ulm university universität ulm

PHY and MAC Layer Security in 802.11 Networks

Bastian Königs — Ulm University, Germany — bastian.koenings@uni-ulm.de

I. Introduction

IEEE 802.11-based wireless networks are being deployed in large numbers in home, business, and public environments but also in critical environments like hospitals or production plants where reliance on their availability is crucial. 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], also intends to use WiFi for bedside drug administration[2]. Many more applications of WiFi in sensitive domains are envisioned or already implemented.

The initial approach to WLAN security was called *Wired Equivalent Privacy (WEP)* and proved to be insecure [2], [3]. Later, the amendmet IEEE 802.11i [4] provided more substantial authentication, integrity, and confidentiality protection.

Even though such security mechanisms having been introduced to the standard the availability of wireless LANs remains a particular challenge. Availability is a concern not only because jamming the physical medium 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.

Actually, despite use of modern encryption in 802.11i, management messages are send in the clear, are not authenticated, and can therefore easily be spoofed. This work focuses on the common standard amendments 802.11h and 802.11n that are less often studied by security researchers despite being in wide use. A total of four previously unknown attacks have been identified. Two of them, the *quiet attack* and the *channel switch attack* have been implemented and analyzed in detail.

In the remainder, first a classification of previously known attacks on 802.11 availability will be given in Section II. Next the four new attacks will be introduced (Sec. III) and the main findings of a detailed study of the *quiet attack* and the *channel switch attack* will be presented in Section IV.

II. Classification of Previous Attacks

A couple of earlier publications have addressed attacks on the availability of 802.11 networks. Figure 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. The attacks could be grouped into four categories:

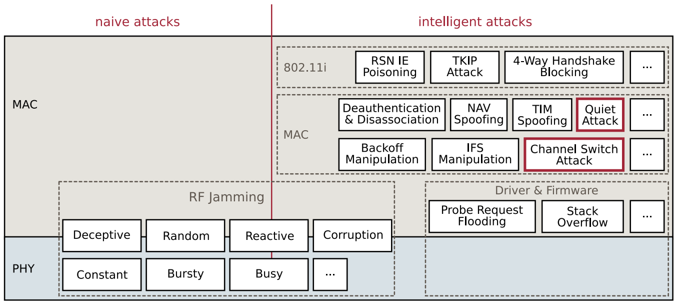

Fig. 1. Existing attacks on the availability of 802.11 WLANs.

1) *RF Jamming Attacks.* The goal of RF jamming is to distort the radio signal of another sender by sending signals or noise on the same radio channel, thereby preventing proper reception of the signal at the receiver(s).
2) *MAC Layer Attacks.* MAC layer attacks target 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., for fair medium access, an attacker is able to prevent others from participating in the wireless network.
3) *802.11i Attacks.* Although 802.11i actually belongs to the MAC layer, these attacks form 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 DoS 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 or firmware. In that case the effect of the DoS attack is not limited to unavailability of the network but impacts the whole system.

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

[2] http://www.wi-fiplanet.com/columns/article.php/3793226

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

Attacks that have been simulated (S), implemented (I), not yet tested but are theoretically applicable (T), or not applicable (-) in 802.11 infrastructure BSS or IBSS networks. *Attacks marked with * are newly presented in this work.*

A. *Current State of the Art*

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 the first goal of this work is to identify additional weaknesses and new DoS attacks that stem from those amendments.

The second observation is that many attacks are only described theoretically or have been tested only in simulation, as shown in Table I. However, as experience shows, 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 [5].

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 the 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 DoS 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

The four new identified attacks on 802.11 availability fall in the category of MAC layer attacks. The *quiet attack* and the *channel switch attack* based on 802.11h will be the focus of the remainder. Also the *ATIM attack* and the *DELBA attack* which exploit power saving mechanisms in ad hoc mode (IBSS) and the block acknowledgement of 802.11e/n, respectively, will be shortly presented.

The main purpose of the amendemt 802.11h has been the introduction of frequency spectrum management mechanisms to enable the usage of the 5 GHz band in Europe. One of these mechanisms is dynamic frequency selection (DFS), which is mandatory in Europe for 802.11a/n devices operating at 5.25–5.35 GHz and 5.47–5.725 GHz [6]. 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, DoS effects can be achieved.

Management information can be easily forged because, unlike data messages, they are neither encrypted nor integrity protected and require no authentication. The future amendment 802.11w [7] aims to change this for disassociation, deauthentication and action frames, but not for beacon messages. So even when the amendment will be implemented in the future, at least three of the following attacks remain feasible.

A. *Quiet Attack*

To be able to accurately measure the current channel for other activities, an access point (AP) includes a *quiet element* in beacons or probe responses. The quiet element specifies a certain time interval for which receiving stations of the BSS have to be silent, i.e., send no messages, so that channel measurement can take place. The quiet element, depicted in Figure 4 b), 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. The *switch mode*, see Figure 4 c), 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 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 to change to a different channel. *New channel number* can even be set to an invalid channel. To further enhance the efficiency of the DoS 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.

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.

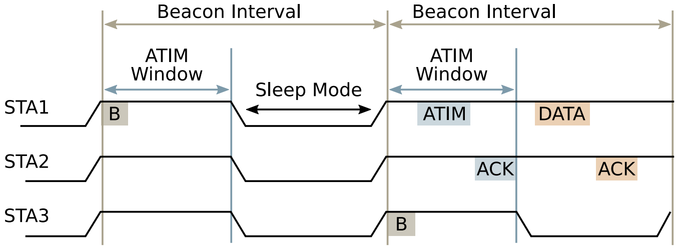

Fig. 2. Power saving mechanism in an IBSS.

In an IBSS the power saving process is realized 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. Figure 2 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. 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 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 introduced by amendment 802.11e and also used in upcoming 802.11n. 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 Figure 3.

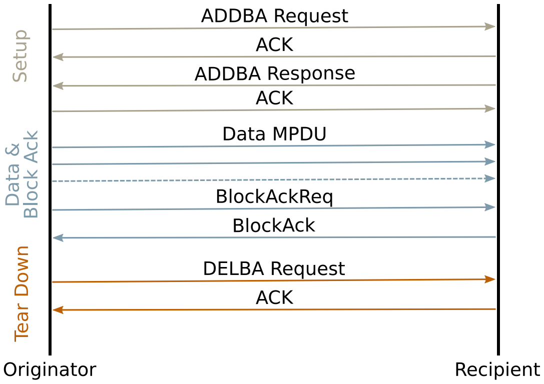

Fig. 3. Phases of the block acknowledgement.

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 frees the buffers of sender and receiver.

As DELBA messages are unprotected action frames, an advesary can forge the DELBA message to terminate block acknowledgement communication and free buffers on sender and receiver side.

IV. Analysis of Quiet and Channel Switch Attacks

To allow an efficiency-evaluation of the quiet and channel switch attack, the number of injected packets required to achieve a one minute DoS effect was measured in a real-world testbed setup. Both attacks were tested with 15 devices: Intel 2100B, Intel 2200BG, Intel 3945ABG, Intel 4965AGN, Intel 5100AGN, Ubiquiti SRC, Airport Extreme, Intersil ISL3890, Lucent Wavelan, iPhone 3G, iPod Touch 2G, Nokia 770, Nokia N810, Nokia E51, Nokia E71.

To compare the results with a well known attack, an efficiency-optimized version of the deauthentication attack was tested as well. This attack exploits the association process

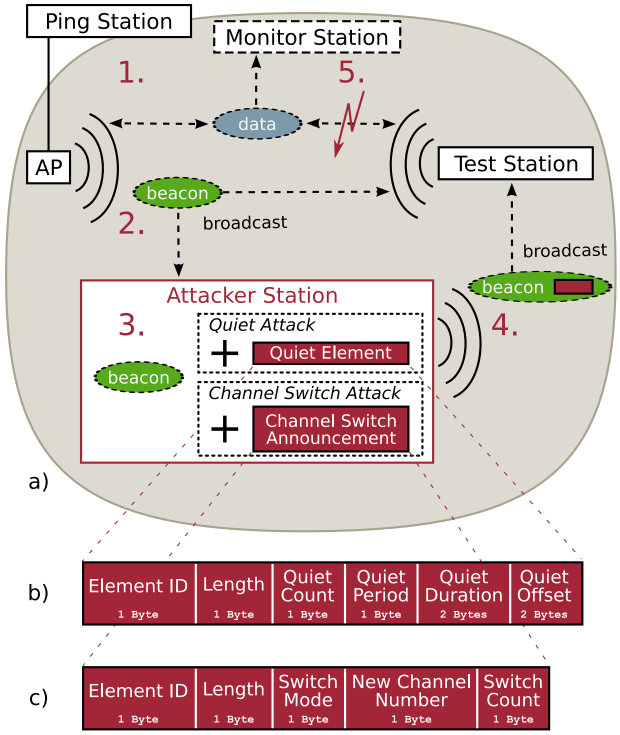

Fig. 4. Attack testbed and attack flow of quiet attack and channel switch attack a) and the corresponding frame format of the quiet element b) and channel switch announcement c).

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, an attacker could forge this message on behalf of the station or the AP. The attack was implemented in such a way, that one deauthentication message was sent whenever a data packet of the test station was received.

A. Testbed Setup

The testbed, see Figure 4 a), consisted of an AP, a ping station, a monitor station, the test station and the attacker station. The ping station (1.) used ICMP pings to generate constant data traffic to the wireless test station. The attacker captured beacon frames from the AP (2.), injected the forged information elements (3.), and retransmitted the modified beacon frames (4.) forging the MAC address of the AP. The NIC of the monitor station (5.) 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. Channel switch attacks were executed with varying switch mode, switch count and new channel number. The used frequency was varied between 2.4 GHz and 5 GHz channels.

B. Results

The tests showed that 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 some older devices only operate at 2.4 GHz and therefore not implement IEEE 802.11h. As presented in Table II, 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 II
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. 5). These two examples show that current devices (802.11n) as well as older devices (802.11b) are 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.

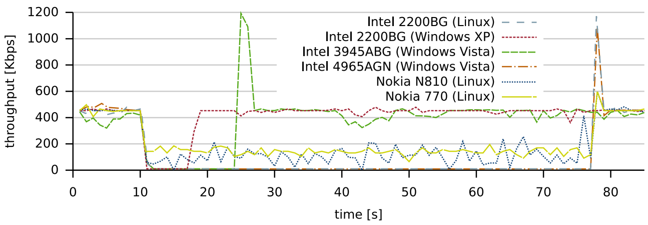

Fig. 5. Measured throughput during quiet attacks with a maximum quiet duration of 65 535 TUs against four attackable devices.

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 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.

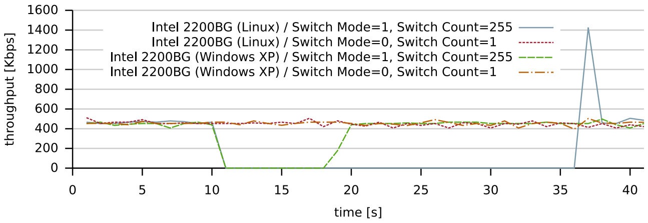

Fig. 6. Measured throughput during channel switch attacks against an Intel 2200 NIC.

Nine devices operating at 2.4 GHz 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 Figure 6. 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.

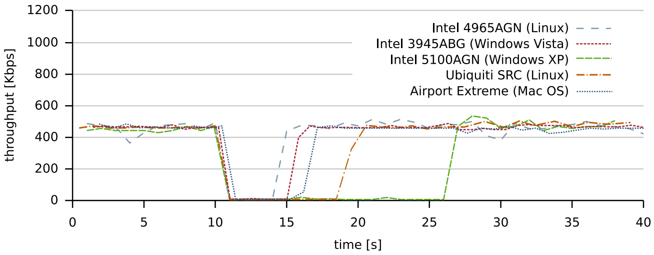

Fig. 7. Measured throughput during channel switch attacks with switch mode 0 and switch count 1 against 5 attackable devices.

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. 7). 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.

V. Conclusion

This work presented a comprehensive overview of the state of the art DoS 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 the 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 5.2 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 because they only require very few messages. As a result, these attacks could be easily implemented on a battery driven mobile device and be used for long-term DoS attacks.

Interestingly, the attacks are also successful with devices operating at 2.4 GHz, although DFS is not required when operating on this frequency band. As a side result it was 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 [6] and must therefore not operate in Europe despite being sold publicly. In general, the 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 5.2 GHz band.

References

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

[2] 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

[3] 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.

[4] 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.

[5] 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.

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

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