Preamble Injection and Spoofing Attacks in Wi-Fi Networks

Zhengguang Zhang and Marwan Krunz
Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ
Email: {zhengguangzhang, krunz}@email.arizona.edu

***Abstract*—In Wi-Fi networks, every frame begins with a preamble that is used to support frame detection, synchronization, and channel estimation. The preamble also establishes compatibility and interoperability among devices that operate different Wi-Fi versions (e.g., IEEE 802.11a/g/n/ac/ax). Despite the crucial functions of the preamble, no guarantees can be made on its authenticity or confidentiality. Only weak integrity protection is currently possible. In this paper, we introduce novel Preamble Injection and Spoofing (PrInS) attacks that exploit the vulnerabilities of the preamble. Specifically, an adversary can inject forged preambles without any payload for the purpose of disrupting legitimate receptions or forcing legitimate users to defer their transmissions. The proposed PrInS attacks are effective irrespective of the Wi-Fi versions used by the adversary and its targets, as the attacks take advantage of the physical (PHY) layer receive state machine and/or capture effect. The efficacy of our attacks are validated experimentally using software-defined radios (SDRs). Our results show that the adversary can almost silence the channel, bringing the throughput of a legitimate user to 2% of its normal throughput. Even at 30 dB less power, the adversary still causes an 87% reduction in the legitimate users' throughput. To mitigate the PrInS attacks, we propose a backward-compatible scheme for preamble authentication.**

***Index Terms*—Wi-Fi networks, injection and spoofing attack, denial-of-service, physical-layer security.**

I. Introduction

Over the past few years, Wi-Fi experienced unprecedented growth, with almost 18.2 billion Wi-Fi devices reported in 2020 worldwide [1]. Many of these devices are deployed for the Internet of Things (IoT) and Machine to Machine (M2M) communications. Such ubiquitous deployment raises security concerns about Wi-Fi networks. Recently, some medium access control (MAC) layer attacks, such as MAC address spoofing [2], downgrade and dictionary attacks against WPA3 [3], and beacon announcement forgery [4], were identified. At the same time, problematic PHY-layer vulnerabilities that lead to privacy leakage [5] and jamming [6] were highlighted. In response to the growing security concerns, various techniques were proposed to enhance Wi-Fi security, including beacon protection [7], friendly jamming [8], and PHY encryption [9]. Most of these techniques mainly focus on the PHY frame payload (i.e., MAC frames), with little attention given to the protection of the PHY frame preamble.

This research was supported in part by NSF (grants CNS-1563655, CNS-1731164, and IIP-1822071) and by the Broadband Wireless Access & Applications Center (BWAC). Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of NSF.

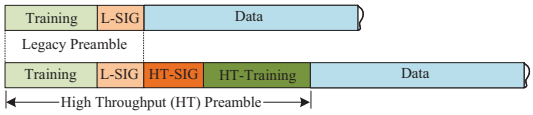


Fig. 1. Simplified legacy and HT PHY frame format of Wi-Fi.

Fundamentally, the vulnerability of the frame preamble is related to the fact that it is publicly known and decodable by every Wi-Fi device. The preamble is composed of Training and Signal (SIG) fields (see Fig. 1). It primarily helps the receiver with the reception and interpretation of data. It also indicates the frame duration, which is needed to reserve the channel. Specifically, Wi-Fi devices use carrier-sense multiple access with collision avoidance (CSMA/CA) to defer channel access for the frame duration of an overheard Wi-Fi transmission. Thus, any attack on the preamble has far-reaching implications on the Wi-Fi network performance. The attack identified in [10] disrupts the frame timing by jamming the Training field with continuous noise or false Training symbols. The jamming signal against the Training field in [11] was carefully designed to spoof the receiver into incorrect frequency offset estimation, hence corrupting the data. However, because the Training fields arrive in the first few microseconds of a frame, it is practically challenging to jam them reactively. So these approaches have to compromise either energy efficiency through continuous jamming or jamming efficacy via reactive jamming with inaccurate timing. Moreover, the impact of the attack in [11] is limited to only a pair of users because the optimal jamming signal is designed with prior knowledge of the channel state information. While prior works aim at undermining the functions of the preamble, we are more concerned about the attack that exploits the functions of the preamble, especially as more system-level information is conveyed in the SIG fields.

In this paper, we shed light on some practical attacks on Wi-Fi preambles. These attacks exploit the vulnerabilities of the preamble, along with PHY-layer receive state machine and capture effect. Specifically, we present Preamble Injection and Spoofing (PrInS) attacks, by which the adversary injects a preamble with forged SIG fields to spoof other devices in the vicinity of the adversary into deferring channel access or incorrectly receiving packets. Considering three injection timing scenarios, we further discuss different PrInS attacks that silence the channel, mislead frame detection, alter received data, and drain user power. Remarkably, there is no strict

timing restriction on such attacks. For example, we demonstrate an attack where an adversary randomly injects forged 802.11ac preambles into an 802.11a network. The attacker spoofs all targets within its communication range, forcing them to defer channel access until the expiration of the announced frame duration (because 802.11a devices can only process the legacy preamble of an 802.11ac frame). Launching this attack efficiently silences the channel and lowers the network throughput. Compared to injecting malicious MAC frames and jamming, PrInS attacks are more efficient in the sense that they require lower power and a shorter attack duration. Furthermore, as PHY attacks, there is no need to manipulate a valid frame with a legitimate MAC address and encryption. Instead, any signal generator or SDR can launch the attacks by manipulating or capture-and-replaying a preamble.

The main contributions of this paper are as follows:

- We investigate the inherent security vulnerability of Wi-Fi to PrInS attacks due to unsecure preamble, receive state machine exploitation, and capture effect;
- We present a comprehensive study of different threat models together with their impacts, targeting one or more devices regardless of their underlying protocols;
- We conduct extensive experiments using SDRs to demonstrate the efficacy and efficiency of the proposed attacks;
- We propose to customize and randomize the frame preamble in a backward-compatible way such that we can authenticate the preamble to mitigate PrInS attacks.

II. Preliminaries

A. PHY Frame Preamble

As shown in Fig. 1, an OFDM-based Wi-Fi frame starts with a legacy (802.11a) preamble that has two components: Training and legacy SIG (L-SIG) fields. The former is a fixed waveform used for frame detection, synchronization, and channel estimation. The latter is mainly used to signal frame-specific properties for two purposes. First, it allocates time for transmission on the channel. Second, it indicates the frame format and any information needed for frame decoding (e.g., rate and length). At the same time, the information in the preamble is used by neighboring devices to defer transmission and automatically filter unintended frames.

To maintain compatibility with earlier Wi-Fi standards and ensure interoperability, the frame preamble is extended to include extra Training and SIG fields. For example, in a high throughput (HT) 802.11n preamble, in addition to the legacy preamble, HT-training and HT-SIG are introduced. The HT-SIG conveys the bandwidth, the modulation and coding schemes (MCS), and other necessary information for HT operation. Generally, the duration, content, and modulation of non-legacy SIG fields vary depending on the PHY frame format. So SIG fields are also used for frame format detection.

B. PHY Carrier Sense and Receive Procedure

Wi-Fi relies on carrier sensing (CS) to avoid collisions. It involves PHY CS via energy detection (ED) and preamble detection (PD), and virtual CS using the network allocation vector. In this paper, we only consider PHY CS as it is related to the proposed attacks. ED detects any ongoing transmission (Wi-Fi or non-Wi-Fi) over the channel by setting a power threshold (e.g., -62 dBm), whereas PD detects a Wi-Fi frame preamble using a lower threshold (e.g., -82 dBm). The PHY CS is used for clear channel assessment (CCA), called CS/CCA mechanism.

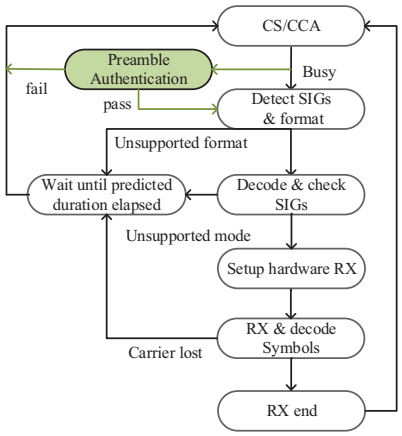


Fig. 2. PHY receive state machine with proposed preamble authentication (shaded part that detects forged preamble and avoids unnecessary wait).

A typical abstracted state machine for the PHY receive (RX) procedure [12, Fig. 21-37] is represented by the unshaded part of Fig. 2. Upon sensing a busy channel through the CS/CCA mechanism, the receiver first detects the SIG fields and determines the frame format. If the frame format is one of the supported formats, the receiver proceeds to decode and check the content of the SIG fields. In this step, the SIG fields are also validated through even parity and cyclic redundancy check (CRC). If the SIG fields are valid and all the announced operation modes are supported, the receiver proceeds to set up the hardware accordingly to receive and decode data symbols. The receive time depends on the frame duration, which can be predicted from the Length field in the L-SIG. If no error is encountered, the receiver will switch back to CS/CCA once reception ends. However, there are some anomalies where the receiver has to prematurely terminate the reception and wait until the predicted frame duration has elapsed before returning to CS/CCA. Three typical errors that lead to this behavior are: an unsupported format or operation mode, and lost carrier.

III. Potential Preamble Vulnerabilities

A. Weak Protection

Despite its importance, the preamble of a Wi-Fi frame is weakly protected, which may compromise the security of the communication. Aside from weak integrity protection (even parity and CRC) for SIG fields, no guarantees can be made on the authenticity or confidentiality of the preamble. As a result, an adversarial device can deceive its neighbors by sending a forged preamble of valid integrity. To make matters worse, the deterministic Training fields and the predictable SIG fields of the preamble are relatively easy to forge. The above weaknesses make the preamble susceptible

to eavesdropping and spoofing. The prior knowledge from eavesdropping usually amplifies the consequences of spoofing. For example, the adversary first eavesdrops on the Rate bits in a previous frame and then injects a forged preamble that signals a lower/higher Rate to spoof the receiver. Thus, the receiver ends up wasting energy on decoding the payload incorrectly. Moreover, injecting a forged preamble for a multi-user transmission is devastating that impacts multiple links simultaneously.

B. Nonuniform Format and Operation Mode

Beyond the Wi-Fi version, the preamble format also varies according to the numbers of antennas and users [12]. The preamble format helps the receiver to detect the PHY frame format. It is done by checking the duration and modulation schemes of received SIG fields in the preamble, as well as the Length field in the L-SIG [13, Fig. 27-63]. Moreover, even if two frames are of the same format (say, 802.11ac), their operation modes indicated in SIG fields differ if they adopt different optional features. In particullar, multiple-input-multiple-output (MIMO) and space–time block code (STBC) are not supported by all 802.11n/ac devices. The problem arises when a legacy 802.11a/g device could not recognize the advanced 802.11n/ac/ax preamble format, or a device detects an unsupported operation mode in a frame of supported format. As shown in Fig. 2, the device will terminate the reception immediately, but wait for the predicted frame duration before a new CS/CCA. An adversary may exploit this to silence the channel by sending preambles with unsupported formats or operation modes.

C. Capture Effect

Following the standard RX state machine, a receiver shall not try to receive another preamble during the reception of the current preamble. Yet, the implementation of most Wi-Fi chipsets breaks the standard due to the capture effect. Specifically, it occurs in a collision where the second preamble arrives in the middle of the first preamble's reception. If the second preamble is not sufficiently strong, the detected energy increment is negligible to the receiver. Thus, the receiver will treat it as interference and stay in the RX state of the first preamble. If the energy level increases significantly upon the arrival of the second preamble, the receiver quits the ongoing reception of the first preamble, and initiates the reception procedure (synchronization, demodulation, decoding, etc.) for the second preamble. Since frame preamble is critical for frame detection and synchronization, it is more vulnerable to capture effect than the payload. Indeed, experimental studies [2], [14] have validated this on Intel, Qualcomm, and Broadcom chipsets. Such design helps a device in dense deployment receiving expected frames despite the interference from alien low-power frames. However, it also opens the door for spoofing attacks.

IV. PrInS Attacks

Having examined the vulnerabilities of the Wi-Fi frame preamble, we present PrInS attacks with three threat models.

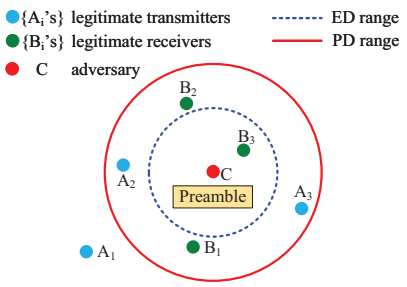


Fig. 3. A Wi-Fi network with an adversary.

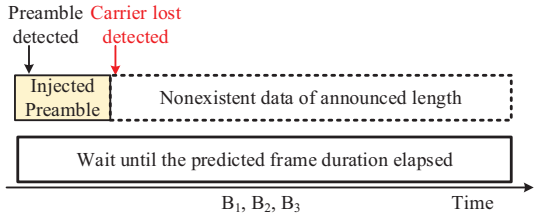
Launching these attacks can silence the channel, mislead frame detection, alter received data, and drain user power. Then, we show that even if the injected preamble is in an unsupported format or operation mode, it still silences the channel.

Assuming a Wi-Fi network shown in Fig. 3, there are multiple legitimate transmitter-receiver pairs (A_i, B_i). The adversary C also locates in the network who injects preambles without payload data to the network. The red solid and blue dashed circles represent the ranges within which the nodes can detect the signal from the adversary by PD and ED, respectively. Namely, all the nodes within the PD range can detect the injected preamble unless being severely interfered with or in the TX state. In the following, we will consider the timing and power of the preamble injection to illustrate three detailed threat models.

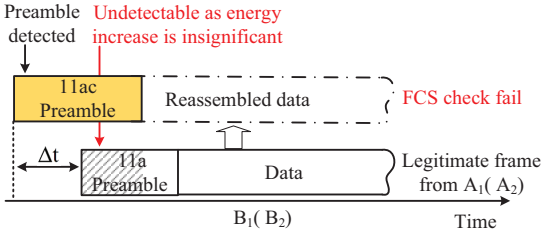
A. Channel Silencing Attack

Fig. 4(a) depicts the scenario when a forged preamble is injected that does not collide with any legitimate frames. The dashed rectangle indicates nonexistent data of the length announced by the injected preamble. In this case, all the legitimate users except A_1 (out of PD range) can detect the injected preamble. Because of the backward compatibility, they can decode the legacy portion of the preamble correctly and predict the frame duration from the Length field in the L-SIG. However, no matter what frame format and operation mode they detect during the reception, the carrier lost will be detected ultimately. Following the RX state machine, they will wait for the frame to finish the nonexistent transmission. As such, an injected preamble that could be as short as $20\,\mu$s reserves the channel for at most 5.383 ms, which is the maximum duration of a PHY frame. In a nutshell, the preamble injection without collision maliciously silences the channel by deferring the channel access of victim users.

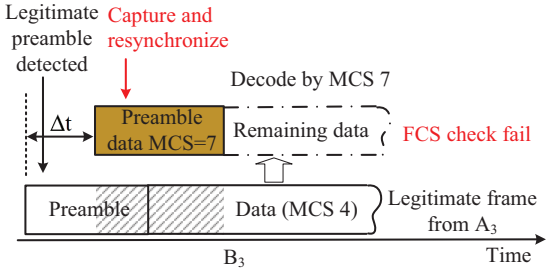
The adversary can further prolong the channel silence time by indicating a longer frame duration with the lowest rate and largest length of data. Even worse, if the announced bandwidth is wide, multiple Wi-Fi channels would be silenced, decreasing the network throughput significantly. It is worth noting that an injected preamble with low power can still succeed as long as the power level is above the PD threshold at the targets. That is the main advantage of the channel silencing attack over typical PHY-layer jamming attacks. Additionally, such an attack does not require accurate timing. Instead, the preamble only needs to be injected without collisions. Indeed, given that one MAC



(a) Channel silencing attack when the injected preamble does not collide with any legitimate frame.



(b) Frame detection attack when the injected preamble arrives first and collides with the legitimate frame.



(c) Data alteration attack when the injected preamble arrives last and collides with the legitimate frame.

Fig. 4. Threat models and PrInS attacks with different timing and power (the darker color the injected preamble, the higher power) .

slot is 9 μs, obtaining 3 slots is fairly easy and sufficient for the adversary to launch the attack.

B. Frame Detection Attack

In the preceding section, we just considered the simple collision-free PrInS attack. Now, we focus on the threat raised by the collision of the injected preamble and a legitimate frame. Since frame detection is one of the primary functions of the preamble, we investigate related threats in this section. Beyond those jamming attacks targeting the preamble to disrupt frame detection, we go further to mislead the frame detection by frame format spoofing.

In Fig. 4(b), the forged 802.11ac preamble is injected and arrives at B_1 (B_2) first, yet a legitimate 802.11a frame arrives at B_1 (B_2) before the end of the injected preamble. Denote the preamble arrival time offset as Δt. This happens if the legitimate transmitter senses an idle channel by mistake in the following two possible scenarios: 1) for B_1, the legitimate transmitter A_1 could not sense the ongoing preamble injection as it is outside the PD range of C; 2) for B_2, the legitimate transmitter A_2 was busy in RX state and missed the PD phase, while the power of the injected preamble is below ED threshold. Here, we assume that B_1 and B_2 support 802.11ac protocol and are backward-compatible to 802.11a. Since the victim receivers (i.e., B_1, B_2) are already in RX state to receive and decode the forged preamble, the legitimate preamble is undetectable if the energy increase is insignificant to reach the capture effect threshold. Because the injected preamble uses robust MCS (BPSK with $1/2$ rate convolution coding), the interference from the legitimate frame would not impact its decoding. However, B_1 (B_2) would mistakenly reassemble the non-overlapping portion of the legitimate frame as payload data for the forged preamble and decode it as 802.11ac frame. In the end, the frame check sequence (FCS) could not pass.

Above all, the legitimate 802.11a frame is detected as a rogue 802.11ac frame with the wrong timing. As opposed to the channel silencing attack where the victims do not bother receiving the data, the energy consumption of the victims for receiving and decoding under the frame detection attack is considerable, which may cause battery depletion.

C. Data Alteration Attack

Fig. 4(c) shows the other collision case, where the injected preamble arrives at B_3 during the reception of the legitimate frame from A_3. There is still a chance for the adversary to succeed because of the capture effect. More specifically, B_3 senses a significant energy increase if the injected preamble overpowers the legitimate one. Then, B_3 switches to synchronize with the injected preamble and decode it. Similar to the frame detection attack, part of the weaker legitimate frame interferes with the strong forged preamble. Once the forged preamble is decoded successfully, B_3 sets up the hardware according to the SIG fields of the injected preamble. And the remaining portion of the legitimate data is received and decoded with incorrect parameters. Hence, the forged preamble manages to spoof B_3 into receiving data with rogue signaling information. Common approaches to achieve this could be injecting a forged preamble with an incorrect MCS or channel coding scheme. For example, B_3 decodes the data with MCS 7 announced by the adversary, while the actual MCS is 4 for the legitimate frame.

Through such attacks, the received data is altered that could not pass the FCS check, which in turn, leads to high packet loss. More threateningly, because demodulation and decoding are energy-consuming, such attacks also cause battery depletion, which is a critical issue for energy-limited IoT devices.

So far, we only assume the injected preamble is decodable. What if the injected preamble is in an unsupported format or operation mode? For instance, the adversary injects an 11ac preamble into a network consisting of devices that are only 802.11a-capable. According to the backward-compatible protocol design, a legacy (802.11a) preamble is always prepended to the dedicated preamble fields for an 802.11n/ac/ax frame. Therefore, a legacy device can still detect and decode the legacy portion of the injected 802.11ac preamble. Nevertheless, it could not decode the subsequent portion of the preamble. Then, it reports an unsupported frame format, but it would not directly switch to CS/CCA state. Instead, it presumes an ongoing Wi-Fi transmission, which is supposed

to end by the time derived from the Length field in the L-SIG. So, it has to wait until the end of this duration. As a result, the targeted channel would be silenced that all the devices within the vicinity of the adversary could not transmit. In the case of unsupported operation mode, taking 802.11ac as an example, the adversary injects an 802.11ac preamble indicating STBC operation, while the target devices do not support it. Although the target devices could decode the whole preamble correctly, they have to report an unsupported mode and terminate the RX. Most importantly, an injected preamble in an unsupported format or operation mode silences the channel regardless of the injection timing discussed above.

In conclusion, the timing and power requirements of the PrInS attacks are flexible. In fact, the PrInS attacks are more energy-efficient compared to typical frame injection and jamming attacks, since it only sends a small segment of a frame at relatively low power.

V. Experimental Evaluation

A. Experimental Setup

1) Implementation and Configurations: As the control and mesurements at the lower layer of commercial off-the-shelf (COTS) Wi-Fi chipsets are unavailable to us, we set up an 802.11a/ac system on an SDR platform. The access point (AP) and the adversary are NI USRP-2944R's, and the station (STA) is an FlexRIO 7975R with an NI 5791 adaptor module. We conduct experiments in a realistic indoor lab environment depicted in Fig. 5. The AP and the adversary are placed 6 ft apart from each other, while both of them are 5 ft from the STA. For simplicity, all the devices operate in SISO mode. The AP and STA run the standard-compliant 802.11 Application Framework [15] for downlink transmission, which is attacked by the adversary who injects forged preambles. We configure the AP to transmit 802.11a/ac data packets of fixed length (1024 bytes) and MCS 4 (16-QAM with $1/2$ code rate). The target packet generation rate is 2000 packets/second and 10000 packets/second for light and heavy traffic, respectively. The adversary is configured to transmit preambles with specific manipulations made to their SIG fields. The center frequency is 2.457 GHz with a bandwidth of 20 MHz.

2) Evaluation Metrics: To assess the impact of PrInS attacks, our most important evaluation metric is the *throughput ratio*, which is defined as the ratio between the throughput in the presence of attack and the throughput in the absense of attack. We also measure the performance under different signal-to-jamming ratios (SJRs) to evaluate the energy efficiency of proposed attacks. Additionally, the packet error rate (PER) is used to evaluate the ratio of frames that do not pass the FCS check under the data alteration attack.

B. Practical PrInS Attacks

1) Channel Silencing Attack: To silence the channel, the adversary is configured to inject 802.11a preambles with a target rate of 1000 preambles/second. Since the adversary only sends the preamble, no ACK frame could be received. To avoid the dramatical increase of adversary's contention window, we set a fixed backoff of 8 slots for its channel access. The value 8 is the mean of the random backoff of legitimate users whose initial contention window size is 15. This setup guarantees fair channel access. Besides, to exclude the impact of MAC layer mechanisms, the RTS/CTS and retransmission are disabled for the adversary.

First of all, we evaluate the impact of announced packet length when the SJR is fixed to 0 dB, and announced MCS is the same as the legitimate one. Fig. 6(a) shows that as the announced packet length increases from 0 byte to 4000 bytes, the throughput ratio decreases from $76\% \sim 86\%$ to $10\% \sim 20\%$. Obviously, the throughput reduction of heavy traffic is more severe than the light traffic. Besides, 802.11ac traffic is also impacted by the injected 802.11a preamble and the throughput ratio is smaller than 802.11a traffic when announced packet length is large. As the frame duration is determined both by the packet length and MCS, we further use MCSs of smaller indices (0 to 3) than the legitimate one, and study its impact by fixing the announced packet length to 4000 bytes. This time, the traffic is light, i.e., 2000 packets/second. Results in Table. I are as expected, the lower the MCS index, the lower the throughput ratio. Specifically, when the adversary announces a data MCS of BPSK (1/2), the throughput ratio is is almost zero (2%). This ratio is consistent when the injected preamble is in unsupported 802.11ac format or unsupported STBC operation mode under different SJR shown in Table. II.

To further understand and quantify the energy efficiency of channel silencing attacks, we adjust the transmit power of the AP and the adversary to obtain an SJR range of $[0, 30]$ dB. The legitimate traffic is light and the announced packet length in the forged preamble is 4000 bytes. The results in Fig. 6(b) demonstrate that even at a 30 dB SJR, the adversary brings the throughput of a legitimate link to 13% of its normal throughput by announcing the lowest MCS. When the injected preamble has the same MCS as legitimate frames, the throughput ratio is 34% at 30 dB SJR.

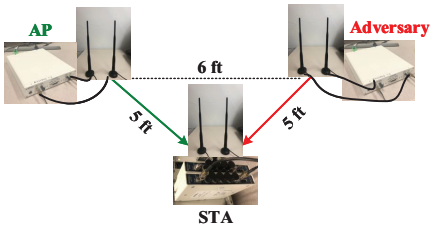
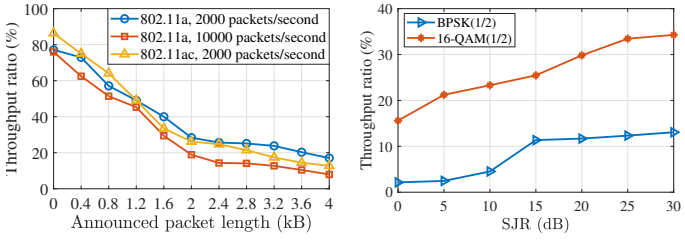


Fig. 5. Indoor experimental setup with SDRs and antennas.



(a) (b)

Fig. 6. Impact of channel silencing attack. (a) Throughput ratio vs. announced packet length, SJR=0 dB. (b) Throughput ratio vs. SJR, announced packet length=4000 bytes.

TABLE I
THROUGHPUT RATIO VS. MCS UNDER CHANNEL SILENCING ATTACK, ANNOUNCED PACKET LENGTH = 4000 BYTES, SJR=0 DB.

MCS index	0	1	2	3
Modulation	BPSK	BPSK	QPSK	QPSK
Code rate	1/2	3/4	1/2	3/4
Throughput ratio	2.15%	4.39%	6.34%	11.43%

TABLE II
THROUGHPUT RATIO UNDER DIFFERENT PRINS ATTACKS.

	Unsupported		Δt	
SJR (dB)	Format	Mode	9 µs	18 µs
0	1.97%	2.43%	9.20%	9.38%
10	2.54%	2.21%	14.81%	67.28%

2) Frame Detection Attack: We first block the signal between the AP and the adversary so that they cannot sense each other. Besides, the backoff of the adversary is fixed to 1 slot (i.e., 9 µs), while the backoff of the AP is set to 2 or 3 slots. Both the AP and the adversary have saturated traffic of 1024-bytes packets modulated by MCS 4, though the adversary only sends preambles. In this way, an injected preamble always collides with a legitimate frame with a certain time offset. The late-arrived legitimate preamble is undetectable at 0 dB SJR, so the throughput ratio is around 9% in Table. II under whatever time offset. However, at 10 dB SJR, $\Delta t = 9$ µs leads to a throughput ratio of 14.81% in contrast to 67.28% when $\Delta t = 18$ µs. Because the STA is running frame detection and synchronization during the first 16 µs of the injected preambles. Those legitimate frames arrive within this period are highly likely to be missed even with high SJR.

3) Data Alteration Attack: Conversely, the forged preamble is injected 9 µs later than the legitimate frame with a higher power (−10 dB SJR) for capture effect. The adversary announces MCS 3 rather than MCS 4 for the actual data. As a result, around $75\% \sim 80\%$ of packets are decoded by the STA with this wrong MCS and fail the FCS check. The PER is close to 0.8, which is far beyond 0.1 required for reliable Wi-Fi transmission. So the throughput ratio is 27.4% in average under such attacks.

VI. COUNTERMEASURES

Preamble authentication is the most straightforward way to combat preamble forgery in PrInS attacks. To facilitate this, the fixed Training field of the preamble could be replaced by a customized and randomized one. Firstly, all the legitimate devices generate the same seed with the network passphrase and current clock of millisecond accuracy. Then, they communicate using novel preambles with a distinct short Training field (STF) generated by the seed according to the eP-Mod scheme proposed in [16], [17]. The novel preambles are backward compatible because eP-Mod maintains the functions of the preambles. The outer adversary who does not know the exact eP-Mod scheme could not forge or replay a preamble with the distinct STF for the target network and current time to spoof the legitimate users. As seen from Fig. 2, upon detecting a preamble by CS/CCA, the receiver has to authenticate the preamble by checking its STF before detecting and decoding SIG fields. A legitimate preamble will pass the authentication and be processed as normal, while the forged preamble will fail the authentication which triggers the receiver to the CS/CCA state without a wait. Thus, the channel is released immediately as the PrInS attack fails.

VII. CONCLUSION

In this paper, we revealed that Wi-Fi networks are susceptible to preamble injection and spoofing (PrInS) attacks, which lead to channel silencing, frame misdetection, data alteration, and battery depletion. To demonstrate the practicality of such attacks, we provided both theoretical analyses based on the IEEE 802.11 protocols and experimental validations on a standard-compliant SDR platform. Our measurements show that the legitimate link suffers around 87% throughput decrease even at a high SJR of 30 dB. We further proposed the backward-compatible defense scheme that authenticates the customized and randomized preamble.

REFERENCES

[1] T. Alsop. (2020) WLAN connected devices worldwide 2016-2021. [Online]. Available: https://www.statista.com/statistics/802706

[2] E. Khorov *et al.*, "Testbed to study the capture effect: Can we rely on this effect in modern Wi-Fi networks," in *Proc. of IEEE Int. Black Sea Conf. on Commun. and Netw.*, Batumi, Georgia, 2018, pp. 1–5.

[3] M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the dragonfly handshake of WPA3 and EAP-pwd," in *Proc. IEEE Symp. on Secur. and Privacy*, San Francisco, CA, USA, May 2020, pp. 517–533.

[4] M. Vanhoef, P. Adhikari, and C. Pöpper, "Protecting Wi-Fi beacons from outsider forgeries," in *Proc. 13th ACM Conf. on Secur. and Privacy in Wireless and Mobile Networks*, Linz, Austria, 2020, p. 155–160.

[5] B. Bloessl, C. Sommer, F. Dressler, and D. Eckhoff, "The scrambler attack: A robust physical layer attack on location privacy in vehicular networks," in *Proc. Int. Conf. on Comput., Netw. and Commun. (ICNC)*, Anaheim, California, USA, Feb. 2015, pp. 395–400.

[6] S. Zhao, Z. Lu, Z. Luo, and Y. Liu, "Orthogonality-sabotaging attacks against OFDMA-based wireless networks," in *Proc. IEEE Conf. on Comput. Commun.*, Paris, France, May. 2019, pp. 1603–1611.

[7] E. Qi *et al.*, "Beacon protection," IEEE, Report doc.: IEEE 802.11-19/0314r2, Mar. 2019.

[8] D. S. Berger *et al.*, "Gaining insight on friendly jamming in a real-world IEEE 802.11 network," in *Proc. ACM Conf. on Secur. and Privacy in Wireless and Mobile Netw.*, New York, NY, USA, 2014, pp. 105–116.

[9] H. Rahbari and M. Krunz, "Secrecy beyond encryption: obfuscating transmission signatures in wireless communications," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 54–60, Dec. 2015.

[10] M. J. L. Pan, T. C. Clancy, and R. W. McGwier, "Jamming attacks against OFDM timing synchronization and signal acquisition," in *Proc. IEEE Mil. Commun. Conf.*, Orlando, FL, USA, Oct 2012, pp. 1–7.

[11] H. Rahbari, M. Krunz, and L. Lazos, "Swift jamming attack on frequency offset estimation: The achilles' heel of OFDM systems," *IEEE Trans. on Mobile Comput.*, vol. 15, no. 5, pp. 1264–1278, 2016.

[12] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std. 802.11, 2020.

[13] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications–Amendment 1: Enhancements for High Efficiency WLAN*, IEEE Std. IEEE 802.11ax, 2021.

[14] J. Lee *et al.*, "An experimental study on the capture effect in 802.11a networks," in *Proc. of the 2nd ACM Int. Workshop on Wireless Netw. Testbeds, Exp. Evaluation and Characterization*, 2007, pp. 19–26.

[15] "LabVIEW communications 802.11 application framework white paper," National Instrument, Tech. Rep., 2019.

[16] Z. Zhang, H. Rahbari, and M. Krunz, "Expanding the role of preambles to support user-defined functionality in MIMO-based WLANs," in *Proc. IEEE Conf. on Comput. Commun.*, July 2020, pp. 1191–1200.

[17] Z. Zhang, H. Rahbari, and M. Krunz, "Adaptive preamble embedding with MIMO to support user-defined functionalities in WLANs," *IEEE Transactions on Mobile Computing*, pp. 1–17, 2021.