# Channel Switch and Quiet Attack: New DoS Attacks Exploiting the 802.11 Standard

Bastian Könings, Florian Schaub, Frank Kargl, and Stefan Dietzel
Institute of Media Informatics
Ulm University, Germany
{ bastian.koenings | florian.schaub | frank.kargl | stefan.dietzel }@uni-ulm.de

***Abstract*—Network communication using unprotected air as a medium leads to unique challenges ensuring confidentiality, integrity and availability. While newer amendments of IEEE 802.11 provide acceptable confidentiality and integrity, availability is still questionable despite broad usage of Wi-Fi technologies for tasks where availability is critical. We will present new security weaknesses that we have identified in the 802.11 standard and especially the 802.11h amendment. Our results are underlined by an extensive analysis of attacks addressing the quiet information element and channel switch announcement in management frames. For some stations a complete DoS effect can be achieved with a single packet for more than one minute. This shows that the newly identified attacks are more efficient than earlier approaches like a deauthentication attack. Tests were performed with a large variety of network interface cards, mobile devices, and operating systems.**

## I. Introduction

IEEE 802.11-based wireless networks are being deployed in large numbers in home, business, and public environments but also in critical environments like hospitals or production plants where reliance on their availability is crucial. For example, Cisco reports that a 802.11n network is being deployed in a German university clinic to monitor vital parameters of patients as they are moved between rooms [1]. The Regional Medical Center in El Centro,[1] CA, also intends to use Wi-Fi for bedside drug administration [2]. Many more applications of wireless networks in sensitive domains are envisioned or already implemented.

The initial approach to WLAN security was called *Wired Equivalent Privacy (WEP)* and proved to be a security disaster [3]–[6]. Later, IEEE 802.11i [7] and the related WPA and WPA2 provided more substantial authentication, integrity, and confidentiality protection. However, recently the security of at least WPA (version 1) has been challenged [8].

Despite such security mechanisms having been introduced to the standard to ensure confidentiality, integrity, and authenticity, the availability of wireless LANs remains a particular challenge. With availability we mean the continued provision of service in the face of intentional denial-of-service (DoS) attacks. Availability is a concern not only because jamming the physical medium is an attack that can hardly be prevented at the protocol level, but mostly because the management protocols have been left out of scope to a large extent when the security solutions were designed.

[1] http://www.ecrmc.org/

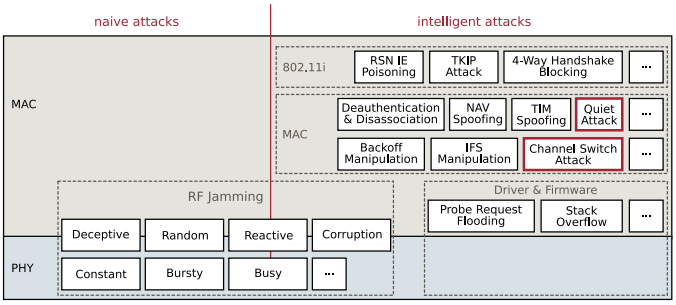


Fig. 1. Existing attacks on the availability of 802.11 WLANs.

Actually, despite use of modern encryption in 802.11i, most management messages are send in the clear, are not authenticated, and can easily be spoofed. In this work, we put the focus on the common standard amendments 802.11h and 802.11n that are less often studied by security researchers despite being in wide use. We have identified a total of four previously unknown attacks. Two of them, the *quiet attack* and the *channel switch attack* will be described and analyzed here.

In the remainder of this paper, we will first describe previously known attacks on 802.11 availability in Section II. Next we introduce four new attacks (Sec. III) before presenting a detailed study of the impact of the *channel switch attack* and the *quiet attack* using a total of 15 different WLAN devices plus different drivers in Section IV. We will show that the new attacks can be launched with far less overhead compared to previous attacks.

## II. Classification of Previous Attacks

A couple of earlier publications have addressed attacks on the availability of 802.11 networks. Fig. 1 gives an overview of these existing attacks. One can distinguish attacks that target the PHY or the MAC layer. Attacking the PHY layer basically involves jamming of the radio band. On the MAC layer, more sophisticated attacks targeting the protocols are possible. We have grouped the attacks into four categories:

1) *RF Jamming Attacks.* The goal of RF jamming is to distort the radio signal of another sender by sending other signals or noise on the same radio channel, thereby preventing proper reception of the signal at the receiver(s).

IEEE 34th Conference on Local Computer Networks (LCN 2009), Zurich, 2009
Author version. Definitive version at http://dx.doi.org/10.1109/LCN.2009.5355149

2) *MAC Layer Attacks.* MAC layer attacks target various protocols in the IEEE 802.11 MAC layer that are responsible, e.g., for association of stations with an access point or for controlling power management. By sending forged protocol messages or by not adhering to certain rules, e.g., rules for fair medium access, an attacker is able to prevent others from effectively participating in the wireless network.
3) *802.11i Attacks.* Although 802.11i actually belongs to the MAC layer, we consider these attacks a category of its own, as they address the security mechanisms that were meant to protect the network. While some 802.11i attacks target authentication or confidentiality, some can also be used to carry out denial of service attacks, e.g., by preventing proper authentication of stations.
4) *Implementation-specific Attacks (Driver/Firmware).* While attacks of the previous categories exploit weaknesses in the standard itself, this category includes all attacks that exploit weaknesses in implementations, e.g., leading to overload situations in stations or APs. Other attacks could crash stations or APs by exploiting stack buffer overflow weaknesses in drivers, etc. While usually being applicable to only a small range of products, the effects can nevertheless be more devastating, as a WLAN driver might easily crash a whole operating system. Then, the effect of the denial of service attack is not limited to unavailability of the network but impacts the whole computer.

Next, we will describe some representatives of these categories, which are summarized by Table I.

### A. RF Jamming Attacks

Xu et al. [9] and Acharya et al. [10] define seven jamming models (see Tab. I). *Constant jamming* is the most common model describing the continuous transmission of a signal or noise to interfere with other ongoing transmissions. Constant jamming attacks have been tested in simulations [10] as well as in real-world testbeds [11]–[13].

Other techniques like *bursty* or *random jamming* transmit jamming signals less frequently to save energy and reduce the probability of detection. The most sophisticated RF jamming techniques are *reactive* and *corruption jamming* which only transmit whenever an ongoing transmission or a certain message is sensed. The former approach has been implemented in a real-world testbed and simulated by Bayraktaroglu et al. [14].

### B. MAC Layer Attacks

A couple of attacks belonging to this group have been identified by Bellardo and Savage [15]. The most common attack is the *deauthentication attack* as it is already implemented in several network hacking tools. This attack exploits the association process stations are required to perform to connect to an AP in an infrastructure BSS. After a connection is successfully established either the station or the AP can shut down the connection by sending a deauthentication message. As management messages are unprotected in the current 802.11 standard, an attacker could forge this message on behalf of the station or the AP. Ahmed et al. [16] presented an interesting version of this attack, where non conform messages, like a data packet with broadcast address as source address, cause the AP to send broadcast deauthentication messages. They called this kind of attack *autoimmune disorder*.

The *NAV reservation* attack [15], [17] exploits the 802.11 distributed coordination function (DCF). An attacker can reserve the network allocation vectors (NAV) of all stations in range by forging the time information in unprotected RTS or CTS control messages. For this attack the maximum DoS effect that can be achieved with a single message is limited to 32 767 µs. However real-world tests showed that many devices do not reserve the NAV in a standard conform manner [15], [17]. Other attacks targeting the DCF are based on exploiting capture effects [18] or forgery of protocol parameters like backoff duration [19] and interframe spaces [20]–[22].

The power saving techniques defined by the standard can also be exploited, e.g., by forging TIM or PS-Poll management messages [15]. This way an attacker could cause the AP to drop buffered messages for a station in sleep mode or cause a station to wake up at wrong points in time and thus miss the beacon of the AP.

Other novel attacks exploit the block acknowledgement mechanism of the 802.11n draft amendment by forging information in BlockAck(Req) messages [23], [24] and ADDBA requests [25]. These attacks can lead to a DoS effect of 10 seconds with a single message [23].

### C. 802.11i Attacks

Glass and Muthukkumarasamy [26] presented and analyzed the feasibility of a DoS attack against TKIP. To prevent key recovery attacks, TKIP implements so-called countermeasures which lead to an interruption of all TKIP based functions for one minute. To trigger these countermeasures an attacker has to intercept and modify two packets within one minute.

He and Mitchell [27] identified further DoS attacks against 802.11i, exploiting the authentication process defined by this amendment. Those are based on forging EAP messages or RSN information elements in beacons or probe responses and continuous flooding of an association request or the first message of the four-way handshake, respectively. As the feasibility of flooding attacks mostly depends on specific implementations, these attacks could also be classified in the following category.

### D. Implementation-specific Attacks (Driver/Firmware)

Ferreri et al. [28] analyzed the impact of flooding attacks on several access points. They injected probe requests, authentication requests, and association requests with an injection rate of about 800 packets per second. The achieved DoS effect strongly depended on the used AP and injected request type. The most effective attack was flooding of association requests.

Other representatives of this category are attacks exploiting weaknesses in drivers or firmware to achieve a stack overflow. Butti and Tinnès [29] identified some weaknesses of that kind

TABLE I
OVERVIEW OF EXISTING ATTACKS

| Attack | BSS | IBSS |
|---|---|---|
| ***RF Jamming Attacks*** | | |
| Constant Jamming | S,I | I |
| Deceptive Jamming | S | T |
| Bursty Jamming | S | T |
| Busy Jamming | S | T |
| Random Jamming | S | T |
| Reactive Jamming | S,I | T |
| Corruption Jamming | S | T |
| ***MAC Layer Attacks*** | | |
| Deauthentication | I | - |
| Autoimmune Disorder | I | - |
| *Management Information Forgery* | | |
| DS Parameter Sets Forgery | T | T |
| Quiet Attack (802.11h) | I* | I* |
| Channel Switch Attack (802.11h) | I* | I* |
| *Attacks on Power Saving Mechanisms* | | |
| TIM/PS-Poll Forgery | T | - |
| Timing Information Forgery | T | T |
| ATIM Forgery | - | T* |
| *Attacks against DCF* | | |
| NAV Reservation | S,I | T |
| Capture-Effekts | T | S |
| Protocol Parameter Manipulation | I | T |
| *Attacks against Block Acknowledgement* | | |
| BlockAck(Req) Forgery (802.11n) | T | - |
| ADDBA Forgery (802.11n) | T | - |
| DELBA Forgery (802.11e/n) | T* | - |
| ***802.11i Attacks*** | | |
| TKIP-Countermeasures Attack | I | T |
| EAP Attacks | I | T |
| 4-Way-Handshake Attack | T | T |
| RSN IE Poisoning | T | T |
| ***Implementation-specific Attacks*** | | |
| Flooding (PRF, ARF, ASRF) | I | T |
| Stack Overflow | I | T |

Simulated attacks (S), implemented attacks (I), not yet tested but theoretically applicable attacks (T), or attacks not applicable (-) in 802.11 infrastructure BSS or IBSS networks. *Attacks marked with a * are newly presented in this paper.*

which could lead to a DoS effect and, even worse, to execute malicious code on the attacked station. The stack overflow was caused by maliciously formed information elements in beacons, probe responses, or association requests.

### E. Current State of the Art

As we can see, up to now attacks focused mostly on the core of the standard and on dedicated security mechanisms. Especially in the group of MAC attacks, researchers have failed to identify weaknesses in amendments like 802.11h despite its availability since 2003. Also not all weaknesses in the new 802.11n have been identified. So our first goal in this work is to identify additional weaknesses and new DoS attacks that stem from those amendments.

Our second observation is that many attacks are only described theoretically or have been tested only in simulation. In our experience, however, the real impact of an attack cannot be judged on this basis. This is due to the fact that many implementations behave not 100 percent standard compliant and that simulations often simplify real-world behavior of wireless systems, especially of many MAC mechanisms [30].

Many of the attacks in Table I have not been tested against a variety of real world equipment. The impact of those attacks can therefore not be determined reliably. So our second goal is to analyze the discovered attacks not only theoretically, but to provide a broad study that gives indications how many systems are vulnerable and how severe the denial of service effect will be or how effectively it can be launched.

The upcoming section describes newly identified attacks while Section IV analyzes two of the attacks in detail.

## III. NEW ATTACKS ON AVAILABILITY

In our research, we have identified four new attacks on availability in 802.11 wireless networks. All of them fall in the category of MAC layer attacks and directly exploit weaknesses in the 802.11 standard or its amendments. The *quiet attack* and the *channel switch attack* based on 802.11h [31] will be the focus of the remainder of this work. We also shortly present the *ATIM attack* and the *DELBA attack* which exploit power saving mechanisms in ad hoc mode (IBSS) and the block acknowledgement of 802.11e, respectively. Detailed discussion and evaluation of the latter two is left for future work due to lack of space.

The amendment 802.11h, released in 2003, extends the capabilities for exchanging management information between stations. 802.11h defines so called action frames, which belong to a certain action category, e.g., spectrum management. Each action category defines its own information elements (IE) tailored to certain management tasks. These IEs can be part of dedicated action frames or be included in other management frames, e.g., beacons.

The main purpose of 802.11h has been the introduction of frequency spectrum management mechanisms to enable the usage of the 5 GHz band by 802.11a and 802.11n in Europe. One of these mechanisms is dynamic frequency selection (DFS), which is mandatory in Europe for 802.11 devices operating at 5.25–5.35 GHz and 5.47–5.725 GHz [32]. With DFS, stations monitor the current channel for other signals, e.g., military radar, and switch to a different channel if the current is occupied. By forging the corresponding management information elements, denial of service effects can be achieved.

Management information can be easily forged because, unlike data messages, they are neither encrypted nor integrity protected by any part of the standard and require no authentication. The future amendment 802.11w [33] aims to change this for disassociation, deauthentication and action frames by including a Management MIC information element (MMIE) in those messages. So even when the amendment will be implemented in the future, at least three of the following attacks remain still feasible, due to the fact that the current draft version of 802.11w (D6.0) does not propose protection of beacons.

### A. Quiet Attack

Assessment of the current channel is an important part of DFS. To be able to accurately measure the current channel for

| Element ID | Length | Quiet Count | Quiet Period | Quiet Duration | Quiet Offset |
|---|---|---|---|---|---|
| *1 Byte* | *1 Byte* | *1 Byte* | *1 Byte* | *2 Bytes* | *2 Bytes* |

Fig. 2. Format of a quiet element.

| Element ID | Length | Switch Mode | New Channel Number | Switch Count |
|---|---|---|---|---|
| *1 Byte* | *1 Byte* | *1 Byte* | *1 Byte* | *1 Byte* |

Fig. 3. Format of a channel switch announcement element.

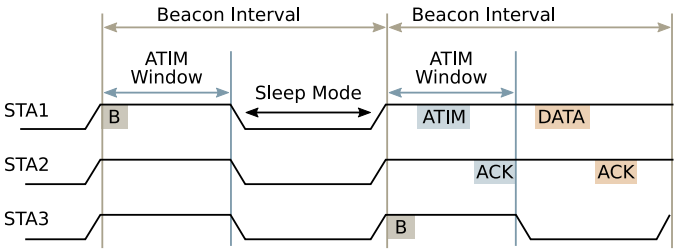


Fig. 4. Power saving mechanism in an IBSS.

other activities, an access point (AP) includes a *quiet element* in beacons or probe responses. The quiet element specifies a certain time interval for which receiving stations of the BSS have to be silent, i.e., send no messages, so that channel measurement can take place. For IBSS, the quiet element may be sent by any station.

The quiet element, depicted in Fig. 2, contains several fields. *Quiet count* specifies the remaining beacon intervals before the quiet interval starts. In case the quiet interval is to be repeated, the *quiet period* field specifies the number of beacon intervals to wait in between. *Quiet duration* specifies the length of the quiet interval in time units (TU), so that stations can reserve their NAV accordingly. The *quiet offset* field can be used to specify an additional offset after the start time, which has to be shorter than one beacon interval.

An adversary could forge the quiet element with the result that stations that adhere to 802.11h and support DFS will remain silent for the specified quiet period. By specifying the maximum value of 65 535 TUs as *quiet duration*, stations can be effectively silenced for up to 67 seconds with a single message. By specifying a periodic repeat, even a continuous DoS effect might be achievable.

### B. Channel Switch Attack

If channel measurement reveals that the channel is already in use, the channel has to be switched. An access point advises all stations of the BSS to change to a different channel with a *channel switch announcement element* included in a beacon, a probe response, or an action frame. In an IBSS, this announcement may be sent by any station.

The format of the channel switch announcement element is depicted in Fig. 3. The *switch mode* regulates if a station can continue sending until channels are switched (value 0) or if it has to cease sending immediately (value 1). As the name suggests, *new channel number* specifies the number of the new channel stations should switch to. *Switch count* gives the remaining beacon intervals before the channel switch.

An adversary could utilize the channel switch announcement element to encourage other stations in the BSS or IBSS to change to a different channel while the AP will remain on the original channel. *New channel number* can even be set to an invalid channel. To further enhance the efficiency of the denial of service attack, *switch mode* can be set to 1 and the *switch count* can be set to the maximum value of 255. This way, stations can be forced to be silent for 255 beacon intervals before switching to the specified channel. Once stations have switched to an invalid channel, they have to wait an additional timeout before trying to establish a connection on a different channel again. Some firmware and driver developers have already recognized the issue and introduced countermeasures, e.g., the MadWifi[2] driver limits the *switch count* to 1.

### C. ATIM Attack

This attack exploits power saving mechanisms in 802.11 IBSS, i.e., networks operating in ad hoc mode. To save power, stations can switch to a sleep mode and power down their radio unit. In an infrastructure BSS, a station would inform the AP before it goes to sleep, and the AP would store incoming packets for that station. The station wakes up in regular intervals and waits for a beacon from the AP containing a traffic indication map (TIM). If the TIM indicates waiting messages for the station it stays awake and requests them from the AP.

In an IBSS this process has to be distributed. The initial station of an IBSS specifies an announcement traffic indication message (ATIM) window, in which all stations have to be awake. In the ATIM window, any station with cached messages for previously sleeping stations can send an ATIM message. If a station is listed in the ATIM, it stays awake for the next ATIM window to receive the data. Fig. 4 provides an example. All stations wake up for the ATIM window, STA1 sends the beacon ($B$). No ATIMs are exchanged so that all stations go back to sleep after the ATIM window is over. In the second ATIM window, STA1 sends an ATIM indicating STA2. STA1 and STA2 stay awake to transmit the data.

By forging the ATIM message, an adversary can force all or specific stations to stay awake. This is a critical issue for devices with restricted energy resources, e.g., mobile or ubiquitous computing devices. If forged ATIM messages are sent repeatedly an energy depletion attack could be mounted against battery-powered devices.

### D. DELBA Attack

The DELBA attack exploits the block acknowledgement, which has been introduced in amendment 802.11e [34] and is also used in the upcoming 802.11n [35]. This mechanism enables a receiver to acknowledge the reception of several messages with a single ACK. The process consists of three phases: setup, data and block ACK, and tear down, as depicted in Fig. 5.

[2]http://madwifi-project.org/ticket/963

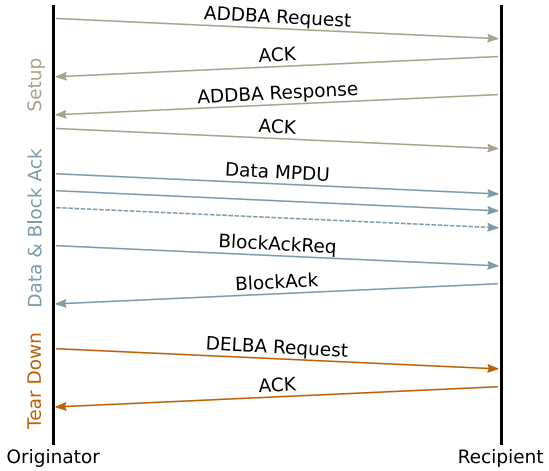


Fig. 5. Phases of the block acknowledgement.

The sender first sends an *add block acknowledgment (ADDBA) request* which specifies buffer size and starting sequence number of the data stream. The receiver sends an *ADDBA response* and may adapt the buffer size to its capabilities. Subsequently, the sender can send several data packets in sequence, up to the previously agreed buffer size. After transmission of the data stream the sender explicitly requests the receiver's ACK (*BlockAckReq*). The receiver sends a *BlockAck* message containing a bitmap which indicates the received packets. Selective retransmission of lost packets is possible. In the tear down phase, the sender sends a *delete block acknowledgement (DELBA)* message which ends the communication and free the buffers of sender and receiver.

802.11n uses this mechanism to specify a transmission window of upcoming sequence numbers in the ADDBA request. The receiver then only accepts packets with sequence numbers inside the transmission window, while others are rejected. While several weaknesses of this mechanism have already been identified (see Sec. II-B), we propose forgery of the DELBA message. The DELBA message terminates block acknowledgement communication and frees buffers on sender and receiver side. Because a DELBA message is an unprotected action frame it can be easily forged by an adversary. By impersonating the sender in an already established block acknowledgement process, the block acknowledgment process between two stations can be terminated prematurely this way. This frees allocated resources and will also drop all packets received so far.

## IV. Analysis of Quiet and Channel Switch Attacks

To allow an evaluation of efficiency of the quiet and channel switch attacks, we measured the number of injected packets required to achieve a one minute DoS effect in a real-world testbed setup. Both attacks were tested with 15 devices with varying drivers and operating systems (Tab. II) in infrastructure BSS as well as in IBSS topologies. To compare our results with a well known attack we also tested a version

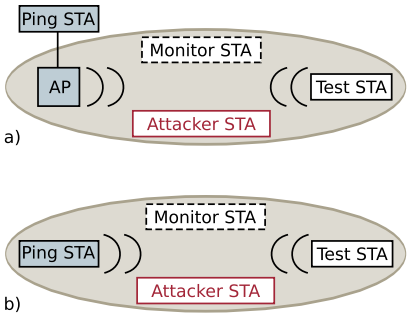


Fig. 6. Attack testbed in a) 802.11 infrastructure BSS topology and b) 802.11 IBSS topology.

of the deauthentication attack which we optimized for packet efficiency. The attack was implemented in such a way, that one deauthentication messages is sent whenever a data packet of the victim station was received. This is already more efficient than a naïve deauthentication attack.

The following subsections describe the testbed setup and the results in detail.

### A. Testbed Setup

All attacks were implemented with the Scapy tool[3] and were executed on a Thinkpad T43 with an Atheros AR5212 NIC in combination with the Linux MadWifi driver, enabling tests of 802.11a/b/g devices. The attacker captures beacon frames from the AP (or another station in IBSS), injects the forged information elements, and retransmits the beacon frames forging the MAC address of the AP (or station). In addition to the attacker station, the testbed (Fig. 6) consisted of a ping station, a monitor station, and the test station. For tests in infrastructure BSS topology, the setup also included an access point. A Cisco Aironet 1130AG and a D-Link DWL-G730 access point were used. The ping station used ICMP pings with a payload of 5,000 bytes and a ping interval of 0.1 seconds to generate constant data traffic to the wireless test station. The NIC of the monitor station (Atheros AR5212 with Linux Madwifi driver) was configured in monitor mode to measure the effect of an attack on the ICMP ping replies. Each attack was launched 10 seconds after the monitor station started capturing data.

The attacks were executed with varying parameters, to assess the effectiveness of different parameter combinations. Quiet attacks were executed with varying quiet durations in the quiet element. Channel switch attacks were executed with varying switch mode, switch count and new channel number in the channel switch announcement. The used frequency was varied between 2.4 GHz and 5 GHz channels.

### B. Results

Our tests showed that in infrastructure BSS mode with Cisco AP all devices were susceptible to the deauthentication attack, five devices to the quiet attack, and six devices to the channel switch attack. The last two numbers are due to the fact that

[3]http://secdev.org/projects/scapy/

TABLE II
OVERVIEW OF TESTED DEVICES, SUPPORTED AMENDMENTS AND USED DRIVERS.

| Device | 802.11 a | b | g | n | Driver Linux | Windows | Mac OS | Symbian |
|---|---|---|---|---|---|---|---|---|
| Intel 2100B | - | ● | - | - | ipw2100 v0.56 | - | - | - |
| Intel 2200BG | - | ● | ● | - | ipw2200 v1.2.2 | XP v9.0.4.39 | - | - |
| Intel 3945ABG | ● | ● | ● | - | iwl3945 v1.2.0 | Vista v10.6.0.46 | - | - |
| Intel 4965AGN | ● | ● | ● | ● | iwlagn v1.3.27 | Vista v11.1.0.86 | - | - |
| Intel 5100AGN | ● | ● | ● | ● | iwlagn v1.3.27 | XP v12.0.0.82 | - | - |
| Ubiquiti SRC | ● | ● | ● | - | madwifi v0.9.4.5 | XP v7.7.0.0 | - | - |
| Airport Extreme | ● | ● | ● | ● | - | - | v5.10.38.9 | - |
| Intersil ISL3890 | - | ● | ● | - | Prism54 v1.2 | - | - | - |
| Lucent Wavelan | - | ● | - | - | Host AP v0.5.7 | XP v7.43.0.9 | - | - |
| iPhone 3G | - | ● | ● | - | - | - | *unknown* | - |
| iPod Touch 2G | - | ● | ● | - | - | - | *unknown* | - |
| Nokia 770 | - | ● | ● | - | cx3110x v0.8.1 | - | - | - |
| Nokia N810 | - | ● | ● | - | cx3110x v2.0.15 | - | - | - |
| Nokia E51 | - | ● | ● | - | - | - | - | *unknown* |
| Nokia E71 | - | ● | ● | - | - | - | - | *unknown* |

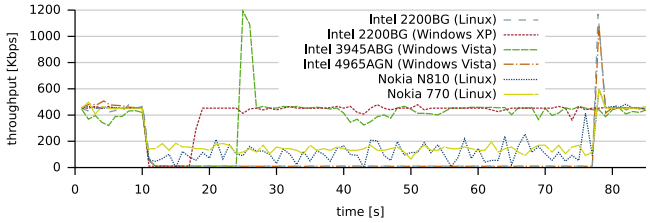


Fig. 7. Measured throughput during quiet attacks with a maximum quiet duration of 65 535 TUs against four attackable devices.

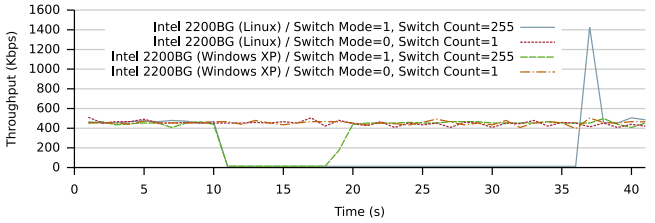


Fig. 8. Measured throughput during channel switch attacks against an Intel 2200 NIC.

some older devices only operate at 2.4 GHz and therefore ignore the quiet elements and channel switch announcements as they need not implement IEEE 802.11h. As presented in Table III, both the quiet attack and channel switch attack were able to achieve a one minute DoS effect with only one injected packet for some devices. The medians of 1 and 3 packets (with respect to the other devices/drivers tested) show the high efficiency of both attacks in comparison to the deauthentication attack with a median of 106 packets. The large difference between the minimum of 11 packets and maximum of 668 packets of the deauthentication attack is caused by the fact that on the one hand some devices failed to reconnect after getting deauthenticated repeatedly and on the other hand some devices continuously reconnected very quickly.

TABLE III
NUMBER OF FORGED MANAGEMENT PACKETS LEADING TO A DOS EFFECT OF AT LEAST ONE MINUTE.

| Attack | Minimum | Maximum | Median |
|---|---|---|---|
| Deauthentication | 11 | 668 | 106 |
| Quiet | 1 | 8 | 1 |
| Channel Switch | 1 | 12 | 3 |

*1) Quiet Attack:* The quiet attack achieved a maximum DoS effect of 67 seconds with a single message for the Intel 2200BG under Linux (ipw2200) and the Intel 4965AGN under Vista (see Fig. 7). These two examples show that current devices (802.11n) as well as older devices (802.11b) are

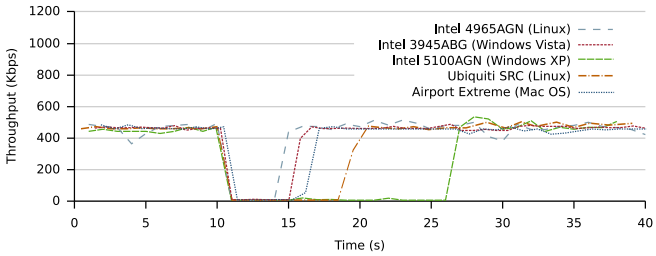


Fig. 9. Measured throughput during channel switch attacks with switch mode 0 and switch count 1 against 5 attackable devices.

susceptible to the quiet attack. The Windows XP driver for the 2200BG as well as the Windows Vista driver for the Intel 3945ABG limited the quiet duration to 8 and 15 seconds, respectively.

A DoS effect of 67 seconds was also observed for the two tested Nokia internet tablets (770, N810), but with significant remaining throughput. Analysis of the captured data showed that this effect was caused by the first fragment of each ICMP ping response which was still sent by the Nokia devices. Even though the first fragment is sent, communication is not possible due to lack of the following fragments. This leads to the assumption that this behavior results from faulty implementation of device driver or firmware.

*2) Channel Switch Attack:* For the channel switch attack, the duration of DoS effects achieved with a single packet varied between 5 to 26 seconds most of the times, depending

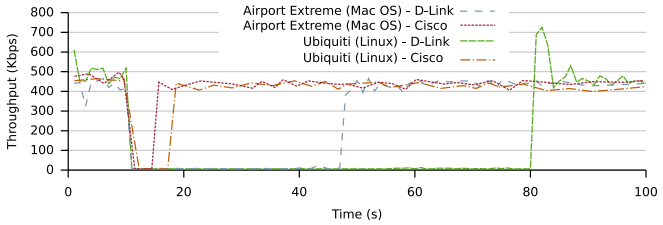


Fig. 10. Measured throughput during channel switch attacks with switch mode 0 and switch count 1 in dependence on the used AP.

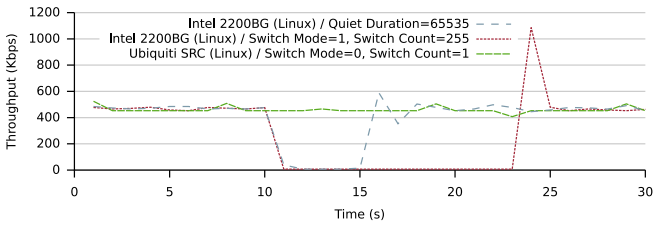


Fig. 11. Measured throughput during attacks in IBSS mode.

on used device and driver. After switching to the new channel, most attackable devices switched back to the old one and reconnected to the AP after a delay of 5 to 15 seconds. However, in some cases the connection of the test station was completely interrupted resulting in a continuous DoS effect. This happened with the Intel 3945ABG under Vista when the new channel number was invalid, and under Linux with this NIC as well as the Intel 4965AGN and 5100AGN when the switch count was greater than 1. With the 4965AGN under Vista the connection was also lost when the switch count was greater than 1, but the switch mode needed to be 1 additionally.

Nine devices operating at 2.4 GHz only ignored the channel switch announcement as expected. Surprisingly, the Intel 2200BG under Linux (ipw2200) could be silenced for 26 seconds with switch mode 1, although the device operates only at 2.4 GHz and therefore does not have to implement DFS. Of all tested device-driver combinations this was the only one adhering to the switch mode 1 in a standard compliant manner. However the device is not switching the channel if the switch mode is 0, as can be seen in Fig. 8. With the Windows XP driver the achieved DoS effect was limited to 7 seconds for the same NIC, regardless of the specified switch count. The Intel 4965AGN completely lost connection when switch mode was 1. All other devices ignored the specified switch mode. The five devices supporting 802.11a ignored switch mode 1 but were attackable with switch mode 0 even when operating on 802.11b/g channels (Fig. 9). Thus a DoS effect of 5 to 15 seconds could be achieved, which was the time the devices needed to switch to the specified channel and back again after failing to resume the connection on the new channel.

The results so far presented were observed in combination with the Cisco AP. We also tested the channel switch attack with a D-Link AP and obtained different results for the Ubiquiti SRC (Linux) and Airport Extreme (Mac OS 10.5) NICs as shown in Fig. 10. The DoS effects for both devices lasted much longer than in combination with the Cisco AP. The analysis of captured data showed that this was caused by different behavior of the APs. After interrupting the connection, which resulted in absence of ACKs from the test station, the Cisco AP stopped forwarding ping requests. Instead it sent several RTS messages to check whether the lack of ACKs was caused by the hidden station problem. Receiving no CTS answer the Cisco AP sent a deauthentication message to the test station. In contrast the D-Link AP continued sending all ping requests regardless of receiving an ACK from the test station and, therefore, never sent a deauthentication message. This missing deauthentication message could be the reason for the longer delay before the test stations tried to reconnect to the AP.

*3) Results in IBSS mode:* To validate the feasibility and effects of our new attacks in IBSS mode, we tested the four most interesting attackable devices, namely the Ubiquiti SRC, Intel 2200BG, Airport Extreme and Nokia 770, again in this mode. Only with the Linux drivers for the Intel 2200BG and Ubiquiti SRC we obtained different results, shown in Fig. 11. With the 2200BG the achieved DoS effects were 7 seconds for the quiet attack and 13 seconds for the channel switch attack, both less than in infrastructure mode. With the Ubiquiti SRC the channel switch attack had no effect at all. This shows that implementations of BSS and IBSS functionality in device drivers or firmware are often detached from each other, although some 802.11 mechanisms, e.g. in the case of 802.11h, do not differ in BSS and IBSS.

## V. Conclusion

We presented a comprehensive overview of the state of the art denial of service attacks on 802.11 networks and proposed four new attacks: the quiet and channel switch attacks exploiting DFS mechanisms (802.11h), the ATIM attack exploiting the power saving mechanism in IBSS mode, and the DELBA attack exploiting the block acknowledgement mechanism (802.11e/n).

Channel switch and quiet attack have been the focus of our analysis. They exploit management information elements introduced with 802.11h for dynamic frequency selection. DFS allows the operation of 802.11a/n devices in the 5 GHz band in Europe and other countries without interfering with other applications, e.g. military radar.

By simply forging quiet or channel switch information a DoS effect of up to one minute can be achieved with a single message. Thus, the presented attacks are very energy efficient and also harder to detect than previous attacks. As a result, these attacks could be easily implemented on a battery driven mobile device and be used for long-term DoS attacks.

A solution to avoid those attacks would be the exclusive use of secured action frames in the way the upcoming 802.11w amendment proposes. Information in beacons could then completely be ignored or at least be compared with information in actions frames to keep standard compliancy.

Interestingly, the attacks are also successful with devices operating at 2.4 GHz, although DFS is not required when

operating on this frequency band. A reason for this could be cost and time saving purposes of vendors by reusing driver and firmware implementations in different devices. As a side result we found that some 802.11a/n devices ignore the quiet elements and channel switch announcements and are therefore not standard compliant. These devices and drivers violate EN 301 893 [32] and must therefore not operate in Europe despite being sold publicly. In general, our studies have shown that all tested devices do not fully adhere to 802.11h or show unexpected behavior of some kind. Thus it has to be concluded that dynamic frequency selection (DFS) based on channel measurement only exists theoretically at the moment, although it has been already introduced in 2003 and is mandatory in Europe for all devices operating in the 5 GHz band.

## REFERENCES


[1] Cisco, "German hospital leads with 802.11n mobility," 2009. [Online]. Available: http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6973/case_study_c36-522101.pdf

[2] L. Phifer, "Case study: Leveraging next-gen wi-fi to transform healthcare," jan 2009. [Online]. Available: http://itmanagement.earthweb.com/mowi/article.php/3794341/Case-Study-Leveraging-Next-Gen-Wi-Fi-to-Transform-Healthcare.htm

[3] 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, pp. 1–24. [Online]. Available: http://portal.acm.org/citation.cfm?id=646557.694759

[4] 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*. Rome, Italy: ACM, 2001, pp. 180–189. [Online]. Available: http://portal.acm.org/citation.cfm?id=381695

[5] A. Stubblefield, J. Ioannidis, and A. D. Rubin, "Using the fluhrer, mantin, and shamir attack to break WEP," in *Network and Distributed System Security Symposium (NDSS)*. The Internet Society, 2002.

[6] W. Arbaugh, N. Shankar, Y. Wan, and K. Zhang, "Your 802.11 wireless network has no clothes," *Wireless Communications, IEEE*, vol. 9, no. 6, pp. 44–51, 2002.

[7] IEEE, "Std 802.11i - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 6: Medium Access Control (MAC) Security Enhancements," IEEE, 2004.

[8] E. Tews and M. Beck, "Practical attacks against wep and wpa," in *WiSec '09: Proceedings of the second ACM conference on Wireless network security*. New York, NY, USA: ACM, 2009, pp. 79–86.

[9] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*. Urbana-Champaign, IL, USA: ACM, 2005, pp. 46–57. [Online]. Available: http://portal.acm.org/citation.cfm?id=1062689.1062697

[10] M. Acharya, T. Sharma, D. Thuente, and D. Sizemore, "Intelligent jamming in 802.11b wireless networks," in *Proceedings of OPNETWORK*. Washington D.C., USA: OPNET, 2004.

[11] M. Ståhlberg, "Radio jamming attacks against two popular mobile networks," Helsinki University of Technology, 2000. [Online]. Available: http://www.tml.tkk.fi/Opinnot/Tik-110.501/2000/papers/stahlberg.pdf

[12] C. Wullems, K. Tham, J. Smith, and M. Looi, "A trivial denial of service attack on IEEE 802.11 direct sequence spread spectrum wireless LANs," in *Wireless Telecommunications Symposium*, 2004, pp. 129–136.

[13] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan, "Understanding and mitigating the impact of RF interference on 802.11 networks," *SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 4, pp. 385–396, 2007.

[14] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "On the performance of IEEE 802.11 under jamming," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, 2008, pp. 1265–1273.

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

[16] S. Ahmad, J. V. R. Murthy, and A. Vartak, "Autoimmunity disorder in wireless LANs," DEFCON, 2008, DEFCON 16. [Online]. Available: http://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-ahmad.pdf

[17] B. Chen, V. Muthukkumarasamy, N. Guimaraes, P. Isaias, and A. Goikoetxea, "Denial of service attacks against 802.11 DCF," in *Proceedings of the IADIS International Conference: Applied Computing*, 2006.

[18] Y. Zhou, D. Wu, and S. M. Nettles, "Analyzing and preventing MAC-layer denial of service attacks for stock 802.11 systems," in *Workshop on Broadband Wireless Services and Applications (BROADNETS)*, 2004.

[19] D. J. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," in *Proc. MILCOM*, October 2006.

[20] D. J. Thuente, B. Newlin, and M. Acharya, "Jamming vulnerabilities of IEEE 802.11e," in *Proc. MILCOM*, 2007, pp. 1–7.

[21] M. Acharya and D. Thuente, "Intelligent jamming attacks, counterattacks and (Counter)^2 attacks in 802.11b wireless networks," in *Proceedings of OPNETWORK*. Washington D.C., USA: OPNET, 2005.

[22] L. Guang and C. Assi, "Vulnerability assessment of ad hoc networks to MAC layer misbehavior," *Wireless Communications and Mobile Computing*, vol. 7, no. 6, pp. 703–715, 2007.

[23] N. Cam-Winget, D. Smith, and J. Walker, "IEEE 802.11-07/2163r0 – A-MPDU security issues," IEEE, 2007. [Online]. Available: https://mentor.ieee.org/802.11/file/07/11-07-2163-01-000n-a-mpdu-security-issues.ppt

[24] L. Qian, N. Cam-Winget, and D. Smith, "IEEE 802.11-08/0755r1 – review of 802.11n A-MPDU DoS issues," IEEE, 2008. [Online]. Available: https://mentor.ieee.org/802.11/file/08/11-08-0755-01-000n-review-of-a-mpdu-dos-issues.ppt

[25] J. Wright, "High speed risks in 802.11n networks," in *RSA Conference*. ARUBA Networks, 2008. [Online]. Available: http://www.willhackforsushi.com/presentations/rsa2008-wright.pdf

[26] S. Glass and V. Muthukkumarasamy, "A study of the TKIP cryptographic DoS attack," in *15th IEEE International Conference on Networks (ICON)*, 2007, pp. 59–65.

[27] C. He and J. C. Mitchell, "Security analysis and improvements for IEEE 802.11i," in *12th Annual Network and Distributed System Security Symposium*, 2005, pp. 90–110.

[28] F. Ferreri, M. Bernaschi, and L. Valcamonici, "Access points vulnerabilities to DoS attacks in 802.11 networks," in *IEEE Wireless Communications and Networking Conference (WCNC)*, vol. 1, 2004, pp. 634–638 Vol.1.

[29] L. Butti and J. Tinnés, "Discovering and exploiting 802.11 wireless driver vulnerabilities," *Journal in Computer Virology*, vol. 4, no. 1, pp. 25–37, 2008.

[30] Q. Chen, F. Schmidt-Eisenlohr, D. Jiang, M. Torrent-Moreno, L. Delgrossi, and H. Hartenstein, "Overhaul of ieee 802.11 modeling and simulation ns-2," in *Proceedings of the 10th International Symposium on Modeling Analysis and Simulation of Wireless and Mobile Systems, MSWiM 2007*, C.-F. Chiasserini, N. B. Abu-Ghazaleh, and S. E. Nikoletseas, Eds. Chania, Crete Island, Greece: ACM, Oct. 2007, pp. 159–168. [Online]. Available: http://doi.acm.org/10.1145/1298126.1298155

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

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

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

[34] ——, "Std 802.11e – part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications – amendment 8: Medium access control (MAC) quality of service enhancements," 2005.

[35] ——, "P802.11n™/D5.0 - draft amendment to STANDARD for information Technology-Telecommunications and information exchange between systems — local and metropolitan networks-Specific requirements-Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY). amendment 4: Enhancements for higher throughput." 2008.