SIGTAM: A Tampering Attack on Wi-Fi Preamble Signaling and Countermeasures

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

***Abstract*—The preamble is crucial for frame reception and interpretation in Wi-Fi networks. It carries essential information (e.g., length, rate, etc) in multiple Signal (SIG) fields that are needed to decode the payload portion of the frame. In this paper, we first use measurements and security analysis to identify the vulnerabilities of the SIG fields in terms of confidentiality, predictability, and integrity. Then, we introduce the SIG tampering attack (SIGTAM) in which the adversary exploits these vulnerabilities to craft and transmit a signal that tampers with legitimate SIG fields. This smart attack can pass the integrity validation including the even parity and cyclic redundancy check (CRC), hence deceiving the receiver(s). The resulting SIG fields not only lead to frame discard or decoding error at the receiver(s) but also channel access disorder at neighboring devices. We further strengthen this attack by making it robust to channel impairments and synchronization errors. The attack is quite stealthy in that it targets fewer than 20% of the subcarriers for a duration of $4\ \mu s$ only. Simulations and over-the-air (OTA) experiments are conducted on IEEE 802.11a/ax networks, which show that the proposed attack achieves almost 100% packet drop and packet error rates. Finally, we propose and evaluate schemes that detect the attack, identify impacted subcarriers, and retrieve the legitimate SIG fields based on their equalized frequency-domain symbols.**

***Index Terms*—Wi-Fi networks, IEEE 802.11, wireless security, preamble signaling, stealthy attack.**

I. Introduction

Wi-Fi is a key component of the wireless ecosystem, accounting for about 63% of the mobile traffic volume and more than 16 billion devices in 2021 [1]. Its success is mainly attributed to continuous advancements in its coverage, capacity, efficiency, and security. While many IEEE 802.11 standards and amendments have been issued on various aspects of Wi-Fi [2], [3], a given device typically supports only a subset of these standards/amendments and their mandatory/optional features. To facilitate interoperability and backward compatibility, Wi-Fi devices advertise their networking capabilities at both the medium access control (MAC) and physical (PHY) layers. At the MAC layer, beacon and probe frames broadcast various supported capabilities from which two devices choose common ones for communication. The frame-specific configurations of some of the chosen capabilities are then conveyed in the preamble at the PHY layer. For example, the Signal (SIG) field in the preamble may indicate the selected data rate out of several supported rates that are announced in a probe frame. Other parameters signaled in the frame preamble include the length, bandwidth (BW), and some system-level information such as resource unit (RU) allocation [4]. The preamble signaling mechanism enables the receiver to tune its hardware for the reception and interpretation of detected frames.

However, the performance of a Wi-Fi system is greatly impacted if the MAC and PHY signaling are maliciously jammed, forged, or tampered with. For instance, beacon spoofing attacks [5], [6] can cause unfair channel access, battery depletion, and channel switching. These attacks can be exploited to launch more advanced attacks [7]. To address such vulnerabilities, the latest IEEE standard [8] adopted beacon integrity and replay protection [9]. Whereas the preamble signaling mechanism is still left unprotected.

Therefore, we explore vulnerabilities of the Wi-Fi preamble signaling mechanism and present a novel SIG tampering attack (SIGTAM) on Wi-Fi SIG fields. In this attack, an adversary that detects a Wi-Fi preamble reactively transmits a crafted signal on selected subcarriers, aiming to tamper with the legitimate SIG fields captured by the receiver. SIGTAM exploits the predictability and weak integrity of the SIG fields, along with their structures and construction process, including interleaving, encoding, and modulation. The proposed tampering attack is immune to error detection and correction at the receiver, hence passing the integrity check. As such, the receiver is deceived into receiving frames with incorrect SIG fields. Thus, it may discard undesired frames before decoding the payload or get errors while decoding. Meanwhile, the neighboring devices may defer their channel access due to overheard misleading SIG fields. By attacking SIG fields over a short burst ($4\ \mu$s) and only on a few selected subcarriers, SIGTAM is quite stealthy. Yet, not only does it cause denial-of-service (DoS) similar to [10], [11], but it also enables more sophisticated attacks on crucial system-level information. In particular, network disturbance occurs when changing the Basic Service Set (BSS) color bits used for spatial reuse coordination among overlapping BSSs, or modifying RU allocation in multi-user (MU) communications. To defend against the attack, we propose to detect SIGTAM and identify attacked subcarriers based on the amplitude of equalized SIG fields or channel estimation. Further recovery of legitimate SIG fields is achieved by flipping the symbols' constellations on identified subcarriers under attack.

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.

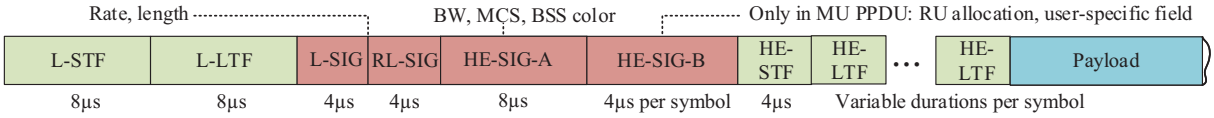


Fig. 1. MU HE-PPDU in Wi-Fi 6 with various SIG fields.

The main contributions of this paper are as follows:

- We expose and analyze the fundamental weaknesses of the SIG fields in Wi-Fi frames, specified by IEEE 802.11a/g/n/ac/ax.
- We introduce a stealthy attack–SIGTAM that exploits the identified weaknesses to modify the SIG fields of the frame preamble while passing the integrity check.
- We present an algorithm for designing the adversarial signal, which maximizes the attack efficacy while guaranteeing its robustness against channel impairments and synchronization errors.
- We conduct extensive simulations and hardware experiments on software-defined radios (SDRs) to demonstrate the effectiveness of the proposed SIGTAM in terms of packet error rate (PER) and packet drop rate (PDR). Our results show the attack achieves up to 100% PER and PDR with low energy. The proposed attack is robust against synchronization errors within $0.4\mu s$ and 7.8 kHz in time and frequency, respectively.
- We develop countermeasures for detecting SIGTAM and retrieving the correct SIG field with 100% probability as long as the normalized attack energy is below 0.58 or beyond 0.93.

II. Wi-Fi Preamble Signaling Mechanism

A. Overview of the Mechanism

We show in Fig. 1 the PHY protocol data unit (PPDU) of Wi-Fi 6, i.e., High Efficiency (HE) wireless local area network (WLAN) [4], as an example of PPDU based on orthogonal frequency-division multiplexing (OFDM). The PPDU starts with the legacy preamble fields, including a legacy short training field (L-STF), a long training field (L-LTF), and a SIG field (L-SIG). Their counterparts in the HE preamble fields are appended after the repeated L-SIG field (RL-SIG). The training fields (TFs) are publicly known waveforms used for frame detection, synchronization, channel estimation, and automatic gain control. The SIG fields signal frame-specific capabilities and properties. For instance, the L-SIG indicates frame length and rate. Note that in an HE PPDU, the L-SIG only indicates the basic rate of 6 Mbps for HE SIG fields. The payload rate is derived from the modulation and coding scheme (MCS) and the number of spatial-time streams (NSS), which are conveyed in HE-SIG-A. Channel bandwidth (BW) and BSS color are also signaled in HE-SIG-A. HE-SIG-B appears only in MU HE-PPDUs and is used to communicate RU allocation and user-specific information for MU transmission. (Very) High Throughput (HT/VHT) PPDUs in IEEE 802.11n/ac systems have similar formats and SIG fields to HE-PPDUs.

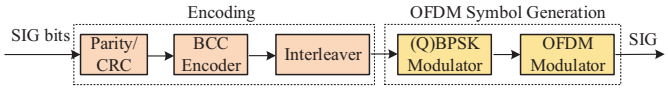


Fig. 2. Block diagram for SIG field construction.

As shown in Fig. 2, the even parity and cyclic redundancy check (CRC) bits of the SIG bits are calculated and appended after the SIG bits for error detection and integrity check. The resulting bits are encoded as binary convolution codes (BCC) of rate $1/2$ before being interleaved. The interleaved bits are mapped to BPSK or quadrature BPSK (QBPSK) symbols, and finally OFDM-modulated to construct the SIG fields.

The preamble signaling mechanism ensures interoperability and backward compatibility between Wi-Fi devices. More specifically, upon detecting a frame, the receiver determines the PPDU format from the constellations of SIG fields and length. If the PPDU format is supported by the receiver, it proceeds to decode and check the content of the SIG fields. In this step, the SIG fields are also validated through parity and CRC. If the SIG fields are valid and all the announced capabilities are supported, the receiver proceeds to tune its hardware accordingly to receive and decode the payload. At the same time, neighboring devices defer transmission for a time duration estimated from the length and rate values, or they automatically filter unintended frames by station (STA) ID and BSS color.

B. Security Vulnerabilities

1) Weak Integrity: The integrity of SIG fields is already protected though too weak to combat adversarial attacks. Particularly, the L-SIG is protected by the extremely weak even parity. Any attack that flips even numbers of bits can successfully pass the parity check. As for other SIG fields, they are protected by CRC with the generator polynomial $G(D) = D^8 \oplus D^2 \oplus D \oplus 1$, where "$\oplus$" is the operator for modulo-2 addition throughout this paper. As shown in Fig. 3, the serial input SIG bits to the linear feedback shift register (LFSR) get their CRC bits $\{C_7, C_6, \ldots, C_0\}$. According to the property of the generator, any bit error pattern $E(D)$ which is an exact multiple of $G(D)$ will not be detected. For example, the error pattern "100000111", corresponding to errors at input bits b_j, b_{j+6}, b_{j+7}, and b_{j+8} are undetectable. Moreover, the HE-SIGs truncate the original 8-bit CRCs and use the first 4 bits $\{C_7 \ldots C_4\}$ as their CRCs. We conclude from Fig. 3 that modifying the last two input bits will at most impact C_3, leaving the 4-bit CRC unchanged. This means that the 4-bit CRC compromises the integrity strength.

2) Lack of Confidentiality: PHY-layer fields, including SIG fields, are not encrypted. Unlike payload bits, the SIG bits are not scrambled to introduce randomness. In addition, the

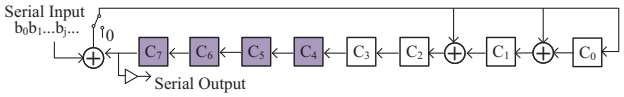


Fig. 3. CRC calculation for SIG fields other than L-SIG. The shaded bits are the truncated 4-bit CRC used by HE-SIGs.

TABLE I
RATE AND LENGTH OF VARIOUS FRAMES.

Frame	(b)ACK	RTS	CTS	Beacon	Data
Rate	6(24)	6	6	6	54(72)
Length	14(86)	20	14	299 ∼ 388	200(1600)

interleaver which writes the encoded SIG bits in rows and reads them out in columns is deterministic. Each group of 48 or 52 BCC encoded bits enter the $row \times col$ interleaver, whose structure is 4×13 for HE-SIGs and 3×16 for other SIG fields. The original ith encoded bit will be mapped to the subcarrier of index p given by: $p = (i \bmod col) \times row + \lfloor i/col \rfloor$. Such weaknesses expose crucial information in the SIG fields to potential adversaries. Furthermore, it enables the adversary to manipulate the SIG fields in the frequency domain to impact the corresponding target encoded bits.

3) Predictability: To make matters worse, most of the SIG fields are predictable. To validate this, we captured several packet traces over multiple operational Wi-Fi networks[1]. We observed that 97.8% of IEEE 802.11n frames have a BW subfield of 20 MHz, while most IEEE 802.11ac frames are 40 MHz. In both cases, the main coding scheme is BCC, rather than LDPC. Notably, the statistics in Table I demonstrates that the rate and length for most control frames (e.g., ACK, RTS, CTS) do not change frequently unless STAs join or leave changes the lowest capabilities of the network. And each BSS generally has two beacon lengths for the 2.4 GHz and 5 GHz bands, respectively. Not surprisingly, the lengths of data frames are often around 200 and 1600 bytes, corresponding to burst traffic (e.g., browsing) and streaming applications, respectively. We also observed traffic patterns where a few consecutive quality-of-service (QoS) frames of the same rate and length are followed by a block ACK and the inter-frame spacing (IFS) is 16 μs. This is mainly attributed to enhanced MAC features such as aggregation, block ACK, and transmission opportunity (TXOP). In addition, the type and arrival time of the next frame are also predictable from various MAC protocols. For instance, beacons are usually broadcasted every 102 ms. Moreover, RTS, CTS, data, and ACK frames come in sequence.

III. SIG TAMPERING ATTACK

In this section, we present the stealthy SIG tampering attack that exploits all of the above weaknesses and other Wi-Fi protocols to modify various SIG fields with profound implications on network performance.

A. Threat Model

Consider the Wi-Fi network in Fig. 4, where multiple legitimate STAs are associated with an Access point (AP). We

[1]We used a Cudy AC-1300 Wi-Fi USB adaptor equipped to a laptop running Wireshark on the Linux system.

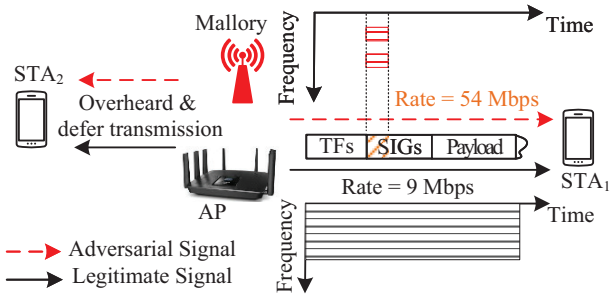


Fig. 4. Threat model and an example of the SIG tampering attack.

only depict two STAs to show downlink (DL) attacks. The threat in uplink (UL) is similar, which we will not discuss in detail. The channels between the AP and STAs are Rician fading channels modeled by [12], [13] plus AWGN. We assume the network operates in mixed mode as seen in practice. That is, the control and management frames are in legacy (IEEE 802.11a/g) PPDUs, while the data frames are in non-legacy (IEEE 802.11n/ac/ax) PPDUs. Though the SIG fields are replicated on various 20 MHz channels and multiple antennas, without loss of generality, we focus on the 20 MHz single-input-single-output channel.

Suppose an adversary called Mallory attempts to tamper with the legitimate SIG fields reactively. She is equipped with basic Wi-Fi capabilities sufficient to eavesdrop on the preamble and MAC header of legitimate frames and craft adversarial signals. Her ultimate goal is to degrade the network performance in two ways. First, this adversarial signal would fool the intended receiver(s) into filtering out frames by mistake or decoding the frame with incorrect SIGs and then discarding it due to errors. Second, Mallory's signal aims to manipulate the channel access of devices within the vicinity by injecting a misleading BSS color or Length subfield to cause network disturbance. This would help her conspirator gain the privilege of channel access. Generally, broadcast frames or MU frames are ideal targets for this attack because multiple links would be impacted. In particular, subsequently corrupted beacons due to tampering can lead to disconnections. To make her attack stealthy and energy-efficient, Mallory targets the most critical SIG fields on a few selected subcarriers for a short time duration. Fig. 4 illustrates an example of the DL attack, where Mallory transmits on a subset of subcarriers to tamper with the Rate subfield of 9 Mbps, changing it to 54 Mbps. In the following, we will show the attack strategy and techniques in detail.

B. L-SIG Tampering

The L-SIG consists of 24 information bits $b_0, \cdots, b_{23}$, as illustrated in Fig. 5. These bits are encoded into BCC of rate $1/2$ by the encoder in Fig. 6. Each input bit b_j has two output bits B_{2j} and B_{2j+1}, and b_{17} is the even parity bit. Flipping an even number of bits in the L-SIG allows the attack to evade the even parity check. However, to maximize the effectiveness of the attack, we study the optimal number and positions of the target SIG subfields. First of all, we claim Proposition 1, whose proof is trivial based on the analysis of the BCC encoder.

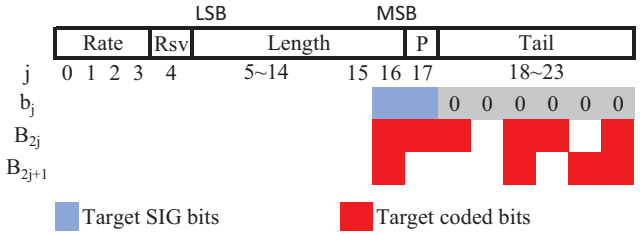


Fig. 5. Example L-SIG tampering attack by flipping two adjacent bits: most significant bit (MSB) b_{16} of Length subfield and parity bit b_{17}.

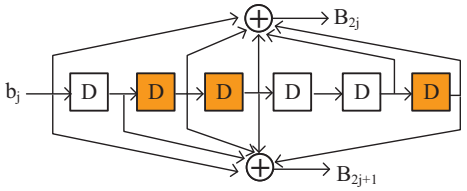


Fig. 6. Binary convolution encoder for SIG fields.

Proposition 1. *To tamper with the L-SIG fields by attacking the fewest number of subcarriers, while evading error detection and correction, Mallory must flip two adjacent SIG bits. More specifically, tampering with $b_j b_{j+1}$ only changes coded bits $B_i, i \in I = 2j + \{0, 1, 2, 4, 8, 9, 10, 13, 14, 15\}$, which are mapped to 10 subcarriers.*

Modifying the Length subfield to a larger or a smaller value can be problematic to a legitimate receiver. If the Length subfield is changed to a larger value, then according to the receiving state machine [8, Fig. 17-20], the legitimate receiver expects more data than what it has already received. It terminates the reception with an error code "Carrier Lost" sent to the MAC. However, the receiver still waits until the frame duration predicted by the Length and Rate subfields has elapsed. Meanwhile, other neighboring devices who overheard the attacked L-SIG have to defer their transmission for the same duration plus an extended IFS. On the other hand, changing the Length subfield to a smaller value would interrupt the legitimate reception in advance, and cause a frame check sequence (FCS) failure due to data loss.

The Length subfield of L-SIG almost always conveys values below 1600 bytes ($b_{16} = 0$) according to our preliminary measurements in Table I. Thus, flipping b_{16} and parity bit b_{17} adds the frame length by $2^{11} = 2048$ bytes while maintaining even parity. Following Proposition 1, to flip the target uncoded bits $b_{16}b_{17}$ ($j = 16$) in blue shown in Fig. 5, Mallory has to flip coded bits in red. In turn, flipping the first nonzero bit and its subsequent bit changes the Length subfield to a smaller value. In any case, flipping any two consecutive bits in the Length subfield leads to either a larger or smaller value.

The Rate subfield is quite significant for frame reception. For a legacy frame, this subfield is directly mapped to the MCS of the payload. So a tampered Rate subfield leads to demodulation and decoding errors, and eventually frame errors. In non-legacy frames, the Rate subfield is fixed to 1101. Therefore, a non-legacy frame will be misdetected and decoded as a legacy one if its Rate subfield is modified by the adversary. Though flipping 2 out of 4 bits in the Rate subfield is sufficient to carry out the attack, Mallory must also make sure the resulting Rate subfield is standard-compliant. We found that any 2-bit error pattern $e \in E, E = \{1100, 0110, 1010\}$ can change the legitimate Rate subfields $r \in R, R = \{1101, 1111, 0101, 0111, 1001, 1011, 0001, 0011\}$ to a standard-compliant one. In other words, $\forall r \in R, \forall e \in E, r \oplus e \in R$. According to Proposition 1, Mallory should generate the error pattern 1100 or 0110 to save energy. For simplicity, we only consider the former pattern where $b_0 b_1$ (i.e., $j = 0$) are modified.

Algorithm 1 SIG Tampering Attack Algorithm.

Monitor and compute CFO Δf_{AM} and channel $\boldsymbol{h}_{SM}$
Eavesdrop legitimate SIG field $\hat{\mathcal{S}}$ and channel $\boldsymbol{h}_{AS}$
Predict the target SIG field of the next frame
procedure CRAFT ADVERSARIAL SIGNAL
  Input: $I, \hat{\mathcal{S}} = \{\hat{S}_k\}_{1 \le k \le 64}$
  Initialize target subcarriers set $\Gamma = \emptyset$
  $\mathcal{K} = \{-28 : 28\} \setminus \{-21, -7, 0, 7, 21\}$
  $N = length(I)$
  if Attacking HE-SIG **then**
    $col = 13,\ row = 4,\ p_0 = 0$
  else
    $col = 16,\ row = 3,\ p_0 = 3$
  end if
  for $i \in I$ **do**
    $p = (i \mod col) \times row + \lfloor i/col \rfloor$
    $k = \mathcal{K}(p + p_0)$
    $\Gamma = \Gamma \cup k$
  end for
  $\mathcal{S} = \{S_k\}_{1 \le k \le 64} = \mathbf{0}$
  for $k \in \Gamma$ **do**
    $S_k = -\sqrt{E_a \times 64/N}\hat{S}_k \exp(j2\pi\Delta f_{AM})$
    if $\boldsymbol{h}_{AS}$ was overheard in sounding feedback **then**
      $S_k = S_k \boldsymbol{h}_{AS}\{k\}/\boldsymbol{h}^*_{SM}\{k\}$
    end if
  end for
  Construct an OFDM symbol $s = \mathcal{F}^{-1}(\mathcal{S})$ and add CP;
end procedure
Detect preamble or predict its arrival from traffic pattern
Estimate the start time of the target SIG field
Transmit s at the estimated timing

Denote the indices of target coded bits as $I = \{i_n\}_{1 \le n \le N}$, where N is the number of these bits (10 in this case). The indices I are further mapped to the corresponding set of subcarriers Γ by the deterministic interleaver. Mallory generates the adversarial signal based on the reference SIG field predicted from the target STA's recent traffic. Denote the frequency-domain reference SIG field as $\hat{\mathcal{S}} = \{\hat{S}_k\}_{1 \le k \le 64}$. Then, crafting the adversarial signal is straightforward by getting symbols on the target subcarriers from the reference L-SIG, flipping them, and scaling them by the normalized attack energy E_a. The OFDM modulation on the obtained $\mathcal{S}$ by Inverse Fourier Transform (IFT) and adding the cyclic prefix (CP) is then

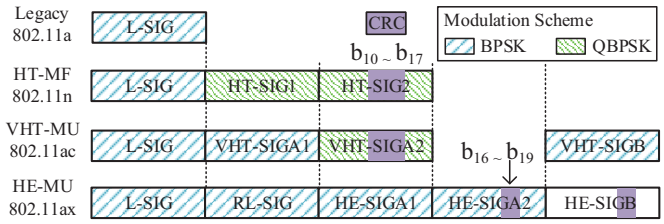


Fig. 7. SIG fields in various IEEE 802.11 PPDU formats.

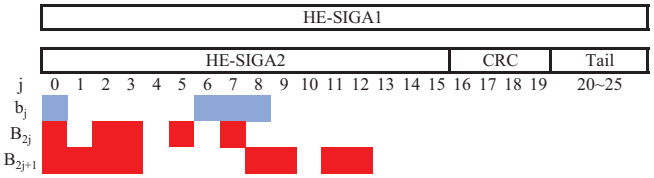


Fig. 8. Example HE-SIG tampering attack: flipping four bits with an error pattern 100000111 that does not change the CRC.

conducted. The whole attack process is explained in Alg. 1 and some enhancements from Steps 20 to 22 will be explained later in Section III-D.

C. Non-legacy SIG Fields Tampering

Fig. 7 presents various non-legacy SIG fields along with their CRC bits and modulation schemes in different PPDUs. In the HT-SIG2 and VHT-SIGA2, bits $b_{10}, \cdots, b_{17}$ are 8-bit CRCs for the whole HT-SIG and VHT-SIGA, respectively. Similarly, bits $b_{16}, \cdots, b_{19}$ of HE-SIGA2 are 4-bit CRC for the whole HE-SIGA. It is worth noting that: (1) HT-SIGs and VHT-SIGA2 are QBPSK modulated; and (2) each HE-SIG consists of 26 uncoded bits, 2 bits more than other SIG fields. Accordingly, Alg. 1 adapts the interleaving and subcarrier mapping depending on the target SIG fields to craft adversary signals. Recall our analysis in Section II-B1, we propose the attack strategy as stated in Proposition 2.

Proposition 2. *For a non-legacy SIG field, Mallory should tamper with it to create an error pattern* 100000111 *that does not change the CRC. Moreover, HE-SIGs can also be maliciously modified at* b_{14} *and/or* b_{15} *right ahead of the* 4*-bit CRC without impacting it.*

For illustration, we show in Fig. 8 the attack that tampers with b_0, b_6, b_7, b_8 of HE-SIGA2 by flipping 13 coded bits in red on their corresponding subcarriers. Because the attacked SIG subfields are related to TXOP duration and coding, such an attack causes unfair channel access and decoding error. Similarly, tampering with any other 4 bits of HE-SIGA1 or HE-SIGA2 generating this error pattern is effective. Given the index j of the first tampered bit, the indices of the target coded bits can be computed as $I = 2j + \{0, 1, 3, 4, 5, 6, 7, 10, 14, 17, 19, 23, 25\}$. This attack strategy also applies to HT-SIGs and VHT-SIGs. Tampering with $b_{14}b_{15}$ of HE-SIG-A2 is similar to the aforementioned attack against two adjacent bits in L-SIG, and $j = 14$ is used to derive the indices I of 10 target coded bits based on Proposition 1. In addition, tampering with either b_{14} or b_{15} by flipping 10 coded bits of indices $I = 2j + \{0, 1, 3, 4, 5, 6, 7, 10, 12, 13\}$ also works. After the selection of j and derivation of I, the remaining attack procedures are explained in Alg. 1.

We study and summarize possible SIG subfields that are susceptible to SIGTAM and its impacts in Table II. For instance, the legitimate receiver would filter out intended frames by mistake or transmit with too high power causing inter-BSS interference if the MCS and BSS color subfields in HE-SIGA are modified by the attack. Besides, tampering with RU allocation and STA-ID of HE-SIGB leads to incorrect reception and frame filtering in MU transmissions.

D. Challenges and Solutions

However, a practical SIGTAM has to address several challenges.

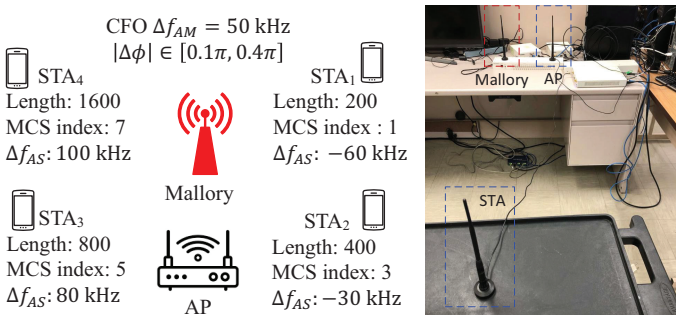
1) SIG fields variation: Despite the QoS data (in a TXOP), control, and management frames whose SIG fields are relatively deterministic, other frames may have variations in certain SIG fields over STAs and time. So the adversary has to keep track of the profile of each STA's SIG fields, and predict the destination STA of the next frame by traffic pattern to select corresponding reference SIG fields. Moreover, as long as the variation is at least 6 bits (BCC depth) away from the target SIG bits, attacks that use the same reference SIG field are still effective.

2) Synchronization: For a successful attack, Mallory should also guarantee a reasonable synchronization of the adversarial signal with the legitimate signal. To this end, at Step 20 of Alg. 1, the estimated carrier frequency offsets (CFOs) Δf_{AM} between her and the AP should be compensated in the generated adversarial signal. To facilitate a real-time reactive attack, the adversarial signal is generated in advance. Mallory keeps sensing the target channel to determine when to transmit. The classical frame detection by energy and L-STF guarantees a coarse timing of the incoming frame. It is optional for Mallory to conduct fine-tuned frame detection and synchronization via the L-LTF. Opting out of this leaves her more time to switch from receiving to transmitting mode before the arrival of the target SIG field. WiFi devices are required to detect a frame within $4\,\mu$s of L-STF and then switch within $2\,\mu$s (see [8, Fig. 10-21]). So she has sufficient time to tune the processing delay such that the adversarial signal superposes well with the target SIG field. As for the propagation delays of the legitimate versus adversarial signals, the gap of several nanoseconds is negligible compared to the 50 ns sample interval. Thanks to certain MAC protocols, the next frame may arrive exactly after the IFS. This further improves the synchronization accuracy.

3) Channel effects: To minimize the difference between the legitimate channel and adversarial channel that incurs failed attack, Mallory should locate around the AP within a distance of a few wavelengths λ. Besides, given the distance between the AP and STA of d, the distance from Mallory to the STA should be $d - m\lambda, m \in \mathbb{Z}$ to guarantee a similar channel [14, §2]. Alternatively, she could eavesdrop on the channel report [4, §27.3.16] to get $\boldsymbol{h}_{AS}$ from the STA to the AP, and estimate the channel $\boldsymbol{h}_{SM}$ from the STA to herself. By channel reciprocity, the adversarial channel from Mallory to

TABLE II
SIG FIELDS TAMPERING AND IMPACTS

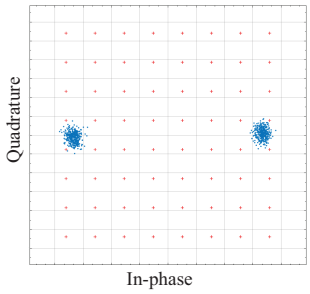
SIG Field	Subfield	Error Pattern	1st index j	Impacts
L-SIG	Rate	1100, 0110	$0/1$	Decoding error, PPDU format misdetection
L-SIG	Length	$b_j b_{j+1}$	$4 \leq j \leq 16$	Channel silencing, FCS failure
HE-SIGA1	MCS and BSS color	100000111	3	Decoding error, undesired filtering
HE-SIGA2	TXOP and Coding	100000111	0	Unfair channel access, decoding error
HE-SIGA2	Doppler	last bit	15	Inaccurate channel estimation
HE-SIGB	RU allocation	100000111	0	Incorrect reception
HE-SIGB	STA-ID	100000111	$0/1/2$	Filtering intended frames by mistake
HE-SIGB	User-specific coding	last 2 bits	14	Decoding error



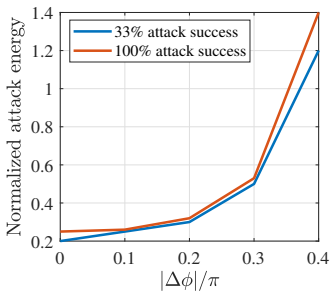
(a) Matlab simulation.

(b) OTA experiments.

Fig. 9. Simulation and experiments setups.



(a) Rate index 1 modified to 7.



(b) Robustness to channel phasor.

Fig. 10. Efficacy and robustness of tampering Rate subfield in L-SIG.

the STA is $\boldsymbol{h}_{MS} = \boldsymbol{h}^*_{SM}$, where "$*$ " is the conjugate operator. This information is then used to compensate the channel in the adversarial signal at Step 22 of Alg. 1. Even if these conditions are not met, the use of (Q)BPSK modulation and strong forward error correction (FEC)–$1/2$ BCC encoding make the attacked SIG fields resilient to errors introduced by channel impairments.

IV. Performance Evaluation

In this section, we validate the effectiveness, energy efficiency, and robustness of the proposed SIGTAM.

A. Implementation and Setup

1) Simulation: To access bit-level information in SIG fields, we perform MATLAB simulations of the proposed SIGTAM on IEEE 802.11a/ax transmissions under the WLAN channel Model-B with AWGN of 20 dB SNR. The network setup is depicted in Fig. 9(a). The four single-antenna STAs are distributed $3 \sim 5$ meters from the single-antenna AP, which is 1 meter from Mallory. The frequency offsets and most frequent SIG subfields in Data frames of each STA are also listed. The frequency offset between the AP and Mallory is 50 kHz, and the adversarial channel has an absolute phase offset $|\Delta\phi|$ in the range of $[0.1\pi, 0.4\pi]$ from the legitimate channel.

2) Over-the-air Experiments: We further implement and launch the proposed SIGTAM on a testbed built on Matlab and USRPs. As shown in Fig. 9(b), the AP and Mallory are USRP 2922s, both of which are 2 meters from the STA implemented on USRP 2942. All three devices are equipped with single antennas and operate on 2.48 GHz with 20 MHz bandwidth.

3) Evaluation Metrics: To assess the impact of SIGTAM, we define the following evaluation metrics. *Packet drop rate (PDR):* the ratio between the packets that are dropped before decoding the payload and all the transmitted packets. The drop could be attributed to invalid SIG fields or BSS color and STA-ID mismatches. *Packet error rate (PER):* the ratio between the packets that encounter decoding errors due to incorrect SIG fields and all the transmitted frames. *Normalized attack energy E_a:* the energy of adversarial signal normalized by the energy of a legitimate SIG field.

B. Effectiveness and Energy Efficiency

We first vary the rates of Data frames sent to STA_2 and tamper with the Rate subfield of the L-SIG by flipping the first two bits. For convenience, we index the Rate subfield values in ascending order as $0 \sim 7$. The original and corresponding tampered Rate indices are shown in Table III. Those lower Rate subfield values with indices $0 \sim 4$ are changed to higher values and vice versa. For example, in Fig. 10(a), the Rate index 1 is modified to 7. So the actual BPSK payload symbols are mistakenly demodulated as 64-QAM by the receiver. Given the unchanged Length subfield, the predicted frame duration is shorter. As a result, the receiver terminates the reception before the actual end of the frame and fails the FCS check (error code 3). In contrast, upon detecting a Rate subfield changed to a lower one and unchanged Length subfield, the receiver who expects more data reports "Carrier Lost" (error code 4). Though the PERs when tampering with different Rate subfield values have significant differences at low attack energy, PERs when normalized attack energy is 0.26 are 100% for all Rate subfield values. Besides, the PER is not only impacted by the Rate subfield itself, but also part of the Length subfield that is encoded together with it. With the same attack energy, the PERs for ACK/CTS (14 bytes) frames are lower than the PERs for Data (400 bytes) frames, which in turn, are lower than the

TABLE III
PACKET ERROR RATE WHEN TAMPERING RATE SUBFIELD OF L-SIG IN DL FRAMES, DATA LENGTH= 400 BYTES, $|\Delta\phi| = 0.1\pi$

Original Rate index		0			1	2	3	4	5	6	7
Tampered Rate index		6			7	4	5	2	3	0	1
Error code		3			3	3	3	4	4	1	4
Frame type		Beacon	ACK/CTS	Data	Data	Data	Data	Data	Data	Data	Data
PER(%)	$E_a = 0.24$	100	0	45.7	99.6	7.4	0	0	100	0	0
	$E_a = 0.25$	100	0	100	100	100	72.1	93.7	100	31.9	2.8
	$E_a = 0.26$	100	100	100	100	100	100	100	100	100	100
Error codes: 1 format misdetection, 2 invalid SIG, 3 FCS failure, 4 carrier lost											

TABLE IV
PACKET ERROR RATE WHEN TAMPERING LENGTH SUBFIELD OF L-SIG

Original length		200	400	800	1500
Larger length		2248	2448	2848	3548
PER(%)	$E_a = 0.18$	0	100	100	13.1
	$E_a = 0.20$	24.7	100	100	100
	$E_a = 0.22$	100	100	100	100
Smaller length		196	392	784	1498
PER(%)	$E_a = 0.18$	24.7	100	33.7	100
	$E_a = 0.20$	100	100	100	100

PERs for Beacon frames (315 bytes). We also show that the attack is robust to a channel phase offset within 0.4π. Though a larger offset requires higher normalized attack energy up to 1.4 as seen in Fig. 10 (b).

Then, we vary the lengths of Data frames sent to STA_1 and flip bits $b_{16}b_{17}$ of the L-SIG to change the Length subfield to a larger value. As we can see from Table IV, this adds 2048 bytes to the actual Length subfield, and the receiver would report "Carrier Lost" error because it is expecting a longer frame. When maliciously modifying the Length subfield to a smaller value, 2^n bytes are missed, causing FCS failure. Interestingly, it requires slightly less attack energy to change the length to a smaller value than to a larger value. Because the Viterbi decoder is less sensitive to the imperfect adversarial signal near LSB.

Now, we consider all 4 STAs and simulate the SIGTAM in both DL and UL directions. We vary the normalized attack energy from 0.16 to 0.32, the resulting PERs are shown in Fig. 11. Overall, UL tampering attack requires higher attack energy (around 0.3) due to inaccurate reference signal caused by channel effects. Unlike DL attacks, modifying the Length subfield of the L-SIG to a larger value requires less energy than to a smaller value. It is mainly because changing to a larger length is a deterministic flipping at $b_{15}b_{16}$, while changing to a smaller value is dependent on the profile of the source STA.

C. Robustness to Synchronization Errors

We also evaluate SIGTAM with imperfect synchronization. First of all, we tamper with the Rate subfield of L-SIG, MCS and BW subfields of HT-SIG, as well as MCS and BSS color subfields of HE-SIG, respectively. This caused packet drop due to standard-incompliant SIG fields and BSS color or STA-ID mismatches. In Fig. 12(a), the attack causes reasonably high PDR within 0.4μs delay offset. However, the attack is

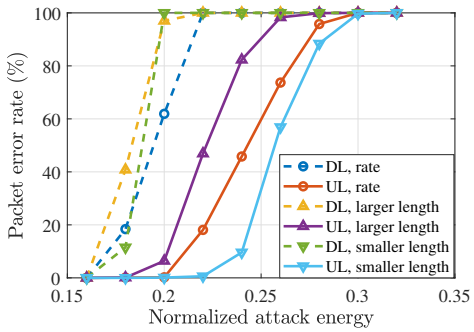
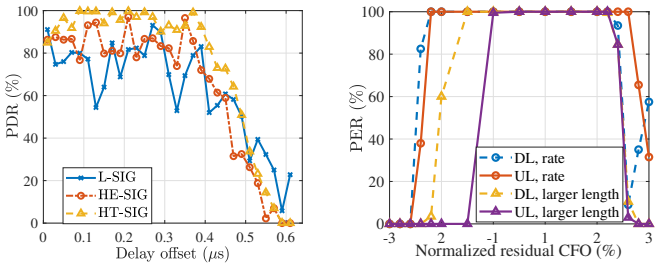


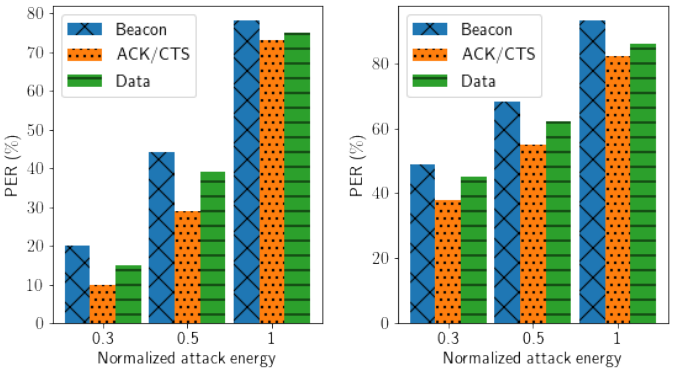
Fig. 11. PER vs. E_a in DL/UL SIGTAM on L-SIG.



(a) PDR vs. delay offset. (b) PER vs. δ_f.

Fig. 12. SIGTAM under imperfect synchronization, $E_a = 0.5$.

less effective beyond this offset, showing a significant PDR decrease. Additionally, the PDR under HT-SIG tampering is less fluctuating compared to the other two cases. Because the attack may not change the target field to the desired value under delay offsets but corrupt the integrity. And integrity failure of SIG fields also leads to packet drop before decoding payload. Yet the integrity failure depends on the delay offset. So the HT-SIG which has stronger integrity compared to the L-SIG and HE-SIG has a consistently higher probability to drop frame under SIGTAM. Besides, Fig. 12(b) shows that when the normalized residual CFO δ_f (the error in the estimation of f_{AM} normalized to subcarrier spacing of 312.5 kHz) is within the IEEE 802.11 regulation of $\pm 3\%$, the PER of Rate subfield tampering is not impacted much, while the PER of Length subfield tampering drops significantly beyond the $[-1\%, 2\%]$ bound. Because the target subcarriers for Length tampering have larger indices than the ones for Rate tampering, hence, are more vulnerable to CFO. On average, SIGTAM can tolerate a residual CFO of 2.5%, which translates to 7.8 kHz.



(a) Without channel compensation. (b) With channel compensation.

Fig. 13. PER vs. E_a for various frames in experiments.

D. Experimental Results

For simplicity, we only transmit Beacon, ACK, CTS, and QoS Data frames whose SIG fields and arrival time can be accurately predicted. Mallory first eavesdrops for a period to get the recent SIG fields and CFO estimations. Then, she generates the adversarial signal according to Alg. 1 and compensates the CFOs and channels if necessary. For each type of frame, we transmitted 5000 frames. Fig. 13(a) is the result when the channel is not compensated. The attack changes the Rate field with a success probability of up to 78%. Fig. 13(b) is the result when the channel is compensated using the channel estimated from the preceding frame. Now the PER is increased above 82% when the normalized attack energy is 1. However, the PER could not reach 100% because the CFO and channel changes from the preceding frame to the current attacked frame are so significant that impact the effect of compensation. In addition to the uncalibrated USRPs, the other reason is the IFS is hundreds of milliseconds due to Matlab-USRP processing, which is far above the values in reality.

V. Defenses and Evaluation

A. Detection and Identification

Since the attack is stealthy in both time (short burst) and frequency (very few dynamically selected subcarriers) domains, it is infeasible to detect through power analysis or spectrum analysis. Instead, we detect directly through signal analysis of the preamble. Although the adversarial signal has a much lower power compared to the legitimate one, its energy on attacked subcarriers is far higher than the legitimate signal to overshadow and flip (Q)BPSK symbols on these subcarriers. However, depending on the energy differences of two signals on attacked subcarriers, the equalized flipped symbols usually have a lower or higher amplitude rather than around 1. Therefore, the receiver only needs to measure the amplitude of each subcarrier in the SIG field after equalizing the channel effect. Those subcarriers with abnormally low or high amplitude indicate a SIGTAM attack on them. In this way, the receiver can detect the attack and identify the attacked subcarriers. Alternatively, the frequency-domain channel estimation on decode-and-reconstructed SIG fields could be exploited to detect and identify the proposed attack. Because the proposed attack does not change the LTFs used for channel estimation. So the normal channel estimation by LTFs is the legitimate channel, while the channel estimation by the SIG fields is impacted by the attack.

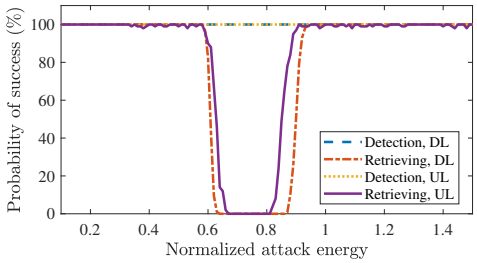


Fig. 14. Probability of successful detection and retrieving in simulations.

We evaluate the detection and identification against UL/DL SIGTAM in L-SIG under our simulation setup, and show the results in Fig. 14. We are able to detect and identify the SIG tampering attack with 100% probability regardless of the normalized attack energy. Because the amplitudes of attacked subcarriers after channel equalization significantly deviate from 1, which is often beyond the threshold of 0.15.

B. Retrieving SIG Fields

Next, to mitigate the impact posed by SIGTAM, we try to retrieve the correct SIG fields. The classic successive interference cancellation does not work for this purpose. Because the adversarial signal itself is not independently decodable and the adversarial channel information necessary for reconstructing the adversarial signal is not available at the receiver. Nevertheless, we know that the constellations of (Q)BPSK symbols on identified subcarriers must have been flipped under attack. So the receiver just needs to flip the (Q)BPSK symbols on identified subcarriers back, and then decode and retrieve the correct SIG field.

Based on the detection and identification, the performance of retrieving legitimate SIG fields, hence the frame is also depicted in Fig. 14. The receiver could retrieve the tampered SIG field and the frame with a probability of around 100% when the normalized attack energy is less than 0.58 or greater than 0.93. However, it is quite challenging to retrieve the SIG fields when the normalized attack energy is in the range of $[0.58, 0.93]$. In these scenarios, even though the attack detection succeeds because of abnormal amplitudes on multiple attacked subcarriers, the deviations of the amplitudes on a subset of attacked subcarriers are too small to be identified. Hence, these unidentified attacked subcarriers are not corrected. Yet as long as the attack is detected, the receiver can abort the reception to avoid destructive impacts of SIGTAM. For future improvement, we could address this issue by the other proposed identification based on channel estimation.

VI. Related Work

Attacks on PHY Signaling: Wireless networks are subjected to spoofing and tampering attacks on PHY signaling. Recent attacks in Wi-Fi networks [10], [11] deceived legitimate users

into deferring their channel access or decoding the frames incorrectly. However, the whole Wi-Fi preamble with malicious SIG fields should be forged and injected without any payload to launch these attacks. They last for a longer time and consume more energy, especially when colliding with legitimate frames. Hence, they are prone to be detected. Similar attacks [15], [16] were also identified in the cellular networks. The SigOver attack [15] crafted messages that overshadow the legitimate broadcast LTE subframes such as system information block to incur DoS and network downgrading. In addition to the concern of high power, crafting a subframe that contains control information along with data is nontrivial. A similar attack strategy as our work was proposed in the SigUnder attack [16], where the 5G synchronization signal block was overwritten on selected subcarriers to guarantee stealthiness without sacrificing efficacy. But both attacks are more likely to succeed when the reference signals are also transmitted to change the receiver's channel estimation. In comparison, our attack does not additionally transmit an adversarial LTF for channel estimation. Most importantly, the target cellular control signals have fixed timing and no integrity protection, which is less challenging to attack than the SIG fields.

Detection: To detect the SIG field spoofing, [11] exploited network and device throughput, timing and energy of RF signal, and PHY interface outputs. The second method is ineffective against our attacks as our lower-power adversarial signal overlays on a tiny part of the legitimate signal. The other two might imply but not confirm the existence of the SIGTAM attack. The authors of [17] consider higher-order statistic analysis of time-domain constellations to detect emulated signals. But the low-power SIGTAM attack barely impacts the time-domain constellations. Power analysis on the pilot and null subcarriers is utilized to detect and identify the set of subcarriers impacted by orthogonality sabotaging attacks [18]. Nonetheless, the SIGTAM attack cannot be detected by time- or frequency-domain power analysis as it only impacts the power of a small subset of subcarriers for around $4\,\mu s$.

Mitigation: Successive interference cancellation (SIC) cancels out interference from another decodable packet of the same technology [19] or cross-technology [20]. However, the adversarial signal in our attack is not decodable, and the received SIG field only differs from the legitimate one on attacked subcarriers. Thus, conventional SIC will cancel out the signal on unattacked subcarriers. The solution in [16] subtracts a scaled-down version of the decoded signal for SIC or applies SIC to equalized symbols on victim subcarriers identified by constellation analysis and/or channel estimation. The first approach needs to adapt the downscaling ratio to channel and transmit power. The other approach looks similar to ours, though our method simply uses equalized SIG field symbols without SIC. The embedded bits in the preamble proposed by [21] can serve as the frame-dependent seed for interleaver randomization or SIG field encryption to thwart the SIGTAM attack. But such defense schemes require modifications to the standards.

VII. Conclusions

In this paper, we identified weaknesses in the SIG fields of the preamble and presented an intelligent attack – SIGTAM. With this attack, the adversary can maliciously modify the SIG fields by transmitting on a small set of selected subcarriers for only $4\,\mu$s. Our evaluations show that the legitimate links suffer almost 100% PER and PDR even when the adversarial signal energy is as low as around $20\% \sim 30\%$ of one legitimate SIG field. More importantly, such an attack is effective even with imperfect time and frequency synchronization. We also proposed easy-to-implement defense mechanisms that achieved a successful detection and recovery of 100% in most cases.

References

[1] W.-F. Alliance, "Value of Wi-Fi," 2021. [Online]. Available: https://www.wi-fi.org/discover-wi-fi/value-of-wi-fi

[2] "Official IEEE 802.11 work group timelines," May 2022. [Online]. Available: https://www.ieee802.org/11/Reports/802.11Timelines.htm

[3] B. Verney, "IEEE 802.11 standard and amendments," July 2020. [Online]. Available: https://wifiwizardofoz.com/802-11-standard-and-amendments/

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

[5] A. Martínez *et al.*, "Beacon frame spoofing attack detection in IEEE 802.11 networks," in *Proc. Intl Conf. on Availability, Rel. and Secur.*, Barcelona , Spain, 2008, pp. 520–525.

[6] B. Könings, F. Schaub, F. Kargl, and S. Dietzel, "Channel switch and quiet attack: New DoS attacks exploiting the 802.11 standard," in *Proc. of the IEEE Conf. on Local Comput. Netw.*, 2009, pp. 14–21.

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

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

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

[10] Z. Zhang and M. Krunz, "Preamble injection and spoofing attacks in Wi-Fi networks," in *Proc. IEEE Global Commun. Conf.*, 2021, pp. 1–6.

[11] S. Gvozdenovic, J. K. Becker, J. Mikulskis, and D. Starobinski, "Truncate after preamble: PHY-based starvation attacks on IoT networks," in *Proc. ACM Conf. on Secur. and Privacy in Wireless and Mobile Netw.*, Linz, Austria, July 2020, pp. 89–98.

[12] V. Erceg, L. Schumacher, P. Kyritsi *et al.*, "TGn Channel Models," IEEE, Report Doc. IEEE 802.11-03/940r4, May 2004.

[13] J. Liu, R. Porat, N. Jindal *et al.*, "TGax Channel Models," IEEE, Report Doc. IEEE 802.11-14/0882r4, Sep 2014.

[14] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

[15] H. Yang *et al.*, "Hiding in plain signal: Physical signal overshadowing attack on LTE," in *Proc. USENIX Secur. Symp.*, Santa Clara, US, Aug. 2019, pp. 55–72.

[16] N. Ludant and G. Noubir, "SigUnder: A stealthy 5G low power attack and defenses," in *Proc, ACM Conf. on Secur. and Privacy in Wireless and Mobile Netw.*, 2021, p. 250–260.

[17] X. Zhang, P. Huang, L. Guo, and Y. Fang, "Hide and seek: Waveform emulation attack and defense in cross-technology communication," in *Proc. IEEE Intl. Conf. on Distrib. Comput. Syst.*, 2019, pp. 1117–1126.

[18] 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.

[19] S. M. R. Islam, N. Avazov *et al.*, "Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges," *IEEE Commun. Surveys Tutorials*, vol. 19, no. 2, pp. 721–742, 2017.

[20] S. Gollakota, F. Adib, D. Katabi, and S. Seshan, "Clearing the RF smog: Making 802.11n robust to cross-technology interference," *SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 4, p. 170–181, Aug 2011.

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