*, 2007. http://standards.ieee.org/getieee802/download/802.11-2007.pdf.

[18] IEEE. *802.11i-2004, Amendment 6: Medium Access Control (MAC) Security Enhancements*, 2009. http://standards.ieee.org/getieee802/download/802.11i-2004.pdf.

[19] IEEE. *802.11w-2009, Amendment 4: Protected Management Frames*, 2009. http://standards.ieee.org/getieee802/download/802.11w-2009.pdf.

[20] IETF. *The AES-CMAC Algorithm*, 2006. https://tools.ietf.org/html/rfc4493.

[21] B. Koenings. Sicherheit der phy- und mac-schicht in 802.11-netzwerken. Master's thesis, University of Ulm, January 2009.

[22] A. Subblefield, J. Ioannidis, and A. D. Rubin. *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*, 2002.

[23] J. R. Walker. *IEEE 802.11-00/362 - Wireless LANs Unsafe at any key size; An analysis of the WEP encapsulation*. IEEE, 2000.

Name: Dominik Lang Matriculation number:

Declaration of Academic Honesty

I herewith declare that I have prepared this thesis on my own, using only the materials mentioned. Ideas taken, directly or indirectly are identified as such.

Ulm, ...

Dominik Lang