Run Away If You Can:
Persistent Jamming Attacks against Channel Hopping Wi-Fi Devices in Dense Networks

Il-Gu Lee, Hyunwoo Choi, Yongdae Kim, Seungwon Shin, and Myungchul Kim

Graduate School of Information Security
Korea Advanced Institute of Science and Technology (KAIST)
291 Daehak-ro, Yuseong-gu, Daejeon, Republic of Korea 305-701
{iglee9,zemisolsol,yongdaek,claude,mck}@kaist.ac.kr

Abstract. Wireless local area networks (WLANs) can adopt channel hopping technologies in order to avoid unintentional interferences such as radars or microwaves, which function as proactive jamming signals. Even though channel hopping technologies are effective against proactive types of jamming, it has been reported that reactive jammers could attack the targets through scanning busy channels. In this paper, we demonstrate that reactive jamming is only effective against channel hopping Wi-Fi devices in non-dense networks and that it is not effective in dense networks. Then, we propose a new jamming attack called "*persistent jamming*", which is a modified reactive jamming that is effective in dense networks. The proposed persistent jamming attack can track a device that switches channels using the following two features, and it can attack the specific target or a target group of devices. The first feature is that the proposed attack can use the partial association ID (PAID), which is included for power saving in the IEEE 802.11ac/af/ah frame headers, to track and jam the targets. The second feature is that it is possible to attack persistently based on device fingerprints in IEEE 802.11a/b/g/n legacy devices. Our evaluation results demonstrate that the proposed persistent jamming can improve the attack efficiency by approximately 80% in dense networks compared with the reactive jamming scheme, and it can also shut down the communication link of the target nodes using 20 dBm of jamming power and a 125 ms response time.

Keywords: WLAN, jamming, channel hopping, device tracking, ID, fingerprint, security.

1 Introduction

Wireless local area network (WLAN) technologies are an essential feature of everyday life because they are used in home networking, smart mobile devices, network infrastructure, and much more. These applications require very high throughput and long service coverage. In order to meet these demands of the users, WLAN technologies have been evolving to use wider channel bandwidths for IEEE 802.11n/ac [2,4] in the 2.4/5 GHz industry science and medical (ISM) band, and they support lower receiver sensitivity for a wider range of up to approximately 1 km for IEEE 802.11af/ah in the TV white space or sub-1 GHz frequencies [5,6]. As more and more wireless devices are connected and wireless access points (APs) are densely deployed in the scarce frequency spectrum and

A. Stavrou et al. (Eds.): RAID 2014, LNCS 8688, pp. 362–383, 2014.

in the limited region, the failure probability of packet transmissions is expected to increase due to interference from other devices and jammers. Because the 2.4 GHz band is already congested and the 5 GHz band will be congested soon [15], the wireless environment may suffer severe interference from unintentional jammers and intentional jammers [9,17].

Recent studies have demonstrated that various proactive jamming methods such as constant, random, and deceptive jamming can be launched easily in wireless networks [10,26]. Meanwhile, in order to manage jamming attacks, wireless nodes can adopt a channel hopping scheme through which nodes can switch their channel frequencies as required in order to improve the link quality [10,28,29]. If a certain channel is not available due to jamming signals, the wireless nodes switch channels to another idle channel according to the channel hopping protocol; consequently, the wireless nodes can avoid proactive jamming attacks. In the literature, several studies have proposed a smart jamming scheme called "*reactive jamming*" for efficient jamming attacks [10,26]. The reactive jammer, which is the most popularly discussed method for disturbing channel hopping nodes, investigates a busy channel in order to identify a channel-hopped node and begins emitting a jamming signal as soon as it senses activity on that channel because the shared nature of the wireless medium allows adversaries to easily monitor the communications between wireless devices. Therefore, even though the target nodes have switched to another channel due to the jamming signal, the jammer can switch to the target node's new channel and attack again. However, the reactive jamming schemes assume that attackers can locate a channel-hopped target because the network is not dense [10,26,28,29]. If there are multiple devices using different channels, the challenging question to the adversary is how to determine which channel is being used by the target device.

Our contribution In this paper, we first demonstrate that the existing jamming attacks are not effective against channel hopping devices in dense networks. Because there are multiple nodes in the channel in dense networks, a conventional jammer cannot identify the target node's channel among the multiple candidates due to the lack of channel awareness and device information. In this situation, the only way to disturb a specific node's communication is to emit a jamming signal to all busy channels and, consequently, the detection possibility of the jamming attack increases and the jamming efficacy decreases in terms of the attacker's cost and attacking damage. For this reason, a jamming attack in a dense network is considered extremely difficult. Despite the limitations, in order to stop this, in this paper we propose a new jamming method called "*persistent jamming*", which is a novel attack in the form of modified reactive jamming. Moreover, we demonstrate that identifying a channel hopping device and launching a jamming attack in a dense network are feasible. Based on the observation that the partial association identification (PAID) and device fingerprints can be used to identify channel hopping devices in dense networks, the attacker can persistently track and jam target devices. Our evaluation results demonstrate that persistent jamming using the PAID and device fingerprint detection can improve the attack efficiency by approximately 80% in dense networks compared with the reactive jamming scheme, and it can continuously degrade the throughput to close to zero against channel hopping target devices in order that the communication link is disconnected with a 20 dBm jamming power and 125 ms response time.

Our work provides the following three key contributions.

- This is the first investigation of the limitations of the unprotected PHY header that is identified using PAID and fingerprints extracted from the frame header in order to track a target device or a target group of devices, and to examine the feasibility of persistent jamming.
- Persistent jamming is experimentally evaluated in a field programmable gate array (FPGA) prototype that was designed and verified for commercialization as an IEEE 802.11n/ac Wi-Fi chipset.
- The proposed attack is also implemented and evaluated in a cycle true and bit true emulation platform in order to demonstrate its feasibility and performance in a dense network.

The remainder of the paper is organized as follows. In Section 2, we present the related work on the jamming attack and mitigation. In Section 3, we overview the WLAN frame format to discuss the security implications of frame headers, and propose the persistent jamming attack based on the security limitations of frame headers. In Section 4, we present the experimental setup and demonstrate the evaluation results. In Section 5, we recommend security remedies. The paper is concluded in Section 6.

2 Related Work

In this section, we present the related literature on jamming attack and mitigation.

2.1 Jamming Attack

Wireless LAN networks are highly sensitive to incidental and intentional interferences because they use a carrier sense multiple access with collision avoidance (CSMA/CA) mechanism and an orthogonal frequency division multiplexing (OFDM) modulation. IEEE 802.11-based WLAN devices defer access to a channel if the channel is busy at the transmitter or if it cannot decode the distorted OFDM modulated symbols at the receiver when the interference exceeds a specified tolerance level. Interference occurs when a node transmits a signal without verifying whether another node is accessing the same channel through increasing the clear channel assessment (CCA) threshold. In this way, the malicious node achieves its goal by degrading the signal quality at legitimate receivers or by disabling channel access at legitimate transmitters to disrupt the communication link or shut down legitimate devices. Thus, the availability of the wireless network is subverted easily through jamming attacks, which easily allow an attacker to disturb the wireless devices'communications through emitting electromagnetic signals in the wireless medium. Recently, increasing jamming attacks have been reported because attackers can easily disrupt wireless communications networks using commercial jamming devices and easily modified commercial products [8, 10, 17, 26].

There are two types of jammers: proactive jammers and reactive jammers. The proactive jammers have three forms: constant, random, and deceptive [10].

As their names imply, the constant jammer and random jammer emit a constant jamming signal continuously and jamming signals at random times, respectively, while the deceptive jammer injects decodable packets into the channel. Proactive jammers are the most prevalent jamming form due to their easy implementation that attempts to emit jamming signals irrespective of the traffic pattern in the channel, but they are inefficient in terms of attacking damage, detection probability, and energy efficiency due to the lack of channel awareness. In contrast, reactive jammers only emit a jamming signal if the channel is busy. If there is no traffic in the current channel, the reactive jammer waits and senses the channel for a predetermined time, and then switches to a busy channel and continues to jam. It is a more effective jamming attack even though the implementation is relatively complicated. This channel awareness allows for efficient jamming because it must transmit short jamming signals in a timely manner. The authors of [26] developed a software-defined reactive jammer prototype and demonstrated that a real-time reactive jammer is feasible and a serious threat to WLAN services. However, previous studies on the reactive jammer assuming non-dense networks [10, 17, 26] are limited because it has a low attack success rate when the target device switches to a different channel in a dense network because conventional jammers cannot differentiate a specific device or target group of devices from multiple candidates. In this paper, we focus on a realistic environment, i.e. a dense network, in which there are multiple devices using different channels and, in Section 5, we experimentally demonstrate that the existing reactive jamming is not effective in dense networks.

2.2 Jamming Mitigation

Traditionally, channel hopping and link adaptation techniques have been developed as solutions that mitigate the effect of jamming [1, 14, 16, 19, 22, 23, 31]. Channel hopping techniques attempt to avoid jammed channels through changing the channel among the orthogonally available channel bands. There are three types of channel hopping schemes: proactive, reactive, and passive. A pair of nodes using proactive channel hopping has a hopping sequence that periodically changes [14]. In a reactive channel hopping scheme, a node only switches to a different channel if it detects the presence of jamming signal [1, 16, 19, 23]. If a coordinator or pair of nodes decides to switch channels, all other nodes in the network switch channels as well. Consequently, the proactive channel hopping schemes are fast, but they are not used in WLANs due to their inefficiency and complexity, whereas reactive channel hopping schemes are slow but are used in WLAN products. In some commercial devices, passive-type channel hopping using firmware enables users to switch channels [24], and users can switch channels manually if the link is disconnected. However, passive channel hopping schemes require much longer to avoid interference and could worsen the situation. In addition, the IEEE 802.11h standard defines the dynamic frequency selection (DFS) mechanism in order to avoid interference from radars and other WLAN devices [3]. The DFS mechanism allows an AP and its associated stations to dynamically switch to another channel in order to avoid interference.

Link adaptation techniques can be used to improve link quality in order to compete with dynamically varying interference [22, 24, 31]. A node can mitigate the jamming effect in order to cause the link to be more robust using link adaptation schemes such as transmit power control (TPC), modulation and coding scheme (MCS) control, and CCA threshold control. Link adaptation schemes can be effective against jammers that follow the equivalent isotropically radiated power (EIRP) regulations determined by the Federal Communications Commission (FCC), but a malicious jammer may transmit signals without considering the transmit power limitations and emit radio interference with external power amplifiers even if the output is saturated. Therefore, typical legitimate nodes first attempt to adapt the link through controlling the system parameters, and then they switch channels if the error rate or link quality does not meet the system requirements.

In order to mitigate jamming attacks, the authors in [10] and [28] proposed a series of basic detection methods based on the PHY layer. The basic concept of detecting the jamming attacks was simple: the presence of jamming radio signals at the receiver can affect the received signal strength. In addition, there have been several studies on jamming effect analyses and interference mitigation methods [16,23,24]. The authors analyzed the jamming effects on WLAN systems and presented the TPC and rate control as competition against jammers. In order to achieve this, they presented a smart jammer model that scans the entire spectrum of channels, locates a busy channel, and attacks again. However, in highly dense networks and congested spectra, the attacker cannot identify specific target nodes or a target group because there are numerous candidates, and the busy state does not guarantee that the target devices will be in the channel. Thus, the attacker cannot continue to attack the target devices in dense networks.

3 Our Persistent Jamming Attack

This section introduces the tracking approaches of PHY PAID and device fingerprint to trace the channel hopping target nodes that hop channels while communicating with the AP in order to avoid jamming attacks. We review the frame format and depict the limitations from a security perspective in Section 3.1. In Sections 3.2 and 3.3, we describe the persistent jamming attack mechanism that includes the tracking and jamming techniques using PAID and device fingerprints such as SNR and timing offset.

3.1 Security Limitations

As shown in Figure 1, even though a target node switches to another channel in order to avoid jamming attacks, a persistent jammer can identify the target node's channel frequency based on the frame header information: the ID information in the signal field and the device fingerprint from the preamble. Then, the attacker can use this information to attack more effectively in ways such as tracking and jamming target devices, or jamming at a specific time or frequency. Therefore, through capturing a single packet and examining its header, an adversary can determine the existence of the target in a channel.

The frame header information is becoming more important because modern wireless communication systems have been designed to support advanced transmission techniques for high throughput, high energy efficiency, and quality of service (QoS). Therefore, frame headers include more information for wireless connectivity in the evolving Wi-Fi standards. Frame headers are transmitted using binary phase shift keying (BPSK) modulation and the lowest rate transmission mode (6 Mbps) in order to ensure reliable reception. However, frame headers do not have protection mechanisms, but the data payload is protected by security protocols and encryption techniques. The encrypted data payload uses cryptography to protect the data against eavesdropping, tampering, forging, and other security attacks. Even if the frame is intercepted, the encryption causes the data payload to be unusable. However, the unencrypted header that contains the PAID and device fingerprint is not protected: if the channel frequency of a transmitted packet is tracked, an adversary can easily jam the link to prevent communication. This is a significant threat to wireless device users because the channel frequency usage is important privacy information in a wireless network, and this data can be tracked and jammed by an attacker.

Figure 1 presents the frame structure of the IEEE 802.11ac standard specified in [4]. A frame contains a header, payload, frame check sequence (FCS), and padding/tails. The frame header consists of a preamble, signal fields, service field, and medium access control (MAC) header. The PHY frame header is used in the signal detection, timing acquisition, and signal decoding information, and the MAC frame header includes the address information and control signals. The frame body field contains variable length data information which can be encrypted. The L-STF is used for carrier sensing, gain control, and coarse frequency acquisition; the L-LTF is used for fine frequency acquisition and channel estimation. The signal fields convey information about the rate, length, and transmission mode for the receiver to decode the remainder of the received frame. The VHT-STF is used for fine gain control, and the VHT-LTF is used for channel estimation of the VHT frames. The VHT-SIG-B is used for user-specific information in multi-user transmissions. The service field is originally used to initialize the descrambler. In the data fields, the receiver decodes the incoming symbols and tracks phase errors using pilots. Any receiver can detect the PAID included in the VHT-SIG-A or extract the device fingerprint from the STFs and LTFs because the frame header is not protected. In the IEEE 802.11ac/ah/af standard, the PAID in the physical (PHY) layer header is adopted in order to improve the power efficiency for a specific user's device. The PAID information is

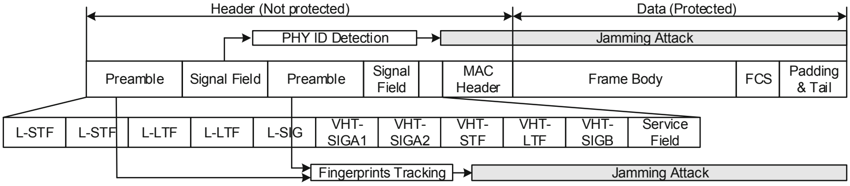

Fig. 1. IEEE 802.11ac WLAN frame structure and persistent jamming attack

a good indicator for identifying a specific node, but there is no PAID information in legacy frames such as IEEE 802.11a/b/g/n. Therefore, we use both PAID and fingerprint detection for our persistent jamming in this paper. Through utilizing the PAID information in the frame header, a persistent jammer is able to detect the changed channel if it has captured the PAID information in previously attacked channels. If there is no device that supports power saving using PAID, an attacker can track and jam a specific target or a group of target devices through analyzing the physical characteristics from the frame header information and using the device fingerprints.

3.2 ID Detection

Because WLAN devices use a contention-based channel access scheme, the preamble and signal field should be detected and decoded by all nodes in the network in order to appropriately defer access to a channel. Based on the CSMA/CA protocol, each device must listen to the channel in order to determine whether it should decode the incoming packet. Although several MAC level power saving schemes exist, they are not designed for the awake mode and they improve power efficiency through increasing the sleep period. In many consumer electronics, it is expected that an active mode device has fewer changes in the sleep mode in order to maintain an awake state that supports QoS. Therefore, the IEEE 802.11ac/af/ah standard defines the physical layer header information in order to determine whether or not to listen and decode an incoming data packet. The physical layer header information for power saving is called PAID, and it is used to identify the intended receiver so that non-intended receivers can avoid unnecessary signal processing for the remainder of the packet and to allow micro-sleeps for physical layer power saving. In order that devices in the same or overlapped basic service sets (BSSs) can avoid having the same PAID and to maximize the power saving efficiency, the PAID is determined by the device's PAID using an offset based on the AP's BSSID with which the device is associated. The additional offset minimizes the probability of the same ID use among OBSSs. Therefore, the PAID in the signal field can be used to identify the destination of the packet for any node in the wireless network. If the frame includes the ID information, it is much easier to identify the target node than the device fingerprint detection because the false positive detection rate of the ID is as low as the error rate of signal field, which is modulated using the BPSK and 1/2 code rate, as described in Section 4.1. As an alternative approach, MAC IDs such as address or SSID can be utilized. The PHY signal field has its own cyclic redundancy check (CRC) so that the receiver can use it reliably at the beginning of the frame, while the data field including MAC ID requires long latency because CRC is attached at the end of the frame even if the MAC ID is not encrypted. Furthermore, PHY header is always modulated by the most robust modulation and coding scheme, but the MAC header can be modulated by higher modulation and coding scheme, which is more susceptible to channel noise and interference.

3.3 Fingerprint Detection

Wireless fingerprinting techniques have typically been investigated for device localization [11, 12, 32]. Location fingerprinting uses deterministic and probabilistic methods for static estimation in order to determine the position using the device's physical characteristics such as the received signal strength indicator (RSSI) and clock jitter. The wireless fingerprinting techniques can be applied in location-based services or to improve the system security level. However, malicious uses of device fingerprints have not been investigated, particularly regarding jamming attacks. In this paper, we first demonstrate that a wireless device can be tracked and attacked persistently if an adversary can extract fingerprints from any frames in the wireless channel. The attacker can track the target device based on the device fingerprints generated using a unique circuit design. An electronic fingerprint or radio channel fingerprint enables the identification of a wireless device using its unique characteristics. An attacker is able to extract and analyze the physical characteristics from the PHY header, such as timing offset, RSSI, signal-to-noise ratio (SNR), and error vector magnitude (EVM); then, it can track and jam a target device using the fingerprints. In this paper, we describe how to extract the SNR and timing offset from these fingerprints in order to demonstrate the feasibility of device tracking. Although any fingerprints can be used for persistent jamming, we demonstrate the feasibility of the attack using the SNR adjusted by the EVM or timing offset assisted by both preamble and pilots due to high accuracy of estimation and reusability of the existing circuits in WLAN devices. Furthermore, in order to improve the uniqueness, we combine two different physical fingerprints, and evaluate them in Section 4.1. In a highly dense network, if higher uniqueness of physical fingerprints is required, we can combine a set of physical fingerprints.

SNR Estimation. As a signal quality indicator in a typical WLAN indoor wireless channel, the SNR can be an important factor in link adaptation based on the transmission signal quality and channel propagation loss in the received signal. An attacker can also use the measured SNR with the captured frame to determine whether a specific device uses the channel frequency in a typical indoor channel. The long training field is 8 μs in length and is composed of two identical 3.2 μs symbols. As a result of the symbol repetition, this long training field can be used to estimate the SNR [30]. The receiver extracts the two long training samples before the fast Fourier transform (FFT) processing in order to estimate the received signal quality including the transmitter/receiver impairments and channel propagation loss. In order to calculate the noise power, the samples from the first long training symbol are subtracted from the samples of the second symbol. Moreover, the two symbols are averaged in order to calculate the signal power. With the noise and signal powers, the receiver can calculate the SNR for the received frame.

The EVM is an error vector magnitude, which is a measurement to calculate distance between the received sample points and the ideal locations. The EVM can be calculated in the frequency domain using a more complicated calculation after estimating the channel response and decoding the signal field, while the

SNR can be calculated in the time domain using a simple calculation with two long training symbols [2,4,18]. The SNR typically has a linear relationship with the EVM [21]. In addition, the EVM allows the receiver to further analyze the characteristics through observing noise patterns in the frequency and time domains as a different form of SNR representation. The EVM is more useful in analyzing digitally modulated signals because the receiver can use the long data payload or pilot subcarriers to measure the signal quality, even though it requires more multipliers and adders to calculate the values of higher modulations. The EVM is a good indicator for relating the analog impairment to the device fingerprints. Through calculating the average EVM for every symbol over the subcarrier indexes of a signal field or the pilot subcarriers during one packet, the attacker can identify the device using the fingerprints. Consequently, the attacker can adjust the SNR calculated at the preamble using the pilots' EVM until the end of the frame.

Timing Offset Estimation. The sampling timing offset results from the oscillator difference between the transmitter and receiver. In the frequency domain, the phase rotation increases as time passes and the amount of phase rotation increases as the frequency increases, which is the same as in the sampling phase error. The IEEE 802.11 standard limits the timing offset to less than +/-20 ppm for WLAN devices. According to the Fourier transform properties, the time shift of the time domain signal has a phase rotation in the frequency domain representation of the signal, where the amount of phase rotation increases as the frequency increases. Thus, the timing offset estimator is derived using the least square rule [20]. In the derivation, the amount of sampling phase error is assumed to be small in order that the exponential term can be approximated using the linear function of the phase error. The accuracy of the estimator can be improved through using more subcarriers in multiple symbols.

Furthermore, because the carrier frequency and sampling frequency in wireless communications systems are driven by a common clock source, the frequency offset estimation result can be used to estimate the timing offset in order to improve the estimation accuracy [13]. The carrier frequency offset (CFO) is the carrier frequency difference between the transmitter and receiver. The phase rotation between two samples in repetitive training symbols separated by a time delay allows the receiver to calculate an accurate estimate of the carrier frequency offset. In WLAN systems, two preamble structures are supported, i.e. short and long preambles. The short preamble consists of 10 repetitions of the same symbol with a duration of 0.8 μs. The long preamble has two repeated symbols with a symbol period of 3.2 μs. Because the symbols are repeated, the phase rotation between two successive symbols can be estimated without knowing the channel response. The CFO is estimated twice using the short and long preambles. The initial coarse CFO is estimated using the short training field, and then the residual fine CFO is estimated using the long training field. The initial value in the timing offset estimator can be appropriately assigned using the CFO estimation, which is calculated using the preamble in advance. Then, the timing offset is adjusted using the phase offsets of the pilot tones in the data.

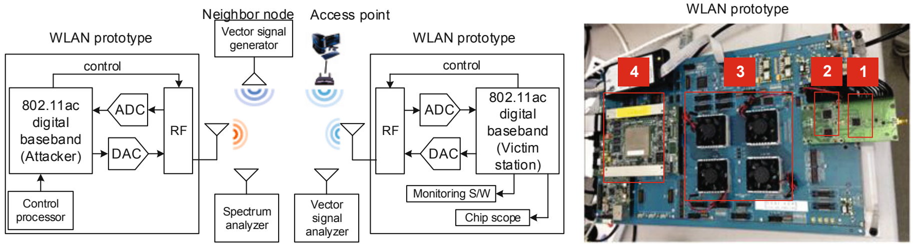

Fig. 2. Experimental setup for the prototype system

4 Implementation and Evaluation of Our Proposed Attack

In this section, we describe the experimental setup for the prototype and emulation for our proposed attack. The prototype is used for realistic experiments in the laboratory, and the emulation environment is used for multiple BSSs. Then, we present the experimental results and discuss their implications.

4.1 Real World Experiment

Experimental Setup. As shown in Figure 2, the experimental setup consisted of two WLAN prototypes, a commercial AP, a vector signal generator (VSG), a vector signal analyzer (VSA), and a spectrum analyzer. The FPGA prototypes satisfy the functionalities and performance requirements of the IEEE 802.11ac standard. One prototype is an attacker that performs a programmed jamming attack using a software controller, and the other prototype is a target node that communicates with the commercial AP. The performances and functionalities can be observed through monitoring software and a chip scope. The target node and AP communicate on channel 44. If the packet error count is larger than a predetermined threshold due to interference, they switch to channel 60. The VSG functions as a neighbor node that sends IEEE 802.11ac compliant frames in channel 52. A spectrum analyzer is used to monitor the full span spectrum in the ISM bands, and the VSA is used to analyze the signal characteristics and its effect. The image in the right of Figure 2 also illustrates the developed WLAN prototype, which consists of (1) MAX2829 RF IC, (2) analog device AD9780 digital-to-analog converter (DAC), Texas Instruments ADS4249 ADC, (3) four Xilinx Virtex6 FPGAs, and (4) an ARM Cortex-A5 processor. The four FPGAs are programmed for functionalities in the IEEE 802.11n/ac system, which has been verified with commercial products to meet the Wi-Fi certification requirements. The developed WLAN prototype can be utilized for a persistent jamming attack, and if the hardware of the other WLAN products supports functionalities for IEEE 802.11ac, such hardware can be used for the proposed attack. In order to reduce development cost, an universal software radio peripheral (USRP) can be used to develop the WLAN prototype as an alternative to the FPGAs.

This prototype was developed in order to verify the functionality and performance of the digital baseband PHY/MAC system before taping for silicon. The circuits targeted in the prototype were designed to support IEEE 802.11a/g/n/ac with a single antenna and to support a high data rate of up to 433 Mbps in the

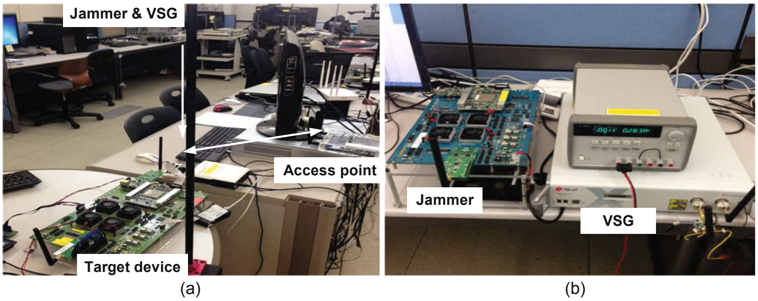

Fig. 3. Experimental setup: (a) overall test configuration and (b) jammer

2.4 GHz and 5 GHz ISM bands. The RF IC is connected to the digital baseband through the ADC and DAC ICs operating at a 160 MHz sampling rate. The digital baseband controls the RF transceiver, which changes the system parameters including the TX/RX mode, gain, channel frequency, and filter mode through external pins or a serial-to-parallel interface (SPI).

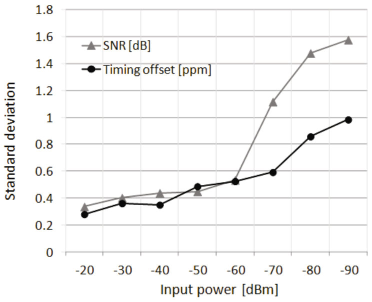

Fig. 4. Wired test: standard deviation of device fingerprints

Evaluation Results. All test results were measured in a laboratory environment. The experimental setup consisted of two FPGA boards: one was an attacker and the other was a target node. Figure 3 illustrates the experimental setup for the throughput measurement at the target node when the attacker used different jamming schemes: reactive and persistent jamming. Figure 3(a) illustrates the configuration of the jammer, neighbor node, target node, and access point, and Figure 3(b) illustrates the FPGA prototype (jammer) and vector signal generator (neighbor node). There is a target node and an AP that communicate in channel 44 or channel 60 using channel hopping in order to avoid jamming signals. They control the transmission rate using link adaptation to mitigate channel variations and jamming effects. In channel 52, a neighbor node periodically sends packets, which are generated by a vector signal generator. The jammer is implemented on the FPGA prototype through setting a high level CCA threshold in order to ignore other nodes'transmissions, and the jammer generates a jamming signal based on a jamming strategy: a reactive or a persistent jamming scheme.

Figure 4 presents the standard deviation of the measured fingerprints in the wired tests. When the input power was larger than 60 dBm, the standard deviation was less than 0.6 dB or 0.6 ppm for short distances. Small incoming signals from 60 dBm to 90 dBm had an accuracy of less than 1.6 dB or 1 ppm over long distances. Therefore, the digital baseband could estimate the SNR and timing offset as accurately as 1.6 dB and 1 ppm using preambles in the physical

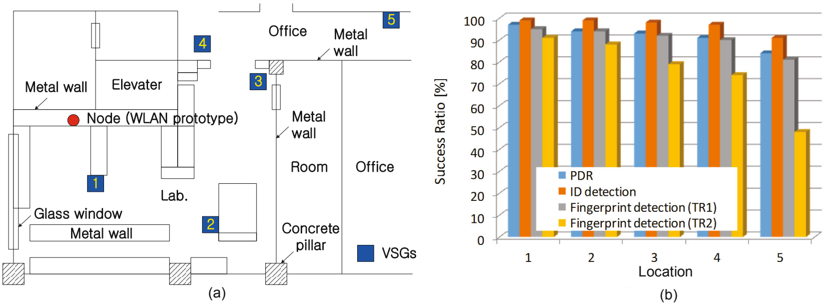

Fig. 5. Wireless test: (a) wireless measurement conditions and (b) detection success ratio vs. location

layer header for the full dynamic range. The SNR-based fingerprinting method is particularly effective for indoor channels because it is not significantly affected by multipath propagation. Furthermore, the accuracy is generally adequate for most indoor wireless applications but could be reduced through temporary physical obstructions or deviations in the radiation pattern of the target device. In low input power regions, the timing offset-based fingerprinting method has the potential to achieve higher accuracy than the SNR-based fingerprint method because the SNR and EVM are influenced more by various noise sources at the receiver in low input power regions.

Figure 5(a) depicts the experimental setup used to measure the detection success ratio of the PAID and fingerprints in wireless conditions. We measured the standard deviation of the SNR and timing offset in wired and wireless conditions. First, we tested the standard deviation in wired conditions using RF coaxial cables and RF attenuators. The VSG transmitted signals with an 8 ppm timing offset and various power levels from the vector signal generator, and the jammer measured the timing offset and SNR based on the received preambles. A Litepoint IQxel vector signal generator was used to create all packets, which were modulated and coded using MCS0 (BPSK and R = 1/2) and were transmitted in the 40 MHz bandwidth. The wired test enabled full control of the channel conditions and precise control while monitoring the results. Then, we performed a wireless test at different locations. We measured the detection success ratio in five different locations in order to include various wireless indoor channel and interference effects. The proposed jammer was located where the packet delivery ratio (PDR) and detection success ratio (DSR) of the PAID and device fingerprints on the SNR and timing offset could be measured. Locations 1 and 2 had line-of-sight (LOS) conditions, while Locations 3, 4, and 5 had non-line-of-sight (NLOS) conditions. The fingerprints were measured in root mean square (RMS) values and the standard deviation of over 100 packets.

As shown in Figure 5(b), we also measured the detection success ratio of the transmitted packet from different wireless conditions. The results demonstrated that the ID detection success ratio was higher than 90% for all locations, and the fingerprint detection success ratio was higher than 80% for all locations. The fingerprint detection performance was also related to the detection threshold.

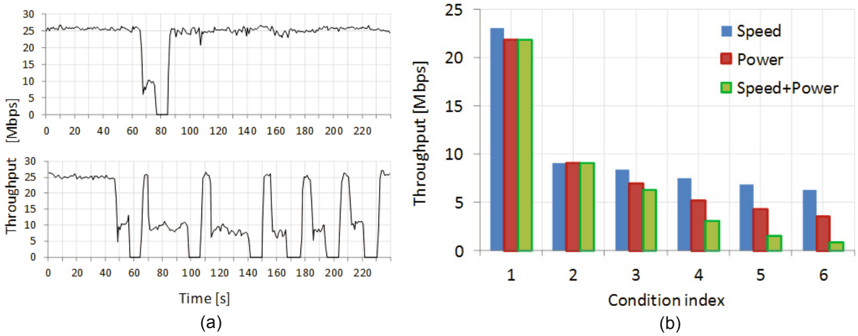

Fig. 6. (a) A throughput measurement at target node for jamming attack reactive jammr (upper), and persistent jammer (lower), and (b) jamming efficacy: throughput vs. speed and power

Two thresholds were used: Threshold 1 (TR1) had a 2 dB SNR and 1 ppm timing offset threshold, and Threshold 2 (TR2) had a 4 dB SNR and 2 ppm timing offset threshold. We observed that there was a trade-off related to the threshold between the detection success ratio and false positive detection ratio. If the threshold was large, the persistent jammer's detection was more frequent. However, the false positive detection probability also increased. In contrast, if the threshold was small, the misdetection probability was higher. The TR1 and TR2 were selected as optimal threshold sets for accurate detection and fast detection in order to cover the full dynamic range of the WLAN, respectively. A fundamental limitation of the accuracy that could be attained when measuring fingerprints resulted from the random noise and fading effects. However, if the distorted packet was filtered and adjusted by EVM and timing offset from pilots at the receiver, the SNR and timing offset measurement directly reflect the signal quality determined using a unique device. Furthermore, the PHY-based ID and fingerprint detection was faster than MAC-based schemes.

We compared the jamming effectiveness of the persistent jamming attack with a reactive jamming attack through observing the throughput at the target node. As shown in Figure 6(a), the reactive jammer succeeded in its first attack on the target node within approximately 65 seconds (above) and 45 seconds (below). After the target node switched to a different channel, the reactive jammer could not attack it because the reactive jammer attacked channel 52 rather than channel 60. In contrast, the persistent jammer switched to the target device's channels. As a result, the measured throughput was continuously degraded even though the target node switched channels. In order to evaluate the efficacy of the jamming schemes over the attacker's capability, different response times and transmit powers were used as described in Table 1. In this table, (x,y) refers to the condition with x second response time (R_T) and y dBm transmit power (T_P). The reactive jammer used only the fastest response time and largest transmit power in order to obtain the best performance, while the persistent jammer had various response times and transmit powers for comparison with the reactive jammer.

Figure 6(b) presents the effective throughput over the condition index from Table 1, as a function of the jamming speed and transmission power for reactive and persistent jammers. The results indicate that reactive jamming is significantly less effective than persistent jamming, which can significantly reduce the throughput of the target node in dense network conditions. The reactive jammer could not improve the jamming efficacy in the communication link even though it had the fastest response time and highest transmit power, while the persistent jammer could improve as the speed and power increased. As we presented in Section 2.1, due to the inefficiency and complexity, Wi-Fi devices use the reactive channel hopping schemes or passive-type channel switching scheme instead of the proactive channel hopping schemes. Therefore, in the current WLAN technologies, the target nodes change their channel frequencies slowly when link quality is degraded statistically. If we assume that target Wi-Fi devices can switch the channel very fast, channel scanning speed is important for persistent jamming attack. The jamming speed including channel scanning time and detection processing time is related to the jamming efficacy. The test results indicate that jamming efficacy could be improved as jamming speed is faster. Regarding the channel scanning time, there are three orthogonal channels in 2.4 GHz ISM and 19 channels in 5 GHz ISM band in 20 MHz channel unit. Therefore, it is possible to detect the target node when the attacker switches at most 5 times for full channel scanning because IEEE 802.11ac supports 80 MHz band operation.

Table 1. Experiment conditions

Condition index	Jamming type	Speed	Power	Speed+Power
1	Reactive	(0.125,0)	(2,20)	(0.125,20)
2	Persistent	(2,0)	(2,0)	(2,0)
3	Persistent	(1,0)	(2,5)	(1,5)
4	Persistent	(0.5,0)	(2,10)	(0.5,1.0)
5	Persistent	(0.25,0)	(2,15)	(0.25,15)
6	Persistent	(0.125,0)	(2,20)	(0.125,20)

4.2 Large-scale Emulation

Experimental Setup. In the developed prototype, it is difficult to evaluate the system in dense network conditions because it is necessary to have numerous hardware and software resources or expensive equipment. In order to overcome such problems, a software-based emulation environment can reduce the evaluation cost and experimental setup time. Therefore, the hardware behavior and performance can be emulated in the developed emulator. The hardware is manufactured using a hardware description language (HDL) in order to perform synthesis, place, and routing with various tools. Our FPGA prototype system was initially developed to be verified using a hardware-like C emulator. The emulator has been described with hardware architecture, and it has a cycle-true and bit-true description. That is, the emulator is programmed like a register

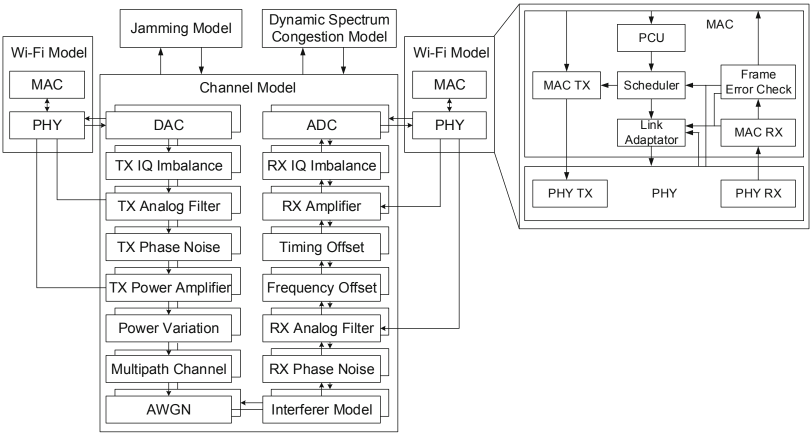

Fig. 7. Emulation environment, channel model, and MAC model

transistor level (RTL) description model, and it has timing and bit widths for all signals. This emulator was verified using a bit-matching process between the RTL and C model. The emulation performance curves are the same as the performance measurement results on the RTL targeted FPGA prototype system. In this way, we developed an emulation model that evaluates attack methods in dense networks.

Figure 7 presents the emulation model used to analyze the jamming effect in dense network conditions. The emulation model consisted of two Wi-Fi models for the sender and receiver, a channel model, a jammer model, and a dynamic spectrum congestion model. The Wi-Fi model had the same function and performance as the developed commercial hardware design. The channel model was developed with the IEEE 802.11 recommended channel model including RF/analog impairments. The dynamic spectrum congestion model randomly generated traffic from multiple nodes in the network. The jamming model could support one jamming strategy among the random, reactive, and persistent strategies. The target Wi-Fi model could mitigate the jamming effect and channel variation using channel hopping and link adaptation. This emulation model enabled the investigation of the jamming impact in dense network conditions.

There were three models in the simulation model: two Wi-Fi models for one AP and one station, and an interferer model for adjacent channel interference (ACI) or co-channel interference (CCI), which is generated using a jamming model and dynamic spectrum congestion model. The impairments that are analyzed include the multipath channel, mismatch between the in-phase and quadrature phase, carrier phase noise, carrier frequency offset, sampling phase noise, sampling frequency offset, signal amplitude variation, and adjacent channel interference variation. The channel models were modeled to have realistic RF/analog and wireless channel impairments. We applied a 50 ns root mean square (RMS) delay spread channel model. The channel model included a RAPP power amplifier with a 10 dB backoff. The phase noise was 104 dBc/Hz at 100 kHz, which was generated using the pole-zero model. The impairment model had a residual frequency error that is caused by oscillators with 8 ppm stability at the legitimate transmitter and receiver. Because the RF PLL and ADC clock use the same oscillator, the timing offset introduced by the ADC was 8 ppm. For simplicity of jamming efficacy comparison, we assumed that the packet size was 1,000 bytes and the packet interval was 16 μs. The SNR and signal-to-interference ratio varied randomly for every packet.

Figure 7 also presents the MAC model, which consists of a TX, RX, error counter, scheduler, power control unit (PCU), and link controller. In order to simulate the proposed scheme in a dynamically varying channel, a link adaptation scheme should be considered. The link adaptation algorithms are grouped into two classes: auto rate fallback (ARF) and SNR-based rate control [22, 31]. The ARF is a statistic-based scheme that has a slow response but simple implementation, whereas the SNR-based rate control is fast and uses the SNR as a good link quality indicator. However, the optimal rate and SNR are not correlated in certain link conditions. In this emulation, the combined scheme of ARF and SNR-based link adaptation was used as the jamming schemes. The link adaptation scheme is operated as an SNR-guided rate adaptation scheme [31] in order to manage the high fluctuations of the SNR, and it adjusts the transmission rate adaptively to the varying channel conditions according to the adaptive ARF. This type of combined rate control is effective in improving the link quality under dynamically interfered varying channel conditions.

Evaluation Results. We developed an emulation environment in order to evaluate the efficiency of the proposed attack strategy and conventional attack strategies in a dense network. The jammer can transmit packets using random jamming, reactive jamming, and persistent jamming strategies. In the emulation model, there are multiple BSSs with 8 access points. Each AP uses 8 different channels in the 5 GHz ISM band. There is one target node, one malicious node, and other legitimate nodes in multiple BSSs. There are up to eight legitimate nodes in the network. The access point transmits 2,000 packets with a 1,000 byte length to the target node. The target node experiences varying channels in terms of SNR and interference levels.

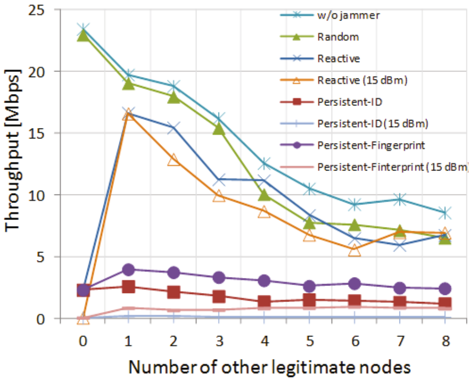

Fig. 8. Jamming efficacy: throughput vs. number of BSSs

Figure 8 presents the degraded throughput for the jamming schemes versus the number of BSSs. Increasing the number of BSSs causes more co-channel and adjacent channel interference in the target device when the jammer is transmitted at a small transmission power (0 dBm). As a result, if there is no malicious jammer, the target node is only affected by interference from other legitimate nodes in multiple BSSs. The random jammer has the worst performance. It is interesting that the reactive jammer is only effective if there are no other nodes, except the target node. However, the persistent jammer significantly degrades the throughput performance of a target node in dense network conditions. If the jammer transmits 15 dB higher jamming power, which is equivalent to 15 dBm transmission power at the output port of the RF amplifier, the measured throughput was close to zero for persistent jamming. This indicates that the effective throughput can be made zero through corrupting every packet being transmitted. In contrast, other jamming schemes were not significantly improved compared with the "w/o jammer" case. The evaluation results demonstrate that persistent jamming can improve the attack efficiency by approximately 80% in dense networks compared with reactive jamming schemes, and it can disconnect the link of the target node with a 20 dBm jamming power and 125 ms response time.

5 Defenses

In this section, we recommend four security defenses against the proposed persistent jamming attacks. In order to protect the ID information in the PHY header, we propose including a non-cryptographic device authentication and dynamic ID allocation mechanism during the standardization process for the next generation of WLANs. In addition, as potential countermeasures against the device fingerprint tracking, we recommend digital predistortion and friendly jamming techniques from an implementation perspective.

5.1 ID Protection

Non-cryptographic Device Authentication. In the current WLAN standards, the signal information in the physical layer header is not protected; thus, the ID in the signal field can be tracked by attackers. A complete solution would be to use a cryptographic mechanism that uses a shared key in the MAC layer in order to achieve authenticity, integrity, and confidentiality. However, the conventional cryptographic mechanisms require key management to distribute, refresh, and revoke the keys. Due to the inefficiency in terms of complexity and overhead, a non-cryptographic scheme in the PHY layer is required for device identification. For example, in a typical indoor wireless channel, the channel response decorrelates rapidly in space [27]. In addition, the channel reciprocity property between a transmitter and receiver can allow legitimate users to use the channel response as a shared key because an attacker, who is located in a different location to the legitimate users, has different channel frequency responses. The legitimate receivers can reliably extract the ID information based on the channel frequency responses of the received frame if the legitimate transmitter sends the ID information encoded using channel frequency responses.

However, the primary drawback of non-cryptographic device authentication using channel reciprocity is that the channel and nodes should be stationary. Thus, it is only applicable to typical indoor environments. Furthermore, from an implementation perspective, in order to fulfill the reciprocity principle at the

RF and analog transceivers that have different circuitry components, both transmission and reception paths should be calibrated for similarity in the transfer functions of the forward and reverse links. In order to achieve link equivalence, calibration schemes using additional circuitries and protocol or signal processing algorithms are required in the system design.

Dynamic ID Allocation. In the cellular network, temporary mobile subscriber identity (TMSI) can be tracked by eavesdroppers on the radio interface. Therefore, the cellular network can change the TMSI regularly in order to avoid the mobile node from being tracked [7]. However, in the latest WLAN standard such as IEEE 802.11ac/af/ah, there have not been considered the security issue of the unprotected frame header during the design of frame structure. The PAID is allocated to a station using an AP when the station associates with the AP, and the PAID is maintained until the station is deassociated. This static ID allocation allows an attacker to reliably snoop and capture the ID information in the wireless channel. However, if the ID is changed periodically based on a synchronized timestamp between the station and AP, it is difficult for the attacker to track the target. From an implementation perspective, dynamic ID allocation is feasible using the time synchronization function (TSF). An 802.11 station maintains a TSF, which is a timer with a modulus 264 counting in microseconds, and it synchronizes their TSF through transmitting and receiving beacons. Each beacon contains the timestamp value of a TSF at the AP, and all stations adjust their TSF considering the propagation and processing delay. As the timestamp value changes over time, if the AP allocates an ID periodically based on the synchronized timer, the stations can update their ID when they receive beacon frames. Furthermore, if the node or group of nodes updates the ID when it switches channels, it is more difficult to track the targets from the previous channel.

The primary drawback of dynamic ID allocation is that an adversary can still intercept the ID information during the same ID period. If the adversary can locate the ID update pattern through tracking the device based on an alternative scheme such as device fingerprints, it can analyze the ID update pattern. In order to reduce the duration of the same ID, the beacon interval should be shortened. However, a reduced beacon interval degrades the network efficiency due to the increased frame overhead and increases the number of wake-ups of power saving stations. Alternatively, in order to reduce the ID update interval, stations must update the ID based on their local timer. In this case, the TSF should be very accurate during a beacon interval because the IDs are determined based on the local timer value at the stations. Even though the dynamic ID allocation scheme is not a complete solution for persistent jamming, it can mitigate the success rate of attacks.

5.2 Fingerprint Protection

Digital Predistortion. The WLAN standards define the tolerance levels for impairments at the receiver. In order to support high data rates and QoS, all digital receivers are required to include compensation circuits for RF/analog and channel impairments. Specifically, WLAN receivers include compensating circuitries such as IQ mismatch correction, DC cancellation, carrier frequency offset correction, symbol synchronization, and sampling time/frequency phase tracking. Thus, if a legitimate transmitter predistorted the transmission signals using a specified amount of offsets for every packet that can be compensated at the legitimate receiver, it is difficult for an attacker to track the device fingerprints because the periodically changed offsets due to the digital predistortion scheme are hidden from others. For example, if the legitimate node randomly changes SNR and timing offset in the range of the tolerance level for every frame, the attacker cannot track the fingerprints due to the randomness while the legimitate receiver can reliably decode the frame.

The primary drawback of digital predistortion against malicious fingerprint detection is that it may degrade a legitimate node that has a residual estimation error and compensation error due to the finite hardware resolution. Therefore, we recommend adaptively using the digital predistortion scheme in frame transmission when the node switches channels due to persistent jamming attacks.

Friendly Jamming. The authors of [25] proposed that friendly jamming could not provide strong confidentiality because data can be extracted from the correlated signals in certain conditions. According to [25], it is only true for simple modulation systems in narrow bandwidths and low radio frequencies. However, because the efficiency of the jamming signal cancellation is inversely proportional to the bandwidth and radio frequencies, it is difficult for an attacker to extract the device fingerprints from friendly jammed signals in WLAN systems that use OFDM modulation in wide bandwidths and high radio frequencies, if the target node transmits friendly jamming signals during the unprotected PHY header transmission. In an implementation viewpoint, WLAN systems which adopt multiple antennas for multiple input multiple output (MIMO) or non-contiguous carrier aggregation techniques can easily support the friendly jamming utilizing the existing hardware resources for transmitting independent spatial streams.

The primary drawback of friendly jamming is that the wireless devices must have extra hardware circuitries in order to generate the jamming signals and, consequently, they consume more energy and cost. This scheme may be only applicable for APs and not for mobile devices because the energy consumption is an important criterion when evaluating portable devices and sensors due to the impact on battery life. In addition, friendly jamming on the frame header field leads to degradation in the signal detection performance at the receiver side of the legitimate node. In order to mitigate this problem, the transmitter may localize the jamming attack [10] and send a friendly jamming signal using a transmit power control or beamforming transmission technique [4].

6 Conclusions

In this paper, we examined the limitations of the existing jamming schemes against channel hopping Wi-Fi devices in dense networks. Even though it is natural for malicious jammers to attempt to identify target nodes in dense networks, it has not been investigated in jamming attack scenarios thus far. Therefore, we proposed and developed a persistent jamming attack to track and jam the target devices based on the PAID and device fingerprints in the frame header. Furthermore, we evaluated the effectiveness of the jamming schemes through empirical experiments and demonstrated that persistent jamming can attack target nodes in dense networks even though they adapt the channel frequency to avoid jamming signals. The evaluation results confirm the superior efficiency of the persistent jamming strategy in a dense network environment in dense network conditions. Finally, we recommended four security remedies to protect the PAID and device fingerprints.

Almost all modern wireless communication systems have the same security limitation in the frame formats which have the unprotected frame header. For low latency and high efficiency, the frame headers are not encrypted in typical wireless systems. Thus, any device can decode the signal information and detect the device fingerprints. However, the frame headers of the modern wireless communication systems include more information for advanced wireless connectivity. If the frame header is not protected, a persistent jammer can track and jam, or an eavesdropper can track and overhear the communication. As future work, this study will be expanded in order to improve the detection success rate of device fingerprints in various channel conditions, and we will implement and evaluate the defense schemes against the persistent jamming attack.

Acknowledgments. This work was supported, in part, by a National Research Foundation (NRF) of Korea grant funded by the Korean government (MEST) under contract numbers 2012R1A2A2A01008244 and 2012-0000979.

References

1. IEEE Standard 802.11h (2003)
2. IEEE Standard 802.11n (2009)
3. Cisco wireless lan controller configuration guide (2010), `http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-0/configuration/guide/c70.html`
4. IEEE P802.11ac, Draft 7.0 (2013)
5. IEEE P802.11af, Draft 4.0 (2013)
6. IEEE P802.11ah, Draft 1.0 (2013)
7. Arapinis, M., Mancini, L.I., Ritter, E., Ryan, M.: Privacy through pseudonymity in mobile telephony systems. In: Network and Distributed System Security Symposium, NDSS (2014)
8. Benslimane, A., Bouhorma, M., et al.: Analysis of jamming effects on IEEE 802.11 wireless networks. In: International Conference on Communications (ICC), pp. 1–5. IEEE (2011)
9. Carious, L.: High-efficiency WLAN. IEEE 802.11-13/033lr5 (2013)
10. Chen, Y., Xu, W., Zhang, Y., Trappe, W.: Securing Emerging Wireless Systems. Springer (2008)
11. Fang, S.H., Hsu, Y.T., Kuo, W.H.: Dynamic fingerprinting combination for improved mobile localization. IEEE Transactions on Wireless Communications 10(12), 4018–4022 (2011)
12. Fang, S.H., Lin, T.N., Lee, K.C.: A novel algorithm for multipath fingerprinting in indoor WLAN environments. IEEE Transactions on Wireless Communications 7(9), 3579–3588 (2008)

13. Gaikwad, R.V., Moorti, R.T.: Apparatus and method for sampling frequency offset estimation and correction in a wireless communication system (2007), US Patent 7,177,374
14. Golmie, N., Rebala, O., Chevrollier, N.: Bluetooth adaptive frequency hopping and scheduling. In: Military Communications Conference (MILCOM), vol. 2, pp. 1138–1142. IEEE (2003)
15. Goth, G.: Next-generation Wi-Fi: As fast as we'll need? IEEE Internet Computing 16(6), 7–9 (2012)
16. Gummadi, R., Wetherall, D., Greenstein, B., Seshan, S.: Understanding and mitigating the impact of RF interference on 802.11 networks. In: Special Interest Group on Data Communication (SIGCOMM), pp. 385–396. ACM (2007)
17. Harjula, I., Pinola, J., Prokkola, J.: Performance of IEEE 802.11 based WLAN devices under various jamming signals. In: Military Communications Conference (MILCOM), pp. 2129–2135. IEEE (2011)
18. Jensen, T.L., Larsen, T.: Robust computation of error vector magnitude for wireless standards. IEEE Transactions on Communications 61(2), 648–657 (2013)
19. Jeung, J., Jeong, S., Lim, J.: Adaptive rapid channel-hopping scheme mitigating smart jammer attacks in secure WLAN. In: Military Communications Conference (MILCOM), pp. 1231–1236. IEEE (2011)
20. Lee, I.G., Choi, E., Lee, S.K., Jeon, T.: High accuracy and low complexity timing offset estimation for MIMO-OFDM receivers. In: Wireless Communications and Networking Conference (WCNC), vol. 3, pp. 1439–1443. IEEE (2006)
21. Mahmoud, H.A., Arslan, H.: Error vector magnitude to SNR conversion for nondata-aided receivers. IEEE Transactions on Wireless Communications 8(5), 2694–2704 (2009)
22. Makhlouf, A., Hamdi, M.: Practical rate adaptation for very high throughput WLANs. IEEE Transactions on Wireless Communications 12(2), 908–916 (2013)
23. Navda, V., Bohra, A., Ganguly, S., Rubenstein, D.: Using channel hopping to increase 802.11 resilience to jamming attacks. In: International Conference on Computer Communications (INFOCOM), pp. 2526–2530. IEEE (2007)
24. Pelechrinis, K., Broustis, I., Krishnamurthy, S.V., Gkantsidis, C.: A measurement-driven anti-jamming system for 802.11 networks. IEEE/ACM Transactions on Networking 19(4), 1208–1222 (2011)
25. Tippenhauer, N.O., Malisa, L., Ranganathan, A., Capkun, S.: On limitations of friendly jamming for confidentiality. In: Symposium on Security and Privacy (SSP), pp. 160–173. IEEE (2013)
26. Wilhelm, M., Martinovic, I., Schmitt, J.B., Lenders, V.: Short paper: Reactive jamming in wireless networks: How realistic is the threat? In: Proceedings on Wireless Network Security (WiSec), pp. 47–52. ACM (2011)
27. Xiao, L., Greenstein, L.J., Mandayam, N.B., Trappe, W.: Using the physical layer for wireless authentication in time-variant channels. IEEE Transactions on Wireless Communications 7(7), 2571–2579 (2008)
28. Xu, W., Trappe, W., Zhang, Y.: Channel surfing: Defending wireless sensor networks from interference. In: Proceedings on Information Processing in Sensor Networks (IPSN), pp. 499–508. ACM (2007)
29. Xu, W., Trappe, W., Zhang, Y., Wood, T.: The feasibility of launching and detecting jamming attacks in wireless networks. In: Proceedings on Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 46–57. ACM (2005)

30. Yang, F., Zhang, X., Zhang, Z.P.: Time-domain preamble-based SNR estimation for OFDM systems in doubly selective channels. In: Military Communications Conference (MILCOM), pp. 1–5. IEEE (2012)
31. Zhang, J., Tan, K., Zhao, J., Wu, H., Zhang, Y.: A practical SNR-guided rate adaptation. In: International Conference on Computer Communications (INFOCOM). IEEE (2008)
32. Zhou, M., Tian, Z., Yu, X., Tang, X., Hong, X.: A two-stage fingerprint filtering approach for Wi-Fi RSS-based location matching. Journal of Computers 8(9) (2013)