Computer Networks 000 (2016) 1–17

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Persistent jamming in wireless local area networks: Attack and defense

Il-Gu Lee[a,b], Myungchul Kim[a,*]

[a] Graduate School of Information Security, KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon, 305-701, Republic of Korea
[b] PHY Research Group, NEWRATEK, 433, 193 Moonji-ro, Yuseong-gu, Daejeon, 305-701, Republic of Korea

ARTICLE INFO

Article history:
Received 28 October 2015
Revised 19 March 2016
Accepted 18 June 2016
Available online xxx

Keywords:
WLAN
Dense network
Persistent jamming
Channel hopping
Device tracking
ID
Fingerprint
Security
Anti-tracking
Anti-jamming

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 WLAN 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. In order to defend against the persistent jamming attack, this paper proposes three defense mechanisms for anti-tracking and anti-jamming; a digital fingerprints predistortion, dynamic ID allocation, and dual channel friendly jamming. The experimental results demonstrate that the proposed defense mechanisms are feasible and effective to significantly decrease the device tracking success ratio of the persistent jamming attack.

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 [1,2] 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 [3,4]. As more and more wireless devices are connected and wireless access points (APs) are densely deployed in the scarce frequency spectrum and 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 [5], the wireless environment may suffer severe interference from unintentional jammers and intentional jammers [6,7].

Recent studies have demonstrated that various proactive jamming methods such as constant, random, and deceptive jamming can be launched easily in wireless networks [8,9]. 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 [10,11]. 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 [8,9]. The reactive jammer, which is the most popularly discussed method for disturb-

* Corresponding author. Fax: +82 42 350 6222.
E-mail address: mck@kaist.ac.kr (M. Kim).

http://dx.doi.org/10.1016/j.comnet.2016.06.024
1389-1286/

ing 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 [8–11]. 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.

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. To the best of our knowledge, there have not been studies for anti-tracking and anti-jamming schemes against the exposed persistent jamming attack. Therefore, in this paper, defense mechanisms are proposed and examined in real testbed and network emulation framework.

Our work provides the following four key contributions.

- This is the first investigation of the limitations of the unprotected physical (PHY) layer 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.
- In order to defend the persistent jamming attack, three anti-persistent jamming mechanisms are proposed; a digital fingerprints predistortion, dynamic ID allocation, and dual channel friendly jamming.
- Persistent jamming attack and defense are experimentally evaluated in a field programmable gate array (FPGA) prototype that was designed and verified for commercialization as an IEEE 802.11n/ac WLAN chipset.
- The proposed attack and defense are 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.

Table 1
Comparison of conventional jamming schemes.

Category	Proactive			Reactive
	Constant	Random	Deceptive	
Complexity	Very simple		Simple	
Jamming effect	Bad		Not bad	Good
Power efficiency	Too bad	Bad		Good
Detection probability	High		Med	Low

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 for the persistent jamming attack. In Section 5, we recommend security mechanisms to defend the persistent jamming attack and demonstrate the feasibility. 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 [7–9,12].

As depicted in Table 1, there are two types of jammers: proactive jammers and reactive jammers. The proactive jammers have three forms: constant, random, and deceptive [8]. 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 implementa-

Please cite this article as: I.-G. Lee, M. Kim, Persistent jamming in wireless local area networks: Attack and defense, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.06.024

Table 2
Conventional channel hopping schemes.

Category	Active type		Passive type	
Subtype	Proactive	Reactive	Firmware	Manual
Hopping method	Predefined hopping sequence	Error statistics	Disconnection	
Applications	Bluetooth, etc.	WLAN, etc.		
Speed	Fast	Slow	Very slow	
Deployment	Not used in WLAN due to inefficiency and complexity	Typical		

tion is relatively complicated. This channel awareness allows for efficient jamming because it must transmit short jamming signals in a timely manner. The authors of [9] 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 [7–9] 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 4, 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 [13–19]. Channel hopping techniques attempt to avoid jammed channels through changing the channel among the orthogonally available channel bands. As described in Table 2, 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 [13,15,16,18]. 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 [20], 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 802.11 h standard defines the dynamic frequency selection (DFS) mechanism in order to avoid interference from radars and other WLAN devices [13]. 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 [17,19,21]. 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 [8] and [10] 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 [15,18,21]. 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. 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 on WLANs

First of all, the security problem of persistent jamming can be described by starting with a parable. Suppose Alice and Bob are communicating with love letters in the cloud. A postman delivers the mail to the destination address (Alice) from source address (Bob) according to the specific commands and information on an envelope via a channel. There are lots of mailmen who are delivering mails in various channels. The mail contents are encrypted in order to prevent a malicious person from reading the message. On the other hand, the mail's envelope is not encrypted, but there are important information such as addresses, identification, affiliation, telephone number, fingerprint, and commands for delivery method. There is a malicious Charlie, Alice's boyfriend, who is a below-average intelligent boy, and another malicious Eve, Bob's girlfriend, who is a smart girl. Charlie attacks all mails in the entire channels, and tries to prevent from delivering or decrypting the mail contents, while Eve attacks specific mails which include Bob or Alice's addresses or their fingerprints included in the unprotected envelope by a tracking and jamming attack approach.

The story of the above love letter is a simple and motivating example of the security limitations of the exposed frame header we will study in this paper. Alice and Bob are the legitimate nodes,

Please cite this article as: I.-G. Lee, M. Kim, Persistent jamming in wireless local area networks: Attack and defense, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.06.024

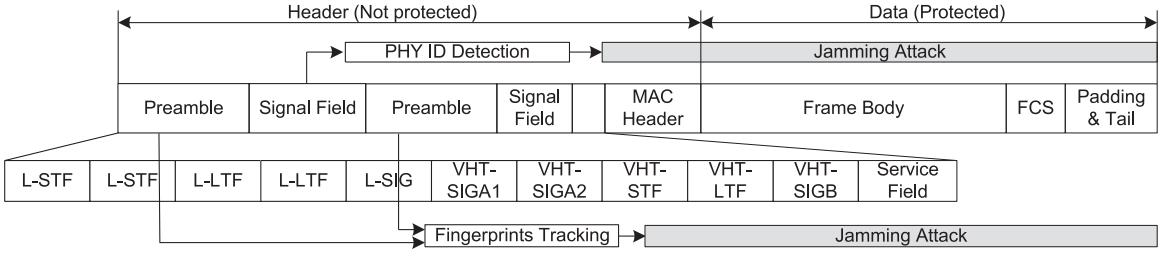

Fig. 1. IEEE 802.11ac WLAN frame structure and persistent jamming attack.

and Charlie and Eve are the malicious nodes. Charlie is a conventional attacker, and Eve is a proposed persistent attacker utilizing frame header vulnerability. Mails and mailmen are messages and channels. The information on the envelope is a frame header which is not a protected part for high efficiency and fast delivery time of messages in typical wireless communications. The mail content is a payload which is encrypted by encryption mechanism and protocol in medium access control (MAC) layer. This story follows the principle of wireless communications in our life. In this story, Charlie may be easily detected by policeman because of his inefficient attacking approach, or he may fail to interrupt them and exhaust himself. In this paper, we will investigate the security limitations of the unprotected frame header in order to enhance the attacking efficiency, and examine the feasibility of launching attacks of jamming attack utilizing the vulnerability. We will demonstrate the feasibility of WLAN attack using persistent jamming with tracking capability in dense networks.

As shown in Fig. 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 WLAN 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 are 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.

Fig. 1 presents the frame structure of the IEEE 802.11ac standard specified in [2]. 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 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 PAID is a 9 bits identifier contained in the VHT-SIG-A. 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 802.11 PHY header 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 PHY layer header is adopted in order to improve the power efficiency for a specific user's device. The PAID information is 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

Please cite this article as: I.-G. Lee, M. Kim, Persistent jamming in wireless local area networks: Attack and defense, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.06.024

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 [22–24]. 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.

Several research demonstrated the feasibility and reliability of physical layer device identification, and malicious use cases of device fingerprinting were introduced [25–27]. However, device fingerprints for persistent jamming attack against channel hopping wireless devices have not been investigated. 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.

Fig. 2 illustrates digital receiving front-end for the OFDM demodulation and the impairment compensation. The digital receiving front-end is equipped with circuits to compensate for signal distortion by an analog element and influence by a varying channel, and includes tracking blocks to compensate for the influence of a clock phase difference between a transmitting block and the receiving block. In the RF receiver, the received radio signal is down mixed and separated to the in-phase and quadrature-phase components. In this down mixing process, any mismatch in the amplitude or phase response of the circuits for the in- and quadrature component generation results in distorted baseband signals. These mismatches are typically manifested as the image generation of the signal itself on the other side of the frequency axis. The unwanted DC signal is generated in various parts of the signal path such as in the mixer and analog to digital converter. Any DC component with a large power not only reduces the precision margin in the digital circuit but also interferes the modulated symbols near DC. In the analog circuit, there are DC cancellers at almost every stage of the signal interface. To reduce the performance degradation, the digital circuit also needs to remove it before any serious signal processing starts. Then, the amplitude and phase mismatches between the in- and quadrature-phase signals are compensated in the I/Q correction block.

The carrier frequency offset should be corrected in the time-domain not to destroy the orthogonality between subcarriers. The demodulation is conducted by using the efficient fast Fourier transform (FFT). The SNR can be estimated after correcting carrier frequency offset using long training sequences. The sampling and carrier phases can be corrected in the frequency domain. To track any carrier phase variation and residual offset, phase tracking is performed after the time-domain correct. The carrier phase variation is contributed from the analog PLL generating the carrier signal. Since the symbol length is relatively long in the OFDM systems, the compensation of the carrier phase noise by using the transmit data is slow, proportional to the symbol length. In the IEEE 802.11-based WLAN systems, the symbol period is 4 μs. This lengthy symbol period limits the phase and frequency tracking capability to those within tens of kilo-Hertz range. The other phase noise outside this band should be lowered by the PLL circuit design technologies. So the tracking loop is needed to compensate this phase accumulation caused by the sampling frequency offset. The same compensation loop can track any significant sampling phase noise. The received signal amplitude may vary due to the power-up time of the transmitter's power amplifier. Any significant temperature change in the radio circuit can also cause the signal amplitude variation. Assuming the amplitude varies rather slow, a tracking loop can be built to compensate this variation. The amplitude variation is tracked in the frequency domain using the demodulated symbols.

3.3.1. 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. In general, the received signal can be expressed as the following equation.

$$r = h \cdot s + n \tag{1}$$

In the equation, r is received signal, s is transmitted signal, h is a channel matrix, and n represents additive white Gaussian noise (AWGN). 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 [28]. 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 measured noise and signal powers, the receiver can calculate the SNR for the received frame. Assuming that P_n, P_r, and P_s

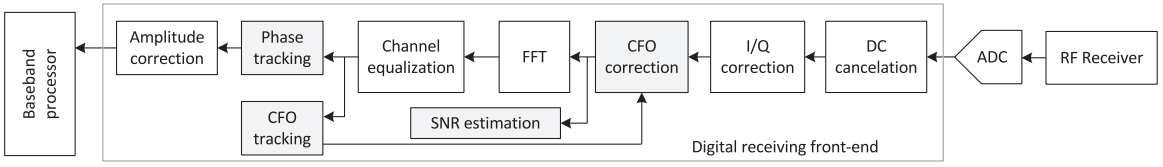

Fig. 2. Digital receiver for SNR estimation and time/frequency offset estimation.

are the noise power, received signal power including noise power, and signal power, respectively, SNR can be estimated as the following equation.

$$P_n = \frac{1}{M}\sum_{m-0}^{M-1}|s(m)+n(m)-s(m+M)-n(m+M)|^2 = 2n^2$$

$$P_r = \frac{1}{M}\sum_{m-0}^{M-1}|s(m)+n(m)+s(m+M)+n(m+M)|^2 = 4s^2+2n^2$$

$$SNR_{est} = \frac{P_s}{P_n} = \frac{P_r - P_n}{P_n} = \frac{2s^2}{n^2} \quad (2)$$

Here, M is 64 samples for 20 MHz bandwidth. In Eq. (2), $s(m)$ and $n(m)$ are the signal and noise for the mth sample of the received frame. If the bandwidth is increased, the receiver can improve the accuracy by frequency diversity gain. Hence, SNR can be calculated as the following Eq. (3).

$$SNR\,[dB] = SNR_{est} - 3\,dB \quad (3)$$

Based on the SNR estimation and packet error ratio, a wireless device can determine channel conditions through measurement-driven decision.

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 [1,2,29]. The EVM is an estimate of the error magnitude of the real signal as compared to the magnitude of the ideal signal. For a given symbol, EVM is calculated as

$$EVM = \sqrt{\frac{\sum_{i=1}^{N}|R(i)-I(i)|^2}{\sum_{i=1}^{N}|I(i)|^2}} \quad (4)$$

In the equation, R is the real signal, I is the ideal signal, N is the number of measured symbols, and i is the measurement index. The SNR typically has a linear relationship with the EVM [30]. 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 and 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.

3.3.2. Frequency/Timing offset estimation

The carrier frequency offset (CFO) and sampling timing offset are resulted 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 frequency/timing offset estimator is derived using the least square rule [31]. 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 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 accuracy of the estimator can be improved through using more subcarriers in multiple symbols.

Since in OFDM systems, multiple modulated signals are transmitted in closely located carriers, even a small carrier frequency offset may destroy the orthogonality between modulated symbols. As in any coherent modulation system, the OFDM receiver needs to track offsets caused by the crystal inaccuracy. The phase rotation in the time domain can compensate the carrier frequency offset completely as long as the estimate of the carrier frequency offset is accurate. The carrier frequency offset can be estimated by measuring the phase rotation between two symbols with some time delay. In the IEEE802.11-based OFDM systems, two preamble structures are supported, short and long preambles. The short preamble consists of 10 repetition of the same symbol whose duration is 0.8 μs. The long preamble has two repeated symbols with the symbol period of 3.2 μs. Since the symbols are repeated, the phase rotation ($=\phi$) between two successive symbols can be estimated without knowing the channel response as given by

$$\varphi = \frac{angle\left(\sum_{k=0}^{M-1} r_k \cdot r_{k-L}^{*}\right)}{L}, \quad (5)$$

In the equation, M is the number of samples used for the estimation and L is the separation length in number of samples between two symbols. The estimated carrier frequency offset is the phase rotation in one sample period. For the short preamble, the L is 16 at the 20 MHz sample and for the long preamble, the L is 64. For the long preamble, whole 64 samples can be used for the estimation. The estimation range of the carrier frequency offset is limited to the phase rotation range caused by the frequency offset in the L separate samples is less than 180 °. If the phase rotation goes beyond the value, the direction of the frequency offset is not distinguishable. Typically, the short preamble with the smaller L than the long preamble is used for coarse estimation and the long preamble for the fine estimation.

The correction of the carrier frequency offset should be done in the time domain to avoid the inter-carrier interference. The correction can be represented as

$$y_k = r_k \cdot e^{-j\cdot\varphi\cdot k} \quad (6)$$

In the equation, r is the received symbol, and y is the compensated symbol. The estimated carrier frequency offset ϕ in Eq. (5) is

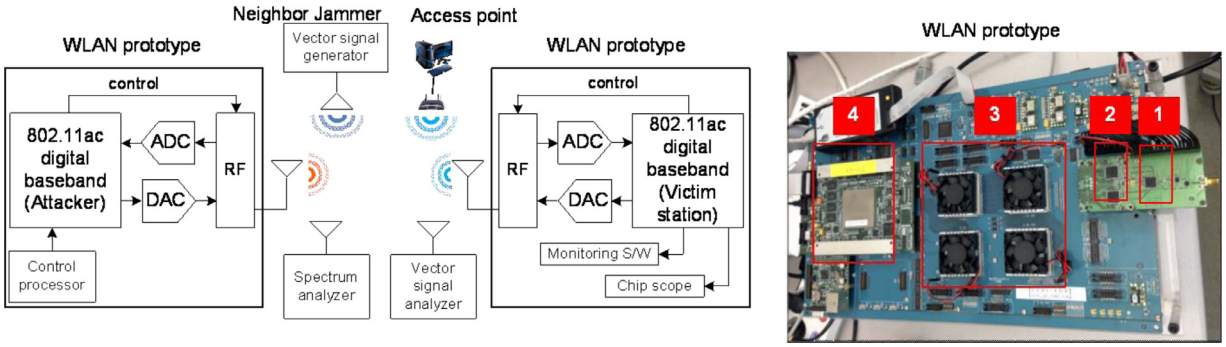

Fig. 3. Experimental set-up for prototype system.

used in the correction of the Eq. (6). As the time index increases, the amount of phase rotation should be increased. In the hardware implementation, a phase accumulator can be used to obtain the phase rotation at a given sample time. 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 [32]. The initial value in the timing offset estimator can be appropriately assigned using the CFO estimation, which is calculated using the preamble in advance.

After compensating the carrier frequency offset using the preamble, there might be a residual offset, and the offset may vary over time due to the temperature change and insufficient supply power. Any causes to make the PLL unstable will contribute to the variation of the carrier frequency. To track down this frequency variation, a carrier frequency tracking loop should be implemented as shown in Fig. 2. The carrier frequency is estimated in the frequency-domain and corrected in the time-domain to avoid the inter-carrier interference. Then, the residual offset is adjusted using the phase offsets of the pilot tones in the data. During the data symbol period, the reliable frequency offset estimate can be obtained with the help of equalized data or pilot signals. Since the channel response is known during the symbol decoding process and the data (or pilot) is known, the phase rotation between two consecutive symbols can be estimated as the frequency variation. The phase tracking result (=ε) can be represented as the following equation.

$$\varepsilon = \sum_{k=0}^{M-1} (r_k \cdot h_k^* \cdot s_k^*)(r_{k-L} \cdot h_{k-L}^* \cdot s_{k-L}^*)^* \tag{7}$$

In the equation, r_k is the received signal in the frequency domain at the subcarrier index k, h_k is the estimated channel response, s_k is the decoded or known transmit symbol, $s*_k$ is the conjugate complex of s_k and M is the number of subcarriers used for the estimation.

4. Implementation and evaluation

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

4.1.1. Experiment setup

As shown in Fig. 3, 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 performance 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 Fig. 3 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, a 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 silicon manufacturing process. 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 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).

4.1.2. Experiment 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. Fig. 4 illustrates the experimental setup for the throughput measurement at the target node when the attacker used different jamming schemes: reactive and persistent jamming. Fig. 4(a) illustrates the configuration of the jammer, neighbor node, target node, and access point, and Fig. 4(b) illustrates the FPGA prototype (jammer) and vector signal generator (neighbor node).

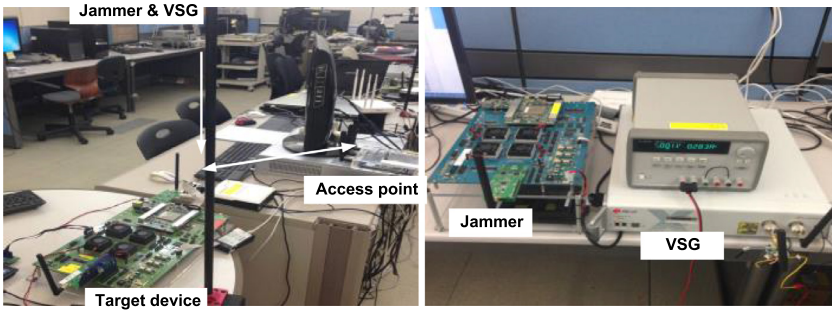

Fig. 4. Experimental set-up: (a) overall test configuration (left), (b) jammer (right).

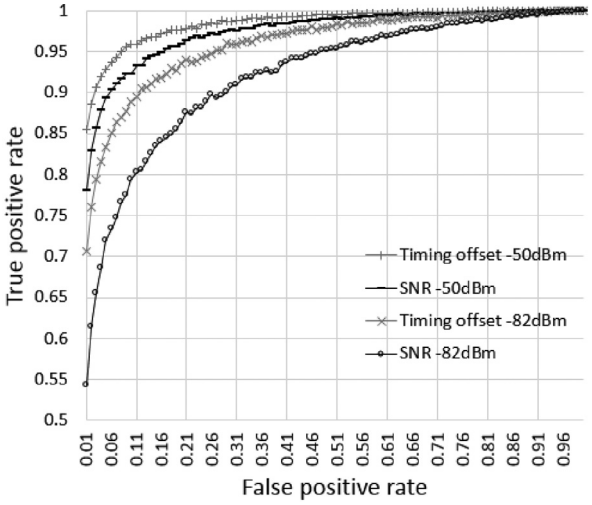

Fig. 5. Wired test: ROC curves of device fingerprints.

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.

Fig. 5 presents the receiver operating characteristic (ROC) curves of the measured fingerprints in the wired tests. When the input power was larger than −50 dBm, the false positive rate was less than 1% for 80% true positive rate. Small incoming signals at the receiver sensitivity level had an accuracy of 3% (Timing offset) and 10% (SNR) false positive rate for 80% true positive rate. In these conditions, the digital baseband could estimate the SNR and timing offset as accurately as 1.6 dB and 1 ppm using preambles in the physical 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.

Fig. 6(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 the transmitted signals had various power levels. 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 Fig. 6(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. 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 Fig. 7(a), the reactive

Please cite this article as: I.-G. Lee, M. Kim, Persistent jamming in wireless local area networks: Attack and defense, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.06.024

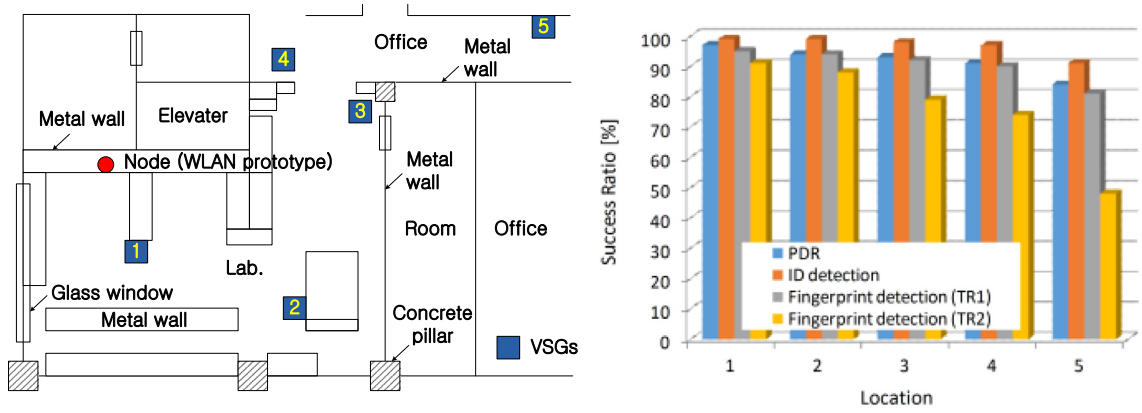

Fig. 6. Wireless test: (a) wireless measurement condition (left), (b) detection success ratio vs. location (right).

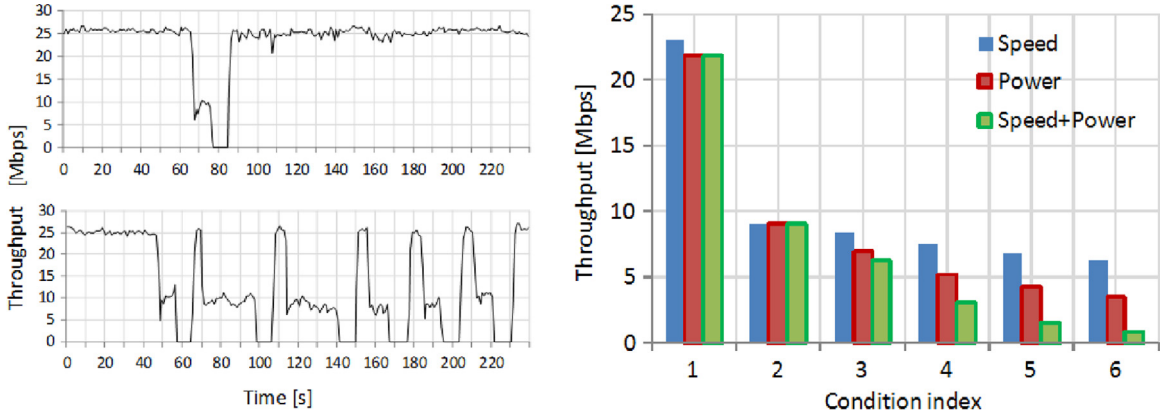

Fig. 7. (a) A throughput measurement at target node for jamming attack reactive jammer (upper), and persistent jammer (lower), and (b) jamming efficacy: throughput vs. speed and power.

Table 3
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		(1,0)	(2,5)	(1,5)
4		(0.5,0)	(2,10)	(0.5,10)
5		(0.25,0)	(2,15)	(0.25,15)
6		(0.125,0)	(2,20)	(0.125,20)

jammer succeeded in its first attack on the target node within approximately 65 s (above) and 45 s (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 3. 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.

Fig. 7(b) presents the effective throughput over the condition index from Table 3, 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, WLAN 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 WLAN 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 when 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.

4.2. Large-scale emulation

4.2.1. Experiment setup

In the developed prototype, it is difficult to evaluate the system in dense network conditions because it is necessary to have

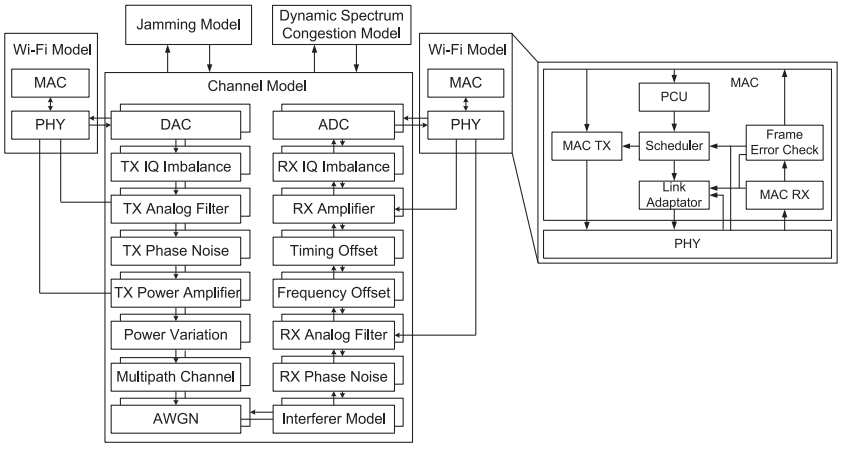

Fig. 8. Emulation environment, channel mode, and MAC model.

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 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.

Fig. 8 presents the emulation model used to analyze the jamming effect in dense network conditions. The emulation model consisted of two WLAN models for the sender and receiver, a channel model, a jammer model, and a dynamic spectrum congestion model. The WLAN 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 WLAN 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 WLAN 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 1000 bytes and the packet interval was 16 μs. The SNR and signal-to-interference ratio varied randomly for every packet.

Fig. 8 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 [17,19]. 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 [19] 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.

4.2.2. 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 2000 packets with a 1000 byte length to the target node. The target node experiences varying channels in terms of SNR and interference levels.

Fig. 9 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

Please cite this article as: I.-G. Lee, M. Kim, Persistent jamming in wireless local area networks: Attack and defense, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.06.024

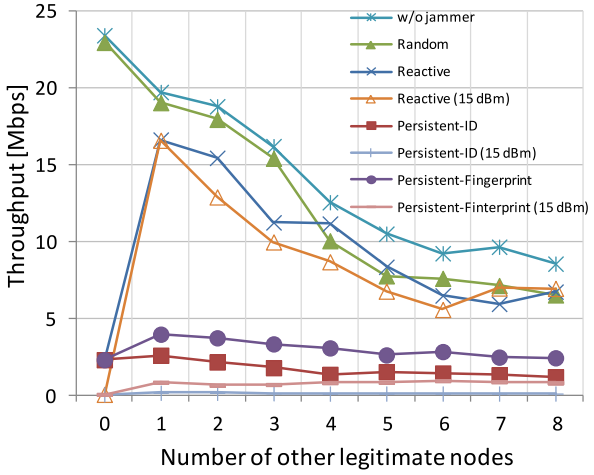

Fig. 9. Jamming efficacy: throughput vs. number of BSSs.

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 against a persistent jamming attack

In this section, we recommend anti-tracking and anti-jamming defenses against the persistent jamming attacks exposed in the previous section. In order to protect the ID information in the PHY header, we propose including a 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. PHY security mechanisms

5.1.1. Fingerprint protection: digital fingerprint 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 predistorts the transmission signals that can be compensated at the legitimate receiver, an attacker cannot track the device fingerprints, and at the same time, the legitimate receiver can successfully receive the signals.

Design of the high throughput WLAN is focused on two important things. One is to provide the maximum data rate and throughput in a near area where a channel is stable and has a high signal-to-noise ratio. The other is to maximally widen a reaching range by minimally reducing a PHY data rate when the signal-to-noise ratio is poor due to long distance. In other words, when channel conditions are fine, a WLAN device can afford to be secured sufficiently by utilizing digital predistortion of fingerprints such as time/frequency offset and signal/noise level at the cost of data rate. When the channel conditions are poor, the reaching range should be secured sufficiently by decreasing the data rate or frame length, and thereby increasing reliability. In the poor channel conditions, digital predistortion is limited to only distort offsets in a tolerance range not to degrade signal quality.

Fig. 10 shows a secure WLAN transceiver which performs digital fingerprint predistortion and impairment correction. In the transmitter, digital baseband generates a data frame. The data is converted to symbols and these symbols modulate the subcarriers of the OFDM system by using the inverse fast Fourier transform (IFFT). The cyclic prefix to mitigate the intersymbol interference is inserted to each OFDM symbol. Then, in the digital fingerprint predistortion circuit, various characteristics such as frequency/timing offset, signal/noise power level, I/Q phase/amplitude ratio, and DC offset can be distorted or compensated to randomize fingerprints. For example, predistorted offset ϕ^i and noise n^i can be added for ith frame. When i is frame index, k is subcarrier index, and x is source signal, the predistorted transmitting signal y is described as the following equation.

$$y_k^i = x_k^i \cdot e^{-j\cdot\varphi^i\cdot k} + n^i \tag{8}$$

The IEEE 802.11 standards require that the transmitters have no more than 20 ppm of frequency offset. Since frequency accuracy is determined by the crystal, it means that the crystal's frequency does not deviate from the required frequency by more than 20 ppm over temperature and time. Thus, the maximum tolerable offset at the receiver should be less than 40 ppm when considering both sides of TX and RX. In this work, in order to protect device fingerprints, the digital transmitting front-end block predistorts frequency/timing offset, signal power, and noise level by a unit of a packet. During the transmission period, the transmitter distorts and sends a data packet as much as a randomly selected offset in the range of the offset tolerance. The offset tolerance can be estimated based on the previously received frames. For example, in the previous frame, the measured offset was 5 ppm, and the offset tolerance is 35 ppm. Accordingly, the receiver can accurately estimate and compensate the offset without performance loss if the sender distorts the offset in the range of the offset tolerance.

In order to distort the signal-to-noise ratio, it is required to know the current link quality and the required link quality. A wireless device can measure and estimate the link quality based on the previously received frame between two communicating nodes. In general, the performance of the state-of-the-art chipset solutions is about 20 dB superior to the standard requirement in terms of transmitter accuracy (6 dB) and receiver sensitivity (14 dB). Furthermore, transmitter can send lower data rate packet and distort signals randomly controlling signal power and noise power in the wider range because the lower data rate mode is more robust to various analog and channel impairment. For example, if the measured link quality is −30 dB EVM and BPSK modulated signal which requires −5 dB EVN, the transmitter can increase noise level or decrease signal power level in the 25 dB range to distort SNR or RSSI.

If a legitimate transmitter predistorted the transmission signals using a specified amount of offsets and SNR for every packet that can be tolerable at the legitimate receiver, it is difficult for an attacker to track the device fingerprints because the periodically changed offsets and signal quality due to the digital predistortion scheme are hidden from others. 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

Please cite this article as: I.-G. Lee, M. Kim, Persistent jamming in wireless local area networks: Attack and defense, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.06.024

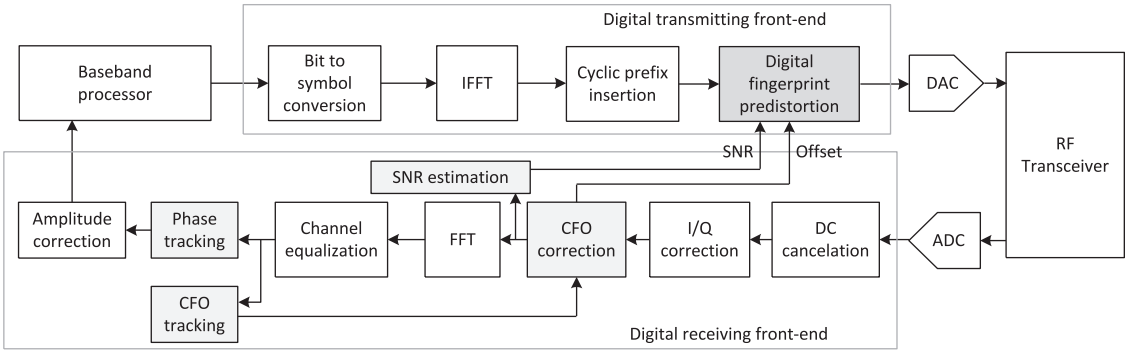

Fig. 10. Secure WLAN transceiver for digital fingerprint predistortion and correction/tracking.

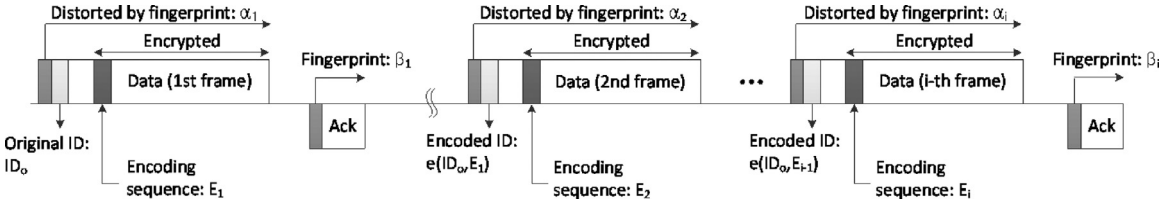

Fig. 11. Digital fingerprint predistortion and dynamic ID allocation.

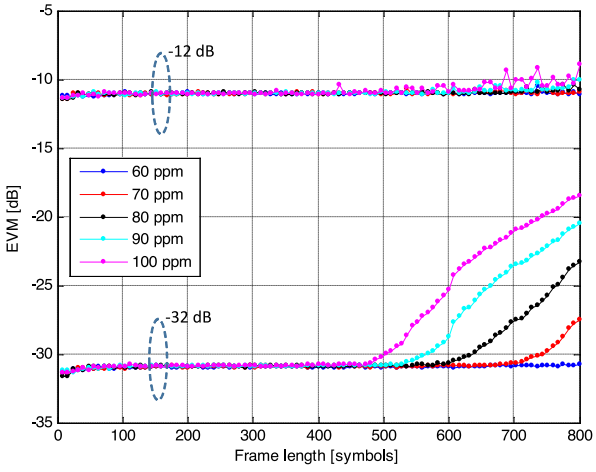

Fig. 12. Frequency offset vs. EVM over frame length.

the randomness while the legitimate receiver can reliably decode the frame. The primary drawback of SNR predistortion against malicious fingerprint detection is that it may degrade a legitimate node that has an insufficient SNR margin in a given link quality and data rate, while timing-offset predistortion does not degrade the performance at the receiver in a tolerable offset range.

5.1.2. ID protection: dynamic ID allocation

One of the most important operations in the handshake of any wireless networks is the proper authentication of the user. 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 [8]. 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. In other words, these channel-based authentication and identification approaches exploit the uniqueness of the connected link channel as an authenticator to distinguish between a legitimate node and an attacker. 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. Several studies have investigated the channel-based authentication method, and demonstrated that rapid decorrelation is feasible in real testbed [8,30,33,34].

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. Therefore, in this paper, as an efficient and practical ID protection method, a dynamic ID allocation mechanism is proposed.

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 [35]. However, in the latest WLAN standard such as IEEE 802.11ac/af/ah, there has 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 disassociated. 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 an encrypted encoding sequence update between the station and AP, it is difficult for the attacker to track the target. Therefore, in this work,

Please cite this article as: I.-G. Lee, M. Kim, Persistent jamming in wireless local area networks: Attack and defense, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.06.024

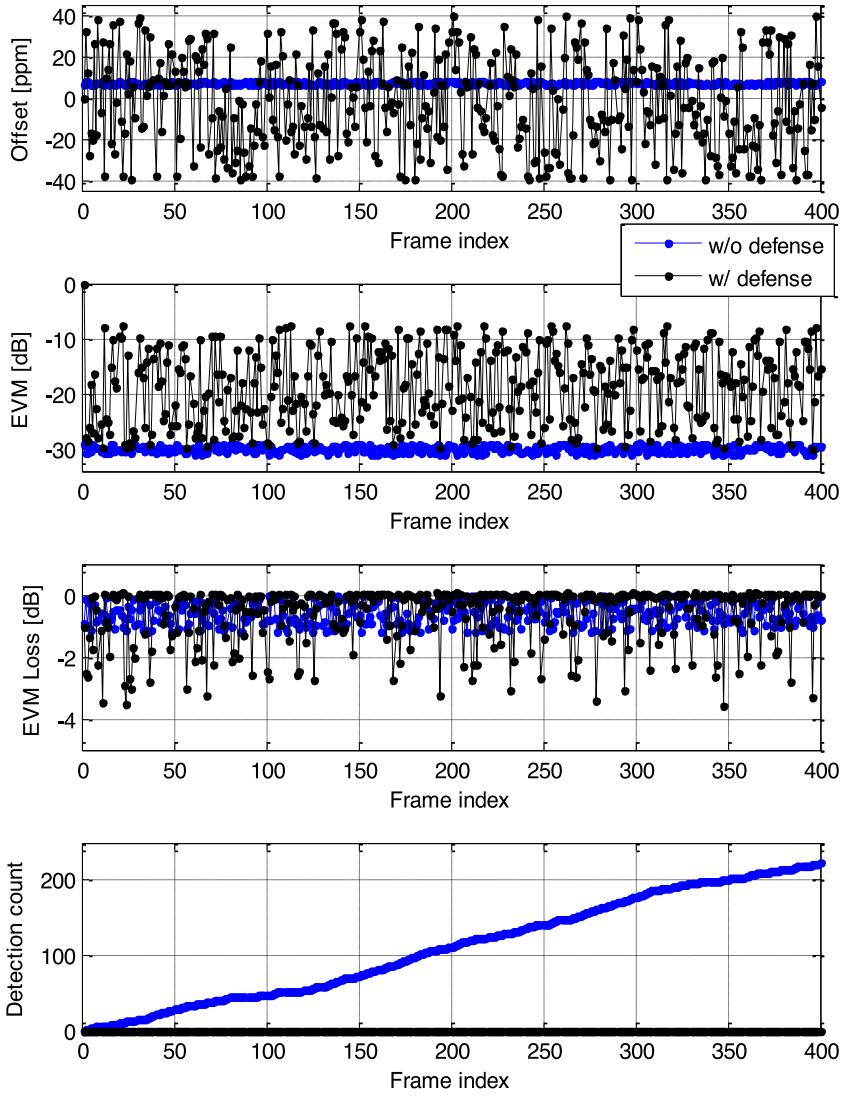

Fig. 13. Digital predistortion and dynamic ID allocation.

a dynamic ID allocation mechanism is proposed to overcome this problem.

From an implementation perspective, dynamic ID allocation is feasible by including an encoding sequence in the encrypted field to protect the PHY ID of the next frame. For example, as shown in Fig. 11, the sender encodes the ID with a random encoding sequence which is successfully delivered in the previous frame, and includes the next encoding sequence in the encrypted field. The encoding function *e(x,y)* can be implemented in various forms. In this paper, the output of the encoding function *e(x,y)* is determined by a bitwise exclusive OR function of *x* and *y*. If the receiver uses the encoding sequence as a key, it can decode the ID. If a frame for PHY security is not delivered due to noise or interference, the communicating nodes keep the previous encoding sequence. 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.

5.1.3. Friendly jamming

The authors of [36] proposed that friendly jamming could not provide strong confidentiality because data can be extracted from the correlated signals in certain conditions. According to [36], 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.

However, the primary drawback of friendly jamming is that the wireless devices must have extra hardware circuits 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.

Therefore, in this paper, a dual channel friendly jamming scheme is proposed. This approach does not require extra hard-

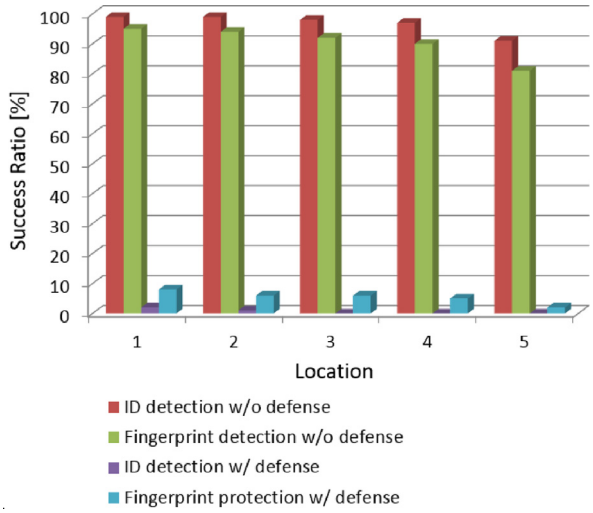

Fig. 14. ID and fingerprints detection success ratio.

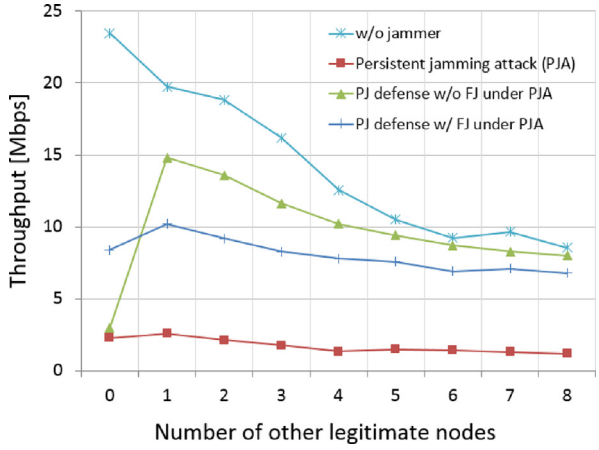

Fig. 15. Defense effectiveness evaluation.

ware resources such as RF, DAC, and baseband transmitter. Instead of concurrent transmission in two different channels using two separate hardwares, the dual channel friendly jamming scheme uses separate frequency channels as a legitimate transmitter and a friendly jammer in a time-division duplexing manner. The legitimate transmission can adopt the proposed digital predistortion and dynamic ID allocation scheme while the friendly jamming signals maintain the same fingerprints. In this case, it makes the persistent jammer track the friendly jammer in the different channel instead of the legitimate node.

5.2. Implementation and evaluation

The proposed defense to successfully protect fingerprints and ID from persistent jammer is evaluated based on the FPGA prototype and network emulation methodology which were used for attack evaluation.

Fig. 12 illustrates the effect of frequency offset for various frame length in the prototype testbed. The EVM has been measured for varying frequency offset over different frame length. The experiment was repeated for 1000 times, then the accumulated values are averaged. The offset correction error should be less than 1% of the subcarrier spacing to have a negligible performance degradation [37] because OFDM is susceptible to frequency offset due to the reduction of amplitude loss of the desired subcarrier and inter-carrier interference caused by neighboring carriers. As a result, the 100 ppm case cannot tolerate more than 550 symbol length frame for a negligible EVM loss of 3 dB, whereas the 60 ppm case can tolerate 800 symbol length frame. Here, the 60 ppm case includes the offset equal to or less than 60 ppm. In the long frame length, the performance was degraded by the inter-carrier interference mainly caused by the frequency offset. The negligible EVM loss is determined by data rate and length of the transmitted frame. For example, the transmitter EVM for 256-QAM modulated signal is required to be a minimum of −32 dB. On the other hand, there are no specifications given for a receiver EVM. Instead, the receiver is specified by the receiver sensitivity for a given data rate. For example, at a certain distance, a receiver might require −28 dB EVM for 256-QAM modulated signal to successfully decode the signals. To have some margin for channel and network variations, the allowed frequency offset might be even lower than the tolerance level. Otherwise, the transmission data rate or length should be reduced to provide more robustness. As shown in the figure, to support a certain EVM for 800 symbol-length frame, say −30 dB, the carrier frequency offset should be 60 ppm or less. If the frame length is 400 symbols, EVM is not degraded even by 100 ppm offset.

Throughput is calculated by dividing the length of a successfully transmitted packet by the time taken to transmit the packet. Therefore, overhead time other than the time that the packet occupies a channel should be reduced to increase the throughput. In order to reduce the communication overhead caused by the interval among preamble, header and random backoff in a MAC layer, a method of using aggregation and a block acknowledgment (ACK) to secure a channel occupying right for a predetermined time is used. The aggregation and block ACK technology can increase the throughput as it can transmit long packets for a channel-access right. However, the aggregation frame transmission also has a problem in that errors propagate due to the long packet length. Large timing offset can greatly affect the packet error ratio because residual offset error propagates and increases error vector magnitude in the long aggregation frame. In a poor SNR channel, residual offset does not degrade the performance for long frames as much as the high SNR channel because low SNR becomes a major noise source.

Fig. 13 clearly shows the advantage of adopting digital fingerprints predistortion and dynamic ID allocation. In this experiment, a −34 dB EVM high quality link was assumed. The ID update period is 10 frames. Digital fingerprints distortion function provides the ranges of 40 ppm offset including the inherent offset and 20 dB SNR. In this experiment, the receiver requires at least -5 dB EVM to decode the BPSK modulated signals successfully. Thus, there is about 3 dB margin. As a result, EVM loss at the receiver was less than 4 dB and packet error ratio was zero. When the digital fingerprints distortion and dynamic ID allocation are used, a persistent jammer could not track the target communicating nodes at all in this condition, and packet error ratio is zero. This indicates that digital fingerprints predistortion and dynamic ID allocation mechanisms are effective to prevent from device tracking and persistent jamming attack.

Fig. 14 shows the ID and fingerprints detection success ratio. The experiment was conducted under the same condition with persistent jammer's ID and fingerprint detection performance evaluation in Fig. 6. If any defense mechanism was not adopted in the system, measurement 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. However, if the proposed defense mechanisms were enabled, detection success ratio was significantly decreased because a persistent jammer could not track the device fingerprints and ID which were changed by digital predistortion and dynamic ID allocation mechanism.

Fig. 15 demonstrates network emulation results for the effectiveness of the proposed defense mechanisms under the persistent

Please cite this article as: I.-G. Lee, M. Kim, Persistent jamming in wireless local area networks: Attack and defense, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.06.024

jamming attack. In this experiment, two defense combination cases are examined; i) 'PJ defense w/o FJ under PJA' case employs digital fingerprints distortion and dynamic ID allocation mechanism without friendly jamming (FJ) under persistent jamming attack (PJA), and ii) 'PJ defense w/ FJ under PJA' case performs digital fingerprints distortion and dynamic ID allocation with the dual channel friendly jamming. If there is at least one legitimate node, the digital predistortion and dynamic ID allocation can mitigate the effect of the persistent jamming attack. On the other hand, if there is no neighboring node, defense performance is poor because persistent jammer does not have another choice. In this case, if the proposed dual channel friendly jamming scheme is adopted, it can reduce the detection success ratio of the persistent jamming attack, but measured throughput is lower than the 'PJ defense w/o FJ' case due to the increased overhead. This indicates that throughput can be improved if an appropriate defense policy is determined by an existence of another active node.

6. Conclusion

In this paper, we examined the limitations of the existing jamming schemes against channel hopping WLAN devices in dense networks. Even though it is natural for malicious jammers to attempt to identify target nodes in dense networks, this 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 effective anti-persistent jamming defense mechanisms to protect the PAID and device fingerprints.

Almost all modern wireless communication systems have the same security limitation in the frame formats which have an 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. Therefore, in this paper, anti-tracking and anti-jamming defense mechanisms are proposed. The prototype experiment and network emulation results show that the proposed defenses are effective in mitigating harmful effects of the persistent jamming attack. As future work, we plan to apply the persistent jamming attack for other wireless networks to test the extendibility of its efficacy and investigate more efficient defense mechanisms against persistent jamming attacks in terms of complexity and defense performance.

Acknowledgments

This work was supported in part by the Korean government (MSIP and IITP) under grant 10044321.

References

[1] IEEE Standard 802.11n, 2009.
[2] IEEE 802.11ac, Draft 7.0, Sep. 2013.
[3] IEEE 802.11af, Draft 4.0, Apr. 2013.
[4] IEEE 802.11ah, Draft 1.0, May. 2013.
[5] Greg Goth, Next-generation wi-fi: as fast as we'll need? IEEE Internet Comput. 16 (6) (2012) 7–9, doi:10.1109/MIC.2012.136.
[6] Laurent Carious, et al., High-efficiency WLAN, IEEE 802.11-13/0331r5 (2013).
[7] Ilkka Harjula, Jarno Pinola, Jarmo Prokkola, Performance of IEEE 802.11 based WLAN devices under various jamming signals, in: Proceedings of the IEEE International Conference on Military Communications (MILCOM), 2011, pp. 2129–2135, doi:10.1109/MILCOM.2011.6127635.
[8] Yingying Chen, Wenyuan Xu, Wade Trappe, Yan Yong Zhang, Securing Emerging Wireless Systems Lower-Layer Approaches, Springer, New York, 2009.
[9] Matthias Wilhelm, Ivan Martinovic, JensB. Schmitt, Vincent Lenders, Reactive jamming in wireless networks: how realistic is the threat? in: Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2011, pp. 47–52, doi:10.1145/1998412.1998422.
[10] Wenyuan Xu, Wade Trappe, Yanyong Zhang, Channel surfing: defending wireless sensor networks from interference, in: ACM/IEEE Proceedings of the International Conference on Information Processing in Sensor Networks (IPSN), 2007, pp. 499–508, doi:10.1145/1236360.1236423.
[11] Wenyuan Xu, Wade Trappe, Yanyong Zhang, Timothy Wood, The feasibility of launching and detecting jamming attacks in wireless networks, in: Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2005, pp. 46–57, doi:10.1145/1062689.1062697.
[12] Abderrahim Benslimane, Abdelouahid El Yakoubi, Mohammed Bouhorma, Analysis of jamming effects on IEEE 802.11 wireless networks, in: Proceedings of the IEEE International Conference on Communications (ICC), 2011, pp. 1–5, doi:10.1109/icc.2011.5962627.
[13] IEEE Standard 802.11 h, 2003.
[14] N. Golmie, O. Rebala, N. Chevrolier, Bluetooth adaptive frequency hopping and scheduling, in: Proceedings of the IEEE International Conference on Military Communications (MILCOM), 2013, pp. 1138–1142, doi:10.1109/MILCOM.2003.1290352.
[15] Ramakrishna Gummadi, David Wetherall, Ben Greenstein, Srinivasan Seshan, Understanding and mitigating the impact of rf interference on 802.11 networks, in: ACM Conference of the Special Interest Group on Data Communication (SIGCOMM), 2007, pp. 385–396, doi:10.1145/1282380.1282424.
[16] Jaemin Jeung, Seungmyeong Jeong, Jaesung Lim, Adaptive rapid channel-hopping scheme mitigating smart jammer attacks in secure WLAN, in: Proceedings of the IEEE International Conference on Military Communications (MILCOM), 2011, pp. 1231–1236, doi:10.1109/MILCOM.2011.6127469.
[17] Arafet Ben Makhlouf, Mounir Hamdi, Practical Rate Adaptation for very high throughput WLANs, IEEE Trans. Wirel. Commun. 2 (2) (2013) 908–916, doi:10.1109/TWC.2013.13.120626.
[18] Vishnu Navda, Aniruddha Bohra, Samrat Ganguly, Dan Rubenstein, Using channel hopping to increase 802.11 resilience to jamming attacks, in: Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), 2007, pp. 2526–2530, doi:10.1109/INFCOM.2007.314.
[19] Jiansong Zhang, Kun Tan, Jun Zhao, Haitao Wu, Yongguang Zhang, A practical SNR-guided rate adaptation, in: Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), 2008, pp. 2083–2091, doi:10.1109/INFOCOM.2008.274.
[20] Cisco, Wireless LAN Controller Configuration Guide, http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-0/configuration/guide/c70.html (accessed 16.03.16).
[21] Konstantinos Pelechrinis, Ioannis Broustis, SkikanthV. Krishnamurthy, Christos Gkantsidis, A measurement-driven anti-jamming system for 802.11 networks, IEEE/ACM Trans. Netw. 19 (4) (2011) 1208–1222, doi:10.1109/TNET.2011.2106139.
[22] Shih-Hau Fang, Ying-Tso Hsu, Wen-Hsing Kuo, Dynamic fingerprinting combination for improved mobile localization, IEEE Trans. Wirel. Commun. 10 (12) (2011) 4018–4022, doi:10.1109/TWC.2011.101211.101957.
[23] Shih-Hau Fang, Tsung-Nan Lin, Kun-Chou Lee, A novel algorithm for multipath fingerprinting in indoor WLAN environments, IEEE Trans. Wirel. Commun. 7 (9) (2008) 3579–3588, doi:10.1109/TWC.2008.070373.
[24] Mu Zhou, Zengshan Tian, Xiang Yu, Xiaomou Tang, Xia Hong, A two-stage fingerprint filtering approach for wi-fi rss-based location matching, J. Comput. 9 (8) (2013) 2374–2381, doi:10.4304/jcp.8.9.2374-2381.
[25] Chrisil Arackaparambil, Sergey Bratus, Anna Shubina, David Kotz, On the reliability of wireless fingerprinting using clock skews, in: Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2010, pp. 169–174, doi:10.1145/1741866.1741894.
[26] Boris Danev, Srdjan Capkun, Transient-based identification of wireless sensor nodes, in: ACM/IEEE Proceedings of the International Conference on Information Processing in Sensor Networks (IPSN), 2009, pp. 25–36, doi:10.1145/1602165.1602170.
[27] Boris Danev, Davide Zanetti, Srdjan Capkun, On Physical-layer Identification of Wireless Devices, ACM Comput. Surv. 45 (1) (2012), doi:10.1145/2379776.2379782.
[28] Fan Yang, Xi Zhang, Zhong-pei Zhang, Time-domain preamble-based SNR estimation for OFDM systems in doubly selective channels, in: Proceedings of the IEEE International Conference on Military Communications (MILCOM), 2012, pp. 1–5, doi:10.1109/MILCOM.2012.6415690.
[29] T.L. Jensen, T. Larsen, Robust computation of error vector magnitude for wireless standards, IEEE Trans. Commun. 61 (2) (2013) 648–657, doi:10.1109/TCOMM.2012.022513.120093.
[30] H.A. Mahmoud, H. Arslan, Error vector magnitude to SNR conversion for nondata-aided receivers, IEEE Trans. Wirel. Commun. 8 (5) (2009) 1536–1576, doi:10.1109/TWC.2009.080862.

Please cite this article as: I.-G. Lee, M. Kim, Persistent jamming in wireless local area networks: Attack and defense, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.06.024

[31] Il-Gu Lee, Eunyoung Choi, Sok-kyu Lee, Taehyun Jeon, High accuracy and low complexity timing offset estimation for MIMO-OFDM receivers, in: Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), 2016, pp. 1439–1443, doi:10.1109/WCNC.2006.1696498.
[32] R.V. Gaikwad, R.T. Moorti, Apparatus and method for sampling frequency offset estimation and correction in a wireless communication system, US Patent 7,177,374, 2007, pp. 1–15.
[33] Xianru Du, Dan Shan, Kai Zeng, L. Huie, Physical layer challenge-response authentication in wireless networks with relay, in: Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), 2014, pp. 1276–1284, doi:10.1109/INFOCOM.2014.6848060.
[34] Liang Xiao, L.J. Greenstein, NaryanB. Mandayam, W. Trappe, Using the physical layer for wireless authentication in time-variant channels, IEEE Trans. Wirel. Commun. 7 (7) (2008) 2571–2579, doi:10.1109/TWC.2008.070194.
[35] M. Arapinis, L.I. Mancini, E. Ritter, M. Ryan, Privacy through pseudonymity in mobile telephony systems, in: Proceedings of the Network and Distributed System Security Symposium (NDSS), 2014, doi:10.14722/ndss.2014.23082.
[36] N.O. Tippenhauer, L. Malisa, A. Ranganathan, S. Capkun, On limitations of friendly jamming for confidentiality, in: Proceedings of the IEEE Symposium on Security and Privacy, 2013, pp. 160–173, doi:10.1109/SP.2013.21.
[37] Richard van Nee, Ramjee Prasad, OFDM Wireless Multimedia Communication, Artech House Publishers, 2000.

Please cite this article as: I.-G. Lee, M. Kim, Persistent jamming in wireless local area networks: Attack and defense, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.06.024

Il-Gu Lee received his B.S. degree in electrical engineering from Sogang University, Seoul, Korea, in 2003, and his M.S. degree in the Department of Information and Communications Engineering from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, in 2005. And he received his Ph.D. in the Graduate School of Information Security in Computer Science & Engineering Department from KAIST in 2016. He has been with the Electronics and Telecommunications Research Institute (ETRI) as a senior researcher from 2005 to 2013, and has been working as a principal architect and project leader for NEWRATEK (KR) and NEWRACOM (US) since 2014. His current research interests are in the area of wireless/mobile networks with an emphasis on digital signal processing, algorithms and protocols, and security. He has authored/coauthored more than 30 technical papers in the areas of wireless networks and communications, and holds about 80 patents. He is also an active participant of and contributor to the IEEE 802.11 WLAN standardization committee.

Myungchul Kim received his B.A. in Electronics Engineering from Ajou University in 1982, M.S. in Computer Science from the Korea Advanced Institute of Science and Technology (KAIST) in 1984, and Ph.D. in Computer Science from the University of British Columbia, Vancouver, Canada, in 1993. Currently, he is with the faculty of KAIST as a Professor. Before joining the university, he was a managing director in Korea Telecom Research and Development Group from 1984–1997 where he was in charge of research and development of protocol and QoS testing on ATM/B-ISDN, IN, PCS, and Internet. He has also served as a member of Program Committees for many conferences including IWTCS, IEEE ICDCS, and IFIP FORTE, and was co-chair of the IWTCS'97 and the FORTE'01. He has published over 100 conference proceedings, book chapters, and journal articles in the areas of computer networks, wireless mobile networks, protocol engineering, and network security.

Please cite this article as: I.-G. Lee, M. Kim, Persistent jamming in wireless local area networks: Attack and defense, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.06.024