Combating Adversarial Covert Channels in Wi-Fi Networks

HOORIN PARK (Member, IEEE), WONWOO JANG (Graduate Student Member, IEEE), JEEKYUNG SUNG (Graduate Student Member, IEEE), HEEJUN ROH (Member, IEEE), AND WONJUN LEE (Fellow, IEEE)

1Department of Information Security, Seoul Women’s University, Seoul 01797, Republic of Korea
2Network and Security Research Laboratory, School of Cybersecurity, Korea University, Seoul 02841, Republic of Korea
3Department of Cyber Security, Graduate School, Korea University Sejong Campus, Sejong 30019, Republic of Korea

Corresponding author: Wonjun Lee (wlee@korea.ac.kr)

This work was supported in part by the National Research Foundation of Korea (NRF) funded by the Korean Government (Ministry of Science and ICT) under Grant 2019R1A2C2088812 and Grant 2022R1G1A1007263, in part by the Korea University, and in part by the Research Grant from Seoul Women’s University under Grant 2021-0385.

ABSTRACT

Physical layer covert channels exploit the characteristics of radio signals to convey secret messages while remaining inconspicuous within wireless channels. With specifically designed modulation schemes, covert channels effectively disguise secret messages as noise. Since the intentionally embedded noise dissipates when the radio signal is decoded as a bitstream, adversaries can maintain a stealthy breach in communication systems. IoT devices, particularly, often utilize vendor-specific firmware and hardware whose security verification is too complex for everyday users. Hence, these devices can easily be compromised to transmit their data to unauthorized adversaries via the covert channels. To this end, we propose a novel countermeasure system, Ghost-Fi Detector, which detects the covert channels reliably and comprehensively. Our attack models reflect a real-world wireless network technology, Wi-Fi, and cover three aspects of its radio signal characteristics including amplitude, phase, and frequency. Since each model induces distinct manifestations in the received signal, there is no dominant universal detection mechanism that detects all the attack models simultaneously. Instead, Ghost-Fi detector consists of six precisely designed complementary defense mechanisms that perform passive radio-frequency analyses. Evaluation results show that Ghost-Fi Detector achieves an average hit rate of 95% with an almost zero false-positive rate for arbitrary Wi-Fi frames.

INDEX TERMS

Covert channel detection system, modulation-based covert channel, wireless network security, Wi-Fi network.

I. INTRODUCTION

Wireless covert channel technology aims at the establishment of stealthy communication links between predefined hosts. To achieve this, the transmitter encodes a secret message into a covert channel behind a legitimate channel. A receiver aware of the covert channel can decode both the legitimate message and the covert message with the shared decoding rule, whereas an innocent receiver can decode only the legitimate message. Since the wireless covert channel does not induce much superficial difference, it is very difficult for innocent receivers to detect the covert channel without proper prior knowledge. In other words, the transmitter can send secret messages while keeping the receiver unaware of the covert channel.

In this context, we particularly focus on a certain type of wireless covert channels that manipulates modulation schemes to send covert messages. Among the various covert channel technologies, the modulation-based approach has a unique position with the following three features. First, the methods achieve very high throughput, while other approaches transmit only a few bytes per packet or one bit per packet interval [1], [2], [3], [4], [5], [6], [7], [8]. Second, the studies create covert channels in the physical layer by
tampers tampering radio signals, whereas other approaches utilize unused fields of specific protocols or meta-information of frames [9], [10]. Third, the legitimate channel is preserved to be decoded even after adding artificial noise which encode the covert messages. It is worth noting that other hosts receiving the covert packet simply take it as a noisy packet. Since the radio signal is very temporal and volatile, manifestations of the covert channel in the wireless signal resemble mere noise; covert messages vanish into the air when only legitimate messages are decoded. Besides, covert channels do not affect the establishment of legitimate channels, hence forestalling the/ innocent receivers from recognizing the additional channel. This makes the modulation-based covert channels invisible to the existing network security solutions.

Although a wide range of studies propose to detect the covert channels [11], [12], [13], they cannot be applied to the recent modulation-based approach. The detection methods use meta information of the received packets such as inter-arrival time. However, the problem is that the covert messages are embedded in the physical layer, and innocent receivers always remove the intended noise silently before transferring the packets from the physical layer to the upper layers, i.e., decapsulation. Thus, the existing detection solutions that work on the upper layers cannot detect the modulation-based covert channels.

In light of the features, we ask how can we detect the presence of the covert channels when the modulation-based covert channels are used by adversaries for information leakage. This paper identifies an emerging class of side-channel attack named modulation-based covert channel attack, where the attacker transmits unauthorized messages with compromised modulation schemes. We refer to the compromised Wi-Fi transmitters as Ghost-Fi. Ghost-Fi comprehensively covers attack models on a real-world wireless network technology, Wi-Fi, with the modified characteristics of radio signals such as amplitude, phase offset, and frequency. While the artificial noise cannot be distinguished from general noise at the legitimate receiver, the adversary can decode the artificial noise into the covert messages. Especially in Wi-Fi, the problem is exacerbated by the fact that the link throughput by the modulation-based covert channels can reach Mbps-level.

Fig. 1 illustrates the concept of Ghost-Fi. For example, we suppose that the adversary shifts the amplitude of the legitimate symbols to encode covert symbols. The user considers that the symbols are modulated by a Phase Shift Keying (PSK) modulation scheme, but Ghost-Fi makes the symbols have different amplitude levels to create a covert channel. Unfortunately, the legitimate receiver does not recognize the covert channel and only demodulates the legitimate channel with PSK since it expects phase-modulated symbols. On the other hand, the attacker acts as a passive eavesdropper who can decode the signal and obtain a covert message using different amplitude levels (i.e., Amplitude Shift Keying (ASK) modulation scheme). We call this type of attack modulation-based covert channel attack.

Once the covert channel is established, Ghost-Fi will continually transmit unauthorized messages in the covert channel. For example, Wi-Fi enabled Internet of Things (IoT) devices such as drones, IP cameras, and Digital Video Recorder (DVR) can be exploited as Ghost-Fi and transmit their sensing data to the adversary using the covert channels. The IoT devices often have vendor-specific firmware and hardware, but security testing or verification of them is not easy for everyday users. Then, the hardware exploitation and firmware compromising can lead to the establishment of covert channels [14], [15]. More seriously, even if the systems are physically separated or isolated, namely air-gapped networks, the covert channels can be used for information leakage [16].

We present Ghost-Fi Detector as a countermeasure system to mitigate the threat of modulation-based covert channel attacks. Since the adversary acts as a passive eavesdropper, it is hard to locate the adversary directly. Hence, Ghost-Fi Detector investigates the received signal from a suspicious transmitter and determines whether the covert channel exists or not. Our approach is based on the passive observation that the creation of a modulation-based covert channel has certain effects on the constellation map of the received signal. Then, the altered features of the modulation schemes provide a critical clue for detecting the covert channels.

The main challenge is that the detector has no prior information about the adversary’s modulation schemes of which component is being manipulated. Therefore, the detector should consider all the possibilities of the covert channels in the received signals. However, since each component brings separate manifestations for the radio signals, there is almost no general-purpose solution with a single detection mechanism. Furthermore, unwanted noise is always included during radio propagation, so the detector should correctly determine if there is a covert channel or common noise in the suspicious incoming signals. To detect any type of modulation-based covert channel without prior knowledge, Ghost-Fi Detector is composed of elaborately designed defense mechanisms based on Automatic Modulation Classification (AMC), frequency offset estimation, and Radio Frequency (RF) characteristics on the received signal, respectively.

First of all, we are motivated that the covert channels must have statistically biased noise values to send covert messages, whereas the common noise is assumed to follow Gaussian noise. We calculate high-order cumulants and wavelet
transform of the received signals. Since the receiver knows what modulation scheme is used to make the legitimate channel, the results should follow the theoretical cumulants. However, when the covert channels exist, the results would be different from the expected values. While general AMC techniques are used to classify unknown signals based on the distinct characteristics of known modulation schemes, we use the techniques to detect the existence of covert channels. Second, since Frequency Shift Keying (FSK) modulation is not effectively identified by AMC techniques, we estimate Carrier Frequency Offset (CFO) for each symbol. If any fluctuations occur in the CFO, we can determine that a CFO-based covert channel attack is detected. Third, we analyze RF characteristics such as Error Vector Magnitude (EVM), amplitude, and phase. If the variance values of the RF characteristic distributions deviate from predefined confidence interval, we determine that the received signal is suspicious. Finally, *Ghost-Fi Detector* concludes whether the covert channel is detected or not from the defense mechanisms.

The major contributions of this work are as follows.

- We focus on an emerging class of attack, termed *modulation-based covert channel attack*, where the attacker eavesdrops on unauthorized messages that are continually sent by the *Ghost-Fi*’s covert channel. Further, our attack models consider the real-world wireless network technology, Wi-Fi, and cover three aspects of the radio signal characteristics: amplitude, phase offset, and frequency offset, comprehensively.
- We design a countermeasure system, *Ghost-Fi Detector*. Since there is no dominant universal detection mechanism for the various modulation-based covert channels, our system consists of six effective defense mechanisms based on two AMC techniques, CFO estimate, and three RF characteristics-based methods, including distributions of EVM, amplitude, and phase.
- We implement three types of *Ghost-Fi* on software-defined radios and evaluate the performance of *Ghost-Fi Detector* in real-world scenarios. Through extensive experiments and simulations, our results show that *Ghost-Fi Detector* achieves an average hit rate of 95% with almost zero false positives.

The rest of the paper is outlined as follows. In Section II, we classify and discuss the existing covert channel techniques. We introduce our system model for the Wi-Fi signal and design the adversarial model in Section III. Section IV describes the details of modulation-based covert channel attacks that aimed at hiding covert messages in noise. In Section V, we present the defense mechanisms for *Ghost-Fi Detector*. Then, we evaluate and analyze the performance of our implementation in Section VI. Finally, we conclude our work in Section VII.

**II. RELATED WORK**

While the term *covert channel* was first used in 1973 [17], and the covert channels in wired and wireless computer communications have been studied comprehensively [11] and in each layer [18], the existing research on modulation-based wireless covert channels have received attention in just a few years.

In this section, we briefly introduce a survey on wireless covert channels applicable to Wi-Fi networks, in three aspects: i) *covert storage channels*, ii) *covert timing channels*, and iii) *modulation-based covert channels* as emerging covert channels. Besides, we discuss why the detection problem of modulation-based covert channels is crucial.

**A. COVERT STORAGE CHANNELS**

Covert storage channels allow the writing of shared objects by a sender and the reading of the object by a receiver [19]. Typically in Wi-Fi networks, the shared objects can be a portion of the Wi-Fi frames such as signal field, OFDM padding, and ACK frames [6], [9], [20].

Yang et al. [21] confirm that the on/off state of Wi-Fi transceiver can be controlled without permission, which can create a covert channel using Wi-Fi backscatter communications [22]. Subramani et al. [23] demonstrate that a malicious hardware trojan in Wi-Fi transceiver can build a covert channel by transmitting modified codewords which will be silently corrected by forward error correction of the legitimate receiver. Although these approaches are insightful, their covert channels can be easily detected by Wi-Fi transceivers with an automated monitoring mechanism.

**B. COVERT TIMING CHANNELS**

Covert timing channels allow a sender to modify its usage of resources over time so that a receiver can observe the usage to decode covert messages from the sender [19]. Traditionally, a sequence of frame inter-arrival times sent by a legitimate sender is modified by the covert channel sender to encode covert messages. Shah and Blaze [24] show that jamming a legitimate Wi-Fi channel creates a covert timing channel. Ogen et al. [25] extend the result from [24] by low-power micro-jamming from a commercial Wi-Fi device. Holloway and Beyah [10] propose a covert timing channel, which controls and modifies the random backoff of the Wi-Fi CSMA/CA mechanism. The channel is realized using off-the-shelf Wi-Fi devices in [26]. Kiyavash et al. [27] implement hardware malware by modifying the random backoff to leak covert messages. Sheikholeslami et al. [28] uses the number of packets transmitted in a time slot. In many cases, covert timing channels have low covert data rates due to the limited number of controllable timing parameters in Wi-Fi networks. Besides, the covert timing channels can be detected based on inter-packet delays [13], [29].

**C. EMERGENCE OF MODULATION-BASED COVERT CHANNELS**

With the emerging interest in the potential of the physical layer, many researchers present new threat models and secure communication methods using the properties of a radio signal [30], [31], [32], [33]. While the above research efforts for covert storage channels have focused on the modification
of bit-level states in Wi-Fi networks mainly, some recent studies move forward to the physical layer, e.g. symbol-level or signal-level states, by using different signal processing techniques. These approaches are motivated by an observation that for better reliability, the transmitters often choose lower-level modulation schemes in low-SNR environments, which makes the rooms for an extra capacity of the covert channels. Existing research efforts use the rooms to encode covert messages by modifying the properties of a radio signal such as amplitude [1], [4], [34], phase [35], [36], and frequency offset [37]. We call these types of covert channels modulation-based covert channels.

Shadow Wi-Fi [38] implements a practical physical layer covert channel on a commercial Wi-Fi chipset firmware by the deliberate change of a transmit filter, though it can embed only one covert symbol per frame. While its detection is relatively easy, the work shows the practical feasibility of adversarial modulation-based covert channels. Rahbari and Krunz [39] propose “P-modulation” to encode the covert bits into predefined preambles in the 802.11 systems. Another modulation-based covert channel is proposed in [1] with a high throughput of Mbps. The aforementioned research efforts mainly focus on the feasibility of the proposed covert channels. On the contrary, our work tries to detect the three types of modulation-based covert channels with our detection mechanisms in practical settings of Wi-Fi networks. We believe that our work can be also easily applicable to other OFDM-based wireless systems.

D. DETECTION OF MODULATION-BASED COVERT CHANNELS

While the focuses of the existing studies are in introducing novel covert channels by manipulating the physical-layer characteristics of radio signals, the methods used by the authors are closely related to the attack models presented in this paper. Since the modifications of radio signals are removed in the decoding process at the physical layer, it is very hard to recognize them by the existing detection methods. To improve this, we introduce two detection mechanisms for the physical layer covert channels theoretically [42]. However, the methods are based on decoding errors that the attacker does not want to cause and do not encompass practical implementation such as OFDM frames in Wi-Fi networks. Further, frequency-shifted covert channels are not considered in their attack models. In [1] and [35], the distributions of EVM and amplitude are proposed as the evidence of covert channels, however, no specific countermeasures are proposed. Besides, the applicability of the distributions to various covert channels is not investigated.

Figure 2 shows the three types of covert channels in IEEE 802.11. The modulation-based covert channel can embed as many bits as the number of data bits transmitted, whereas other types of covert channels contain only a few bits per a single frame. When the transmitter transmits a frame containing a lot of data bits, the number of covert bits increases, and the threat increases as well. Fortunately, the detection of the covert storage and timing channels is relatively easy to detect since the analysis of the arrival time of the packet through the timestamp and the analysis of the bits contained in the header which are also small parts of the frames. On the contrary, modulation-based covert channels embed their bits on the data fields (i.e., OFDM symbols) which occupy most of the frame.

III. SYSTEM MODEL

In this section, we describe the signal model for covert channels in OFDM that our detection system should capture. We also introduce the adversarial model which defines the capabilities of the adversary on the signals.

A. SIGNAL MODEL

Suppose that the symbols in the digital input sequence of n-th subcarrier \( w_n(kT) \) with a symbol period \( T \) is turned into the analog pulse \( w_{a,n}(t) \) as follows:

\[
w_{a,n}(t) = \sum_{k=1}^{K} w_n(kT) \delta(t - kT) = \begin{cases} 
  w_n(kT) & t = kT \\
  0 & t \neq kT
\end{cases}
\]

where \( \delta(\cdot) \) is the Dirac delta function. In Wi-Fi networks, especially in 802.11a/g, we use 48 data subcarriers, 4 pilot subcarriers, and 12 null subcarriers among total \( N = 64 \) subcarriers. To create the covert channels, Ghost-Fi slightly changes the constellation value of \( w_n(kT) \). The details are given in Section IV.

The OFDM block with \( K \) transmitted complex data symbols is represented as:

\[
s(t) = e^{j2\pi f_s t} \sum_{n=0}^{N-1} w_{a,n}(t) \otimes p(t)e^{j2\pi f_n t}, \quad 0 \leq t \leq KT
\]
where $r^2 = -1$, $N$ denotes the number of subcarriers, $f_c$ and $f_f$ are the carrier frequency and subcarrier frequency of the $n$-th subcarrier, $p(t)$ is the transmit pulse shape, and $\otimes$ is the convolution, respectively. For 802.11a/g, the OFDM block consists of 64-point Inverse Fast Fourier Transform (IFFT) and 16 CP samples added to the front. Then, the transmitted signal passes through propagation channels to the receiver. After down-conversion, the baseband received signal can be represented as:

$$r(t) = a e^{i 2 \pi (f_{\text{CFO}} - f_{\text{f}}) t + \theta} s(t) \otimes h(t) + \omega(t)$$  \hfill (3)

where $f_{\text{CFO}}$ is the carrier frequency offset, $\theta$ is the time-invariant phase shift, $h(t)$ is the channel impulse response, and $\omega(t)$ is a baseband complex noise.

At the receiver’s side, the demodulated symbols $\hat{w}_n(kT)$ are obtained from the received signal $r(t)$ with the receive filter $g_{n,k}(t)$:

$$\hat{w}_n(kT) = \int_{-\infty}^{\infty} r'(t) g_{n,k}^*(t) dt$$  \hfill (4)

where $r'(t)$ is the CFO corrected version of the received signal with the CP removed, $(\cdot)^*$ denotes the complex conjugate operation, and $g_{n,k}(t) = g(t - kT) e^{i 2 \pi f_{\text{f}}(t - kT)}$, which is a time-frequency shifted version of the received pulse $g(t)$.

In short, a generic OFDM symbol is transmitted with pulse-shaping as Eq. 2, passed through propagation channels and down-conversion as Eq. 3, and demodulated as Eq. 4.

### B. ADVERSARIAL MODEL

Our adversarial model posits that maliciously manufactured devices such as drones, IP cameras, and DVR can be installed and act as Wi-Fi transmitters to provide their service. Then, each device roles as Ghost-Fi which is compromised by an attacker and has a modified modulation scheme, as detailed later in Section IV. The attacker can use an ill-defined Wi-Fi chip and firmware [43]. The malware also be used for unauthorized modifications of modulation schemes in software-defined radio systems [44]. Once an adversarial device is in the vicinity of the compromised device, it can encode the covert channel in the transmitted signals and store the acquired information. For example, a user deploys Wi-Fi enabled cameras or drones for surveillance of the surroundings, a compromised drone can be used to live stream illegitimate videos over the covert channels. Even worse, it is challenging to detect the compromised device because the legitimate channel behaves as usual. We summarize the capabilities of the adversary as follows:

- **Locate ($A$)**: The adversary $A$ is always aware of the existence of Ghost-Fi and can be located wherever he can listen to the signals from Ghost-Fi. Note that $A$ acts as a passive eavesdropper who does not emit any radio signals.

- **Hide ($C, m_c$)**: A covert message $C$ is encoded with a modulation scheme $m_c$ by manipulating the signal characteristics such as amplitude, phase offset, and frequency offset. Ghost-Fi can choose any $m_c$ to hide a covert message $C$ with this capability.

- **Receive ($m_p, m_c$) $\rightarrow$ $S$**: The adversary always observes the radio channel of Ghost-Fi and receive a signal $S$ modulated by a legitimate modulation scheme $m_p$ with a modulation scheme for covert channels $m_c$.

- **Decode ($S, m_c$) $\rightarrow$ $C$**: This function models the adversary’s ability to obtain a covert message from the signal $S$ using the previously known modulation scheme $m_c$.

- **Configure ($m_c, \{P_1, P_2, \ldots, P_I\}$)**: By default, in order to conceal the modulation scheme $m_c$, Ghost-Fi attempts to remain invisible and to achieve desirable resolution by using various parameters $\{P_1, P_2, \ldots, P_I\}$.

### IV. MODULATION-BASED COVERT CHANNEL ATTACK MODELS

We provide three concrete attack models which our detection system has to distinguish from the legitimate channels. In general, radio signals have three components: amplitude, phase, and frequency. Based on the techniques of existing covert channels, an adversary manipulates one of the components such as amplitude [1], [4], [34], phase [35], [36], and frequency offset [37]. To include additional covert symbols in the radio signals, it is necessary to use a modulation scheme with a low baud rate as a legitimate channel. In the following models, we use the room between the actual capacity of Quadrature Phase Shift Keying (QPSK) and the theoretical maximum capacity to encode the covert symbols, when the QPSK modulation scheme does not fully utilize the Shannon capacity, the theoretical limit of the channel capacity.

### A. PSK-BASED COVERT CHANNEL ATTACK

In this attack, we focus on phase information of each QPSK constellation point. First, a legitimate message is modulated with QPSK. Afterward, a covert message is modulated also using one more QPSK from each point, which is shown in Fig. 3 (a). Therefore, the constellation point of the legitimate symbol is relocated to one of the four points of covert QPSK, keeping the origin at its original location. We refer to the modulation scheme as Double PSK (DB-PSK). Fig. 3 (a) shows the I/Q plane of the DB-PSK covert channel in the ideal case (left) and the actual experiment (right). If the legitimate message $11\text{1}$ is to be sent, one of the four distinct points on the first quadrant is chosen according to the covert symbols to be transmitted.

Attackers can be brought to account in our scenario by leveraging the signal model introduced in Section III. Assuming that a covert symbol is modulated by DB-PSK, the analog pulse of the covert symbol is considered in our signal model as follows. Note that the updated $w_{\alpha,n}(t)$ value, $w_{\alpha,n}^{DB-PSK}(t)$, only applies to the subcarriers that carry covert symbols. The percentage of covert subcarriers can be controlled at the
implementation stage.

\[
w_{a,n}^{\text{PSK}}(t) = \sum_{k=1}^{K} \left( w_n(kT) + b_n \frac{1}{\sqrt{2}} e^{j \frac{2 \pi n (t + 1)}{4}} \right) \delta(t - kT) = w_{a,n}(t) + b_n \frac{1}{\sqrt{2}} e^{j \frac{2 \pi n (t + 1)}{4}} \tag{5}\]

where \(m(t)\) is an integer value that depends on the covert messages to be transmitted at time instance \(t\), which in this case is chosen among \(\{0, 1, 2, 3\}\). The constant \(\frac{1}{\sqrt{2}}\) is the distance between the constellation point of the legitimate symbol and the covert symbol which is used to configure \(m_{\text{DB-PSK}}, d = \frac{1}{7}\) from the distance of a 64-QAM constellation, \(e^{j \frac{2 \pi n (t + 1)}{4}}\) is a corresponding phase shift, and a binary \(b_n \in \{0, 1\}\) means whether the \(n\)-th subcarrier is used for covert channel or not. The resulting signal shown in Eq. 2 is still valid since the new covert pulse is transmitted in exactly the same process as the legitimate pulse.

### B. DIFFERENTIAL AMPLITUDE-BASED COVERT CHANNEL ATTACK

Similar to the ASK modulation scheme, covert messages can be encoded with different power levels in the PSK modulation scheme. In this attack, a covert message is embedded by decreasing the amplitude of the legitimate symbol as several levels. We refer to the attack as Differential Amplitude PSK (DA-PSK), because the shifted amplitude conveys covert messages. Considering the decision boundaries of QPSK modulation, only the phase offset of received signal influences the demodulation results, whereas the amplitude shifts do not have any effects. Hence, DA-PSK enables covert message transmission between Ghost-Fi and eavesdroppers while legitimate receivers would only demodulate legitimate data without suspicion. Fig. 3 (b) demonstrates how a legitimate constellation point is shifted towards the origin, depending on the covert messages in the ideal case (left) and the experiment (right). The linear arrangement of the four constellation points indicate the identical transmitting legitimate symbol. The distance between the origin and each constellation point distinguishes embedded a covert symbol.

We again leverage the signal model in Section III to show how DA-PSK affects the analog pulse as follows:

\[
w_{a,n}^{\text{DA-PSK}}(t) = \sum_{k=1}^{K} (w_n(kT) - b_n dm(kT) w_n(kT)) \delta(t - kT) = (1 - b_n dm(t)) w_{a,n}(t) \tag{6}\]

where \(b_n\) is a binary value that means whether the \(n\)-th subcarrier is used for covert channel or not, \(m(t)\) is an integer corresponding to the covert message within range \([0, 3]\) at time instance \(t\), and \(d\) is the unit of amplitude variation, i.e., \(dm(t)\) is the resulting decrease in amplitude of legitimate symbol. With the lower value \(d\), the covert channel mimics normal signals better. From the distance between two diagonally adjacent constellation points in 64-QAM, we select \(d = \frac{2}{7}\), which is the minimum distance between two covert constellation points. Furthermore, we also use \(d = \frac{2}{7}\) from 128-QAM for high SNR environments, i.e., configure \(m_{\text{DA-PSK}}, d \in \left\{\frac{2}{7}, \frac{2}{11}\right\}\).

### C. ARTIFICIAL CFO-BASED COVERT CHANNEL ATTACK

In this attack, the carrier frequency of the transmitted signal is shifted to include a covert message with an injected CFO value, allowing the eavesdropper to demodulate the covert channel with an FSK modulation scheme. The legitimate receivers will automatically correct the frequency offset without realizing the existence of the covert channel [45]. Fig. 3 (c) provides the visual where a legitimate Wi-Fi signal is shifted to produce covert symbols. The adversary can detect the intended CFO to demodulate covert messages. We name this attack A-CFO after the artificial CFO. Since the artificial CFO is inserted just before mixing the signal with carrier frequency \(f_c\), we can slightly modify the transmitting signal.
model in Eq. 2, instead of the analog pulse model in Eq. 1, as follows.

\[ s^{A-CFO}(t) = e^{2\pi i (f_{c} + m(t))t} \sum_{n=0}^{N-1} w_{a,n}(t) \otimes p(t)e^{2\pi f_{a}t} \] (7)

where \( m(t) \) is either 1 or -1 because A-CFO conceptually utilizes binary FSK. Note that, in this attack, we do not apply the covert channel to individual subcarriers but to the entire carrier frequency. In this case, \( f_{a,CFO} \) should be restricted to preserve the legitimate channel. For our implementation, the legitimate receiver cannot decode the packet with \( |f_{a,CFO}| \geq 50 \text{ kHz} \). According to [46], CFO over 600 kHz hinders the legitimate decoding. However, the target signals have consistent CFO for the entire packet, whereas our implementation includes OFDM block-wise COFos, which require more stringent restrictions. Thus, we select the size of \( f_{a,CFO} \) as 5 kHz or 10 kHz which is tight enough to preserve the legitimate channel, i.e., configure \( m^{A-CFO}, f_{a,CFO} \in \{5k, 10k\} \).

V. DETECTION SYSTEM DESIGN

We suggest six defense mechanisms in our system design to detect the existence of Ghost-Fi. The solution designs are based on two AMC methods, CFO estimate, and three other RF characteristics. The defense mechanisms construct a countermeasure system Ghost-Fi Detector as shown in Fig. 4. We implement two integration methods, one using a Support Vector Machine (SVM) [13], [47] and the other using an OR gate. The following are the details of the components for Ghost-Fi Detector.

A. AUTOMATIC MODULATION CLASSIFICATION

We derive two solutions from AMC which provides a classifier for given unknown signals [48]. Particularly, we are motivated that the covert channel will have distinguishable statistical features since the attacker and Ghost-Fi must share specific encoding/decoding rules for covert channels. AMC does not require any prior information about the given signal, such as the signal power, frequency offset, phase offset, timing offset as well as unknown data symbols. Among the AMC methods, we adopt cumulant-based and Continuous Wavelet Transform (CWT) approaches. These methods are feature-based methods with lower complexity, whereas other likelihood-based methods provide optimal solutions but suffer from high computational complexity to solve optimization problems. While the original feature-based methods are used to classify unknown signals with the characteristics of known modulation schemes, our system uses the features to detect the existence of covert channels.

1) CUMULANT-BASED DETECTION MECHANISM

Rather than the typical AMC algorithm, we use additional information to detect covert channels, such as ideal constellation and signal power. Since Ghost-Fi does not want to affect the demodulation process of the legitimate channel, we can use the theoretical cumulant for a given modulation scheme [49], [50]. Our detection mechanism computes high-order cumulants for the received signal and determines if the constellation is indeed obtained by the given modulation scheme. If the received signal has a covert channel, then the estimated cumulants will be different from the theoretical cumulants. We use high-order cumulant-based features where \( C_{i,j}(r) \) is the \( i \)-th order cumulant with \( j \) conjugated components for received samples \( r[k] \). Using the samples, the second-order cumulants are given by

\[ C_{2,0}(r) = \frac{1}{K} \sum_{k=1}^{K} r^{2}[k], \quad C_{2,1}(r) = \frac{1}{K} \sum_{k=1}^{K} |r[n]|^{2}. \] (8)

The fourth-order cumulants can be expressed using the following joint cumulant function,

\[ \text{cum}(w, x, y, z) = E(wxz) - E(wx)E(zy) - E(wy)E(xz) - E(wz)E(xy) \] (9)

where \( w, x, y, \) and \( z \) are zero mean random variables. For the received samples, we calculate the forth-order cumulants using Eq. 9 as follows.

\[ C_{4,0}(r) = \frac{1}{C_{2,1}^{2}} \left( \frac{1}{K} \sum_{k=1}^{K} r^{4}[k] - 3C_{2,0}(r) \right) \]

\[ C_{4,1}(r) = \frac{1}{C_{2,1}^{2}} \left( \frac{1}{K} \sum_{k=1}^{K} r^{3}[k]r^{*}[k] - 3C_{2,0}(r)C_{2,1}(r) \right) \]

\[ C_{4,2}(r) = \frac{1}{C_{2,1}^{2}} \left( \frac{1}{K} \sum_{k=1}^{K} |r[k]|^{4} - |C_{2,0}(r)|^{2} - 2C_{2,1}^{2}(r) \right) \] (10)

where \( 1/C_{2,1}^{2} \) normalizes the cumulants and removes scale problems. Since we use ideal constellation for QPSK modulation, \( C_{2,0} = 0 \), and \( C_{2,1} = 1 \) (i.e., signal power). With the equal symbol probability, the forth-order cumulants are calculated by \( C_{4,0} = -1, C_{4,1} = 0, \) and \( C_{4,2} = 1 \).
The CWT of the received signal and detect the existence of covert channels, especially using Continuous Wavelet Transform (CWT). The properties of the signal in time and frequency domains, approaches have the distinctive capability to precisely extract various unknown modulation-based covert channel attacks.

### 2) CWT-BASED DETECTION MECHANISM

Among the feature-based (FB) algorithms, wavelet-based approaches have the distinctive capability to precisely extract the properties of the signal in time and frequency domains, especially using Continuous Wavelet Transform (CWT). We use the CWT-based FB algorithm [51] to analyze the received signal and detect the existence of covert channels. The CWT of the received signal $r(t)$ is defined as

$$\text{CWT}(a, \tau) = \int r(t)\psi^*_a,\tau(t)dt,$$

(11)

where $a > 0$ is a scale variable, and $\tau$ is a translation variable.

To express the received signals as a complex envelope, we adopt Shannon wavelet as a mother wavelet. Since Shannon wavelet is known for its infinite differentiability, analytical expressions, and shapely boundlessness in the frequency domain, it is expected that it will be able to show the highest detection performance in our goals. The mother wavelet is defined as

$$\psi(t) = \sqrt{B}\frac{\sin(\pi Bt)}{\pi Bt}e^{2\pi f_c t},$$

(12)

where $B$ is the bandwidth, and $f_c$ is the center frequency. The mother wavelet provides a scaled and translated version of the wavelet called baby wavelet, which is generating $\psi_{a,\tau}(t)$ as follows:

$$\psi_{a,\tau}(t) = \frac{1}{\sqrt{a}}\psi\left(\frac{t-\tau}{a}\right).$$

(13)

Let the received signal $r(t)$ be presented as

$$r(t) = \tilde{r}(t)e^{j(2\pi f_c t + \theta)},$$

(14)

where $0 \leq t \leq T$, $\theta$ is the carrier initial phase, and $\tilde{r}(t)$ is the baseband complex envelope of the signal $r(t)$, defined by

$$\tilde{r}(t) = \sum_{i=1}^{N}(A_i + jB_i)e^{j(f_i t + \phi_i)}g(t - iT),$$

(15)

where $(A_i, B_i)$ are the $i$-th symbols, $N$ is the number of observed symbols, $g(t)$ is the pulse shaping function of symbol duration $T$, and $f_i \in \{f_1, f_2, \ldots, f_N\}$ is the signal frequency at the $i$-th symbol. By taking the amplitude of the $i$-th symbol as $S_i = \sqrt{A_i^2 + B_i^2}$ and the signal $r(t)$ into CWT form, we can extract the transient characteristics of the received signal. Since the characteristics are all distinctive to each modulation technique, this mechanism can detect the existence of a covert channel by comparing these distinctive characteristics. In Fig. 6, we plot the result of the CWT-based detection over non-covert, A-CFO, DA-PSK, and DB-PSK frames with the 100% occupancy of covert subcarriers. The result shows noticeable differences between the covert and non-covert channels with the wavelet transform. Meanwhile, the CWT values of DB-PSK frames have similar results to the values of non-covert frames.

### B. CFO ESTIMATE DISTRIBUTION ANALYSIS

We introduce a new defense mechanism that captures the intrinsic characteristics of the CFO-based covert channels. The mechanism can effectively detect the presence of the CFO-based covert channel by statistically analyzing a distribution of corrected CFO estimates. To establish a CFO-based covert channel, an attacker should inject a specific size of artificial CFO corresponding to each OFDM symbol duration. Our key observation is that the sign-changing of artificial...
CFO value is inevitable to embed the covert bits. In the case of the non-covert channel, these changes are not relatively frequent. Accordingly, the variance of the distribution would be moderate in a specified time window. On the contrary, for a CFO-based covert channel, the sign of CFO estimate value would change frequently, and the distribution would likely appear with significant variance. To this end, we capture this inherent property of the CFO-based covert channel and reflect it into the detection mechanism design to detect the covert channel.

At the receiving chain, the legitimate receiver calculates a CFO estimate by collecting a specified number of the received samples. Each calculated estimate is applied to correct the CFO of received frame and immediately discarded since it is not needed for remaining decoding process [45]. Though a CFO-based covert receiver, proposed in [37], uses a decoding technique to extract covert bits by using a shared CFO value from the attacker’s point of view, our mechanism should detect the covert channel from the viewpoint of the detector without prior knowledge of the CFO value.

Now, we look into the CFO correction procedure to how the mechanism utilizes the complete symbol-wise CFO estimate. In the receiver, an incoming signal \( \hat{r}^{A-CFO}(t) \) is down-converted and observed as follows:

\[
e^{-j2\pi f_{CFO} t} \cdot \hat{r}^{A-CFO}(t)
= e^{j2\pi (f_{CFO} + m(t)f_{a-CFO})t} \cdot B(t),
\]

where \( f_{CFO} \) is the true CFO originated by nature and \( B(t) \) represents the baseband time-domain transmit signal. Since a legitimate receiver does not know about the artificial CFO, \( m(t)f_{a-CFO} \), it tries to cancel out the entire \( f_{CFO} + m(t)f_{a-CFO} \) as if it is the true CFO. Our goal is to follow this correction procedure and harness the complete symbol-wise CFO estimate to observe its distribution. Based on the typical CFO correction procedure of the receiver, we can express a complete CFO estimate \( \hat{f}_{CFO,n} \) for the \( n \)-th OFDM symbol by keeping three intermediate components as follows:

\[
\hat{f}_{CFO,n} = \hat{f}_{ST} + \hat{f}_{LT} + \hat{f}_{r,n},
\]

where \( \hat{f}_{ST} \) is a coarse CFO estimate which can be directly derived from a short-training sequence, \( \hat{f}_{LT} \) is a fine CFO estimate calculated from a long-training sequence, and \( \hat{f}_{r,n} \) is a symbol-wise residual CFO estimate of the \( n \)-th OFDM symbol obtained by using pilot symbols. If the Wi-Fi frame is successfully decodable by a normal receiver, then we can expect that \( \hat{f}_{CFO,n} \) will be very close to the value of \( f_{CFO} + m(t)f_{a-CFO} \) (i.e., the difference between these two would be negligible). That is, the CFO estimate sufficiently reflects the frequent fluctuations of \( m(t)f_{a-CFO} \) injected by the attacker.

In Figure 7, we plot the result of the CFO estimate distributions of covert channels with different injected A-CFO size and the non-covert channel. With the estimated probability density, the mechanism finds out whether the covert channel exists or not. For a non-covert channel, the fluctuation of the CFO estimate is moderate. On the other hand, in the presence of injected A-CFO, the CFO estimate value would show frequent sign changes, and it thrashes significantly from side to side across the origin. This results in recognizable abnormal increase of the variance which may indicate the presence of a CFO-based covert channel. As the A-CFO value increases, the variance of the corresponding distribution also increases. There are noticeable differences when the A-CFO value is injected with the size of 100 kHz and 1 MHz, but the legitimate channel cannot be maintained because the frame cannot be recognized at the legitimate receiver [46]. It is worth noting that the attacker who wants high reliability needs to increase the A-CFO size, but he also should take the high risk of being detected.

C. RADIO FREQUENCY CHARACTERISTICS ANALYSIS

Alongside the methods introduced above, we also implement three analysis methods that rely on the RF characteristics of the received signal [52]. These approaches are based on the insight that the covert channel distorts RF features of the received signal. First, we use the Error Vector Magnitude (EVM). By definition, EVM is computed by calculating the distance between the constellation point of the received subcarrier and the ideal point. Then, for covert channels, the EVM will be larger than for non-covert channels. The existing study also implicates the EVM as an evidence of covert channels [35].

Other features are amplitude and phase variance in incoming frames. We cluster the amplitude variance and phase variance. Note that QPSK modulation scheme has a uniform amplitude but four different phase values \((\pi/4, 3\pi/4, 5\pi/4, \text{and } 7\pi/4)\). Thus, amplitude variance values are clustered as a whole, and phase variance values are clustered according to the quadrant. If the amplitude variance computed from an arbitrary frame is outside the confidence interval computed from the normal signal, the frame is considered to have a covert channel. In [1], the distribution of amplitude is used to indicate the presence of the amplitude-shifted covert channels. Similarly, if the phase variance of any quadrant lies outside the confidence interval computed from the normal signal, the frame is also considered to have a covert channel.
Algorithm 1: Detection Algorithm for Each Defense Mechanism

**Input**: frame /* incoming frame */
**Result**: result /* Boolean result */
**Parameters**: m_type, interval_min, interval_max /* a type of defense mechanism and values for confidence interval */

```plaintext
result ← False;
frame_freq_d ← FFT(frame);
Eq_frame ← WiFi_frame_equalizer(frame_freq_d);
if m_type ∈ {cumulant, CWT, EVM, phase, amplitude}
then
    d_metric ← Calc(m_type, Eq_frame);
    /* Metric calculation for each mechanism */
    if (d_metric[i] < interval_min or d_metric[i] > interval_max) then
        result ← True;
    end if
else
    d_metric ← Calc(m_type, frame);
    /* CFO estimate calculation */
    if (d_metric < interval_min or d_metric > interval_max) then
        result ← True;
    end if
end if
return result;
```

D. DETECTION ALGORITHM

Algorithm 1 shows the detail on the detection algorithm for the above defense mechanisms. In the algorithm, each mechanism is supposed to have its confidence interval.

To estimate the confidence interval, each mechanism needs a training phase before deployment in Ghost-Fi Detector system. In this phase, a detector receives hundreds of legitimate frames to make t-distributions of the signal characteristics such as cumulant, CWT, CFO, etc. The frames are transmitted by other devices at different distances with pseudo-random bits. Then, to detect the covert channels, they use hypothesis testing with the t-distributions. Note that the t-distribution is used to construct the confidence interval for the true mean with a set of observations. To make a decision, each mechanism detects whether its metric is outside the predefined confidence interval for an arbitrary frame input.

For each mechanism, we use different parameters for the confidence intervals. The parameters are determined in the training phase with legitimate 802.11 frames. More precisely, for the cumulant-based mechanism, we define the significance level as 0.1, which shows the best distinguishability over significance levels. It then performs a two-tailed test to detect if there is a covert channel in the received frame when the cumulant metric falls outside the confidence interval. Besides, for the CWT-based, CFO estimate, and other RF characteristics-based mechanisms, we empirically set the significance levels as 0.05 where \( \alpha \in \{0.1, 0.05, 0.01\} \).

Our detection mechanisms work with the standard Wi-Fi decoder. As shown in Fig. 4, the received frame is corrected by the Wi-Fi frame equalizer and investigated by the proposed detection mechanisms. Thus, the algorithm calculates decision metrics of the received frame after FFT and equalization in lines 2-5. On the other hand, CFO estimate detection mechanism does not require the equalization process as shown in the code at lines 10-11. In lines 6 and 12, the algorithm has two-tailed tests with the confidence interval. Then, if the metric falls outside the interval, it returns true to indicate that there is a covert channel in the frame.

VI. PERFORMANCE EVALUATION

In this section, we evaluate our detection system described in Section V. We provide the results of extensive real-world experiments and simulations to show that our Ghost-Fi Detector can effectively track down the embedded modulation-based covert channel attacks.

A. IMPLEMENTATION

We implemented the physical layer of Wi-Fi and added an extension to generate each covert channel described in Section IV at the Wi-Fi transmitter and receiver upon [53]. In the experiments, we built our system based on two USRPs as shown in Fig. 8 (a). One USRP plays the role of Ghost-Fi Detector to detect unknown covert channels in incoming frames. Among the attack models, DB-PSK and DA-PSK support embedding covert symbols into 30%, 50%, and 100% OFDM subcarriers, whereas A-CFO cannot support it due to its basis. We configure the distance between the legitimate symbol and the covert symbol in DB-PSK as 64-QAM, the distances in DA-PSK as 64-QAM and 128-QAM, and the artificial CFO size in A-CFO as 5 kHz and 10 kHz. Since our target attack models are based on QPSK modulation, our implementation is also based on QPSK with a 3/4 code rate.

We placed Ghost-Fi Detector in the marked locations L1-L6 in Fig. 8 (b) with Line-of-Sight (LoS) and Non-LoS (NLoS) scenarios. Each experiment result at a single location is an average of 1200 runs. To mitigate the interference from the dense Wi-Fi systems, i.e., signal collisions, each experiment is conducted at 2.504 GHz using 20 MHz bandwidth. Both legitimate messages and covert messages are generated randomly, and all frames used in the experiments were successfully decoded into legitimate messages at the Wi-Fi receiving chain.

B. EXPERIMENTAL RESULTS

Before we provide the results, we briefly denote several performance metrics for evaluating our Ghost-Fi Detector.
Here, the term True Positive (TP) and True Negative (TN) are defined as the number of successful detection for a covert channel and normal case respectively. Besides, False Positive (FP) is the number of faulty detection indicating a normal case as a covert channel, and False Negative (FN) is the number of detection failure that the detector fails to recognize a presence of covert channel. Further, we define hit rate as $\frac{TP}{TP+FN}$ and False Positive Rate (FPR) as $\frac{FP}{FP+TN}$, respectively.

1) PERFORMANCE OF EACH DEFENSE MECHANISM

In Fig. 9, we plot the hit rate for each defense mechanism to show how well each method captures the covert channels in an LoS scenario.

a: CUMULANT-BASED DETECTION MECHANISM

This method is a powerful detector to the DA-PSK covert channels. On the other hand, DB-PSK and A-CFO covert channels are poorly detected. It is because that the cumulant value is more sensitive to amplitude than to phase jitter and CFO. The cumulant metric of the $N$-PSK ($N > 4$) modulation scheme is also invariant to the number of $N$ [50].

b: CWT-BASED DETECTION MECHANISM

This mechanism shows superior detection hit rates. The DA-PSK covert channels are perfectly detected at all experiment distances, and DB-PSK covert channels are also detected close to 50%. Although CWT gets high detection rates to DA-PSK and DB-PSK at 1 m, hit rates for DB-PSK at other distances show some degradation. When the SNR between Ghost-Fi and the Detector is lowered, the DB-PSK signal shows the same transient characteristic as the normal Wi-Fi signal in the time domain. This exhibits that the CWT-based detection mechanism works powerfully in the vicinity and ensures that the detection of all DA-PSK frames and many DB-PSK frames at further distances.

c: CFO ESTIMATE DISTRIBUTION ANALYSIS

The equalization process of the Wi-Fi receiving chain corrects the CFO, making it difficult to detect the A-CFO covert channels with other detection mechanisms. To this end, this mechanism uses pre-equalization data and shows a high detection rate for the A-CFO covert channels. This implies that, with the incorporation of different detection mechanisms, analyzing the CFO estimate distribution would be quite useful for the integrated Ghost-Fi Detector.

d: EVM AVERAGE ANALYSIS

This method detects the DA-PSK covert channels with high probability due to high EVM anomalies induced by the explicit amplitude shifts. Meanwhile, the DB-PSK covert channels are rarely detected since it has small EVMs where the covert symbols are scattered nearby around the legitimate symbol. Therefore, the non-covert symbols and DB-PSK symbols have a similar distribution for the ideal symbols.

e: AMPLITUDE VARIANCE ANALYSIS

It shows promising results for the DA-PSK covert channels at all distances due to the same reasons as in the case of EVM average analysis. The A-CFO and DB-PSK covert channels are also detected through additive changes of amplitude by...
the remaining CFO and the embedded symbols in DB-PSK, respectively.

**f: PHASE VARIANCE ANALYSIS**
The method shows fair hit rates for the covert channels, but it does not show impressive performance. Nevertheless, it can also be used to complement the integrated *Ghost-Fi Detector*.

The results from experiments show that there is no dominant universal detection mechanism to detect all attack models. Therefore, we incorporate the defense mechanisms to combat various unknown modulation-based covert channel attacks.

2) PERFORMANCE OF INTEGRATED GHOST-FI DETECTOR

Fig. 10 shows the FPR of each detection mechanisms and the integrated system, *Ghost-Fi Detector*. We confirm that all detection mechanisms achieve FPR less than 10%, and our proposed *Ghost-Fi Detector* shows a moderate FPR under 20%. Since *Ghost-Fi Detector* integrates all the six defense mechanisms in a parallel manner with an OR gate, it is more likely to give positive calls than each defense mechanism by observing manifestations that may indicate the presence of covert channels, hence, FPR increases slightly. To alleviate the FPR, we show the performance when the system uses multiple frames as input for the detection process instead of a single frame. As shown in Fig. 13 (a), the approach reduces the FPR dramatically.

**a: IMPACT OF INTEGRATION METHODS**

How to integrate the results of the detection mechanisms has a significant impact on the performance. For the final decision of *Ghost-Fi Detector* in Fig. 4, we implement two integration methods, an SVM and an OR gate. The performance of each integration method is as shown in Fig. 11. For the SVM, different numbers of training frames are used. SVM 1 (SVM 2) uses 100 (50) frames each for a non-covert channel and three types of covert channels for training. In Fig. 11 (a), we observe better FPR in the SVMs than in the OR gate. This is because a small number of positive calls in the SVMs give negative results while a single positive call of each mechanism gives positive results in the OR gate. Conversely, in Fig. 11 (b), SVMs show slightly reduced hit rates. This is also because a small number of positive calls are neglected by the SVMs. However, it is worth noting that the SVMs are trained with the previously defined attack models. Since *Ghost-Fi Detector* is designed to detect any type of modulation-based covert channel without prior knowledge, the training for the SVM is not suitable. Thus, the OR gate is adopted as the integration method for this work.

**b: IMPACT OF GHOST-FI PARAMETERS**

In Fig. 12 (a), we plot *Ghost-Fi Detector*’s hit rate versus each 30%, 50%, and 100% occupancy of covert subcarriers at 1 m in an LoS scenario. Since the DB-PSK covert channels with 30% subcarriers have little effect on the legitimate signal, they are not detected perfectly. Fig. 12 (b) shows the *Ghost-Fi Detector*’s hit rate versus distance between the transmitter and the receiver, 1 m, 2 m, and 3 m each. It shows that the hit rate of A-CFO is slightly reduced at 3 m while the detection rate of other covert channels is maintained. Fig. 12 (c) shows the hit rate of *Ghost-Fi Detector* for each DA-PSK distance of 64-QAM and 128-QAM. The experiments are conducted on the condition that only 30% of subcarriers are used for covert channels. This condition provides the most difficult situation...
for Ghost-Fi Detector to recognize DA-PSK covert channel. Nevertheless, all DA-PSK covert channels are detected for all distances. Fig. 12 (d) illustrates the Ghost-Fi Detector’s hit rate for each injected artificial CFO size of 5 kHz and 10 kHz across the transmission range. Again, we can confirm that analyzing CFO estimate distribution can be helpful when it incorporates with other defense mechanisms as the integrated detection framework.

**c: GHOST-FI DETECTOR WITH MULTIPLE FRAMES**

As shown in Fig. 10, the current Ghost-Fi Detector has a non-negligible FPR. However, the FPR is only the result of using a single frame. Motivated by the principle of the wisdom of crowds, the performance of Ghost-Fi Detector can benefit from multiple frames before declaring the existence of the covert channel. Instead of relying on a single frame, Ghost-Fi Detector can use multiple frames as input for the detection process with a window-based voting mechanism. If the decision of our system hits the ground truth $k$ times over consecutive $N$ frames, it can dramatically reduce the false positive rate with a proper threshold like $\frac{k}{N} \geq \eta = 0.8$.

In Fig. 13 (a), we see that Ghost-Fi Detector performs much better with multiple frames than a single frame. In particular, with five frames, the FPR is close to zero in the transmission range. Besides, as shown in Fig. 13 (b), the hit rate is maintained at 1 m as over 95%. On the other hand, with Kerckhoffs’s assumption, the adversary can choose to encode the covert messages into $l$ frames periodically over $N$ window size, where $l$ is less than $k$. Then, Ghost-Fi Detector can use randomly varying $N$ instead of a static value, which makes it more difficult to hide the covert channel.

**d: DETECTION RELIABILITY WITH DIFFERENT ENVIRONMENTS**

Finally, we present the hit rate and FPR of Ghost-Fi Detector ($N = 5, k = 4$) in different locations and environments in Fig. 14. The location settings L1-L6 correspond to the experiment setting in Fig. 8, and S1-S3 denote simulation environments where the SNR is 15 dB, 20 dB, and 25 dB, respectively. Again, we emphasize that QPSK modulation does not fully utilize Shannon capacity, and most covert channel design strategies take advantage of this room. Note that we employ the distance between legitimate symbol and covert symbol as $\frac{d}{7}$ which makes the same distance between two constellation points in the 64-QAM modulation scheme. When SNR is 15 dB, the Packet Error Rate (PER) of 64-QAM will be close to one [54]. Thus, for the adversary, S1 with 15 dB SNR is the worst condition to eavesdrop on the covert channels. In other words, the attacker also should be in proximity to the transmitter for decoding the covert messages. Nevertheless, for all experiment settings including the simulation environments, Ghost-Fi Detector achieves an average hit rate of 95% with almost zero false positive rates for arbitrary Wi-Fi frames.

**VII. CONCLUSION**

In this paper, we highlighted the side-channel attack model called modulation-based covert channel attack and presented its countermeasure system, Ghost-Fi Detector. Specifically, we demonstrated three concrete real-world attack scenarios using the modification of amplitude, phase, and frequency offset with SDRs. At the same time, to track down the covert channels, six effective defense mechanisms were proposed. Since each mechanism only partially recognizes the existence of covert channels, the overall performance results fluctuate intensively depending on the type of attack. We constructed Ghost-Fi Detector, which integrates the six defense mechanisms to compensate each other and to guarantee stable covert channel detection rates. As a result of the evaluation, each attack is detected with an average hit rate of 95% in all experimental settings. For future research directions, we plan to study adaptive optimization for received signals and the detection method integration scheme to improve the performance. Furthermore, beyond the decision of the presence of the covert channels, it would obtain the type of covert channels being detected, which helps keep track of the leaking information. We expect our work on the wireless physical layer security to lay the foundation for more secure Wi-Fi networks.

**REFERENCES**

[1] S. D’Oro, F. Restuccia, and T. Melodia, “Hiding data in plain sight: Undetectable wireless communications through pseudo-noise asymmetric shift keying,” in Proc. IEEE INFOCOM Conf. Comput. Commun., Apr. 2019, pp. 1585–1593.

[2] X. Zhang, Y.-A. Tan, C. Liang, Y. Li, and J. Li, “A covert channel over VoLTE via adjusting silence periods,” IEEE Access, vol. 6, pp. 9292–9302, 2018.
VOLUME 10, 2022
89957

[3] J.-W. Ho, “Covert channel establishment through the dynamic adaptation of the sequential probability ratio test to sensor data in IoT,” *IEEE Access*, vol. 7, pp. 146093–146107, 2019.

[4] K. S. Subramani, N. Helal, A. Antonopoulos, A. Nosratinia, and Y. Makris, “Amplitude-modulating analog/RF hardware Trojans in wireless networks: Risks and remedies,” *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3497–3510, 2020.

[5] D. Kundur and K. Ahsan, “Practical internet steganography: Data hiding in IP,” in *Proc. Texas Workshop Secur. Inf. Syst.*, 2003, pp. 1–5.

[6] K. Szczypiorski and W. Mazurczyk, “Steganography in IEEE 802.11 OFDM symbols,” *Secur. Commun. Netw.*, vol. 9, no. 2, pp. 118–129, Jan. 2016.

[7] W. Graniszewski, J. Krupski, and K. Szczypiorski, “SOMSteg–framework for covert network channel, and its detection, within HTTP,” *J. Universal Comput. Sci.*, vol. 24, no. 7, pp. 867–891, 2018.

[8] S. Cabuk, C. E. Brodley, and C. Shields, “IP covert timing channels: Design and detection,” in *Proc. 11th ACM Conf. Comput. Commun. Secur. (CCS)*, 2004, pp. 178–187.

[9] T. E. Calhoun, X. Cao, Y. Li, and R. Beyah, “An 802.11 MAC layer covert channel,” *Wireless Commun. Mobile Comput.*, vol. 12, no. 5, pp. 393–405, Apr. 2012.

[10] R. Holloway and R. Beyah, “Covert DCF: A DCF-based covert timing channel in 802.11 networks,” in *Proc. IEEE 8th Int. Conf. Mobile Ad-Hoc Sensor Syst.*, Oct. 2011, pp. 570–579.

[11] S. Zander, G. Armitage, and P. Branch, “A survey of covert channels and countermeasures in computer network Protocols,” *IEEE Commun. Surveys Tuts.*, vol. 9, no. 3, pp. 44–57, 3rd Quart., 2007.

[12] H. Zhao and Y.-Q. Shi, “Detecting covert channels in computer networks based on chaos theory,” *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 2, pp. 273–282, Feb. 2013.

[13] P. L. Shrestha, M. Hempel, F. Rezaei, and H. Sharif, “A support vector machine-based framework for detection of covert timing channels,” *IEEE Trans. Depend. Secure Comput.*, vol. 13, no. 2, pp. 274–283, Apr. 2015.

[14] C.-W. Tien, T.-T. Tsai, I.-Y. Chen, and S.-Y. Kuo, “UFO–hidden backdoor discovery and security verification in IoT device firmware,” in *Proc. Int. Symp. Electr. Electron. Eng. Workshops (ISEEEW)*, Oct. 2018, pp. 18–23.

[15] T. Alladi, V. Chamola, B. Sikdar, and K. R. Choo, “Consumer IoT: Security vulnerability case studies and solutions,” *IEEE Consum. Electron. Mag.*, vol. 9, no. 2, pp. 17–25, Mar. 2020.

[16] M. Guri, A. Kachlon, O. Hasson, Y. Mirsky, and Y. Elovici, “GSMem: Data exfiltration from air-gapped computers over GSM frequencies,” in *Proc. 24th USENIX Secur. Symp. (USENIX Secur.)*, Jun. 2018, pp. 375–389.

[17] N. Kiyavash, F. Koushanfar, T. P. Coleman, and M. Rodrigues, “A timing vulnerability case studies and solutions,” in *Proc. IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 393–405, 2017.

[18] Y. Zhu, Z. Xiao, Y. Chen, Z. Li, M. Liu, B. Y. Zhao, and H. Zheng, “Et Tu alexa? When commodity WiFi devices turn into adversarial motion sensors,” in *Proc. Netw. Distrib. Syst. Secur. Symp.*, Feb. 2020, pp. 1–15.

[19] E. Cottais, J. L. Esteves, and C. Kasmi, “Second order soft-TEMPEST in RF front-ends: Design and detection of polyglot modulations,” in *Proc. Int. Symp. Electromagn. Compat. (EMC EUROPE)*, Aug. 2016, pp. 168–171.

[20] A. Dutta, D. Saha, D. Grunwald, and D. Sicker, “Secret agent radio: Covert communication through dirty constellations,” in *Proc. Int. Workshop Inf. Hiding (IH)*, 2012, pp. 160–175.

[21] Z. Xu and W. Yuan, “Watermarking BER and channel capacity analysis for OFDM-based RF watermarking by constellation dithering in AWGN channel,” *IEEE Signal Process. Lett.*, vol. 24, no. 7, pp. 1068–1072, Jul. 2017.

[22] J. Classen, M. Schulz, and M. Hollick, “Practical covert channels for WiFi systems,” in *Proc. IEEE Conf. Comput. Commun. Netw. Secur. (CNS)*, Sep. 2015, pp. 209–217.

[23] M. Schulz, J. Link, F. Gringoli, and M. Hollick, “Shadow WiFi: Teaching smartphones to transmit raw signals and to extract channel state information with third-party implementations of WiFi networks: A survey and a way ahead,” *IEEE Trans. Mobile Comput.*, vol. 19, no. 2, pp. 1104–1117, Apr. 2022.

[24] M. Christodorescu, S. Jha, S. A. Seshia, D. Song, and R. E. Bryant, “Semantics-aware malware detection,” in *Proc. IEEE Symp. Secure. Privi.* PA, USA, Jul. 1992, pp. 144–152.

[25] C. Kolbitsch, P. M. Comparretti, C. Kruegel, E. Kirda, X. Zhou, and X. Wang, “Effective and efficient malware detection at the end host,” in *Proc. 18th Conf. USENIX Secur. Symp.*, Aug. 2009, pp. 351–366.

[26] N. Xie, Z. Li, J. Tan, and A. X. Liu, “Detection of information hiding at physical layer in wireless communications,” *IEEE Trans. Depend. Secure Comput.*, vol. 19, no. 2, pp. 1104–1117, Apr. 2022.

[27] M. Schulz, D. Wegemer, and M. Hollick, “The nexion firmware analysis and modification framework: Empowering researchers to enhance Wi-Fi devices,” *Comput. Commun.*, vol. 129, pp. 269–285, Sep. 2018.

[28] G. Baldini, T. Sturman, A. R. Biswas, R. Leshchorn, G. Gedor, and M. Street, “Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead,” *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 355–379, 2nd Quart., 2012.

[29] E. Sourour, H. El-Ghoroury, and D. McNeill, “Frequency offset estimation and correction in the LWAIRL architecture,” in *Proc. IEEE 60th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2004, pp. 4923–4927.

[30] C. Shao, W. Jang, H. Park, J. Sung, Y. Jung, and W. Lee, “Phantom eavesdropping with whitened RF leakage,” *IEEE Wireless Commun. Lett.*, vol. 9, no. 2, pp. 232–235, Feb. 2020.

[31] B. E. Boser, I. M. Guyen, and V. N. Vapnik, “A training algorithm for optimal margin classifiers,” in *Proc. 5th Annu. Workshop COLT*. Pittsburgh, PA, USA, Jul. 1992, pp. 144–152.

[32] Z. Zhu and A. K. Nandi, *Automatic Modulation Classification: Principles, Algorithms and Applications*, 1st ed. Hoboken, NJ, USA: Wiley, 2015.

[33] O. A. Dobre, A. Abdi, Y. Bar-Ness, and W. Su, “Survey of automatic modulation classification techniques: Classical approaches and new trends,” *IET Commun.*, vol. 1, no. 2, pp. 137–156, Apr. 2007.

[34] A. Swami and B. M. Sadler, “Hierarchical digital modulation classification using cumulants,” *IEEE Trans. Commun.*, vol. 48, no. 3, pp. 416–429, Mar. 2000.
[51] W. Jang and W. Lee, “Detecting wireless steganography with wavelet analysis,” IEEE Wireless Commun. Lett., vol. 10, no. 2, pp. 383–386, Feb. 2021.
[52] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, “Wireless device identification with radiometric signatures,” in Proc. 14th ACM Int. Conf. Mobile Comput. Netw., Mar. 2008, pp. 116–127.
[53] B. Bloessl, M. Segata, C. Sommer, and F. Dressler, “An IEEE802.11ag/p OFDM receiver for GNU radio,” in Proc. 2nd Workshop Softw. Radio Implement. Forum (SRIF), Aug. 2013, pp. 9–16.
[54] E. Perahia and R. Stacey, Next Generation Wireless LANs: 802.11n and 802.11ac, 2nd ed. USA: Cambridge, U.K.: Cambridge Univ. Press, 2013.

HOORIN PARK (Member, IEEE) received the B.S. and Ph.D. degrees in computer science and engineering from Korea University, Seoul, Republic of Korea, in 2011 and 2020, respectively. He is currently an Assistant Professor with the Department of Information Security, Seoul Women’s University, Seoul. His research interests include RF-powered computing and networking, network security, and trusted execution environment design on the untrusted cloud.

WONWOO JANG (Graduate Student Member, IEEE) received the B.S. degree in computer major from the College of Computing, Hanyang University ERICA Campus, Ansan, Gyeonggi-do, Republic of Korea, in 2018, and the M.E. degree in cybersecurity from the School of Cybersecurity, Korea University, Seoul, Republic of Korea, in 2020, where he is currently pursuing the Ph.D. degree in cybersecurity. His research interests include RF-powered computing and networking, next-generation transport protocols, and deep learning.

JEKYUNG SUNG (Graduate Student Member, IEEE) received the B.Eng. degree in cyber defense from Korea University, Seoul, Republic of Korea, in 2020, where he is currently pursuing the Ph.D. degree with the School of Cybersecurity. His research interests include wireless networking, communications, sensing, and related security issues.

HEEJUN ROH (Member, IEEE) received the B.S. degree in computer science and engineering from Korea University, Seoul, Republic of Korea, in 2009, double-majoring in mathematics, and the M.S. and Ph.D. degrees from Korea University, in 2011 and 2017, respectively. He is currently an Assistant Professor in applied mathematical sciences with Korea University Sejong Campus, Republic of Korea. His research interests include security and privacy in wireless networks, RF-powered computing and networking, and architectural design of cloud computing.

WONJUN LEE (Fellow, IEEE) received the B.S. and M.S. degrees in computer engineering from Seoul National University, Seoul, Republic of Korea, in 1989 and 1991, respectively, the M.S. degree in computer science from the University of Maryland, College Park, MD, USA, in 1996, and the Ph.D. degree in computer science and engineering from the University of Minnesota, Minneapolis, MN, USA, in 1999. In 2002, he joined as a Faculty Member of Korea University, Seoul, where he is currently a Professor with the School of Cybersecurity. His research interests include communication and network protocols, wireless communication and networking optimization techniques, security and privacy in mobile computing, and RF-powered computing and networking. He has authored over 250 papers in refereed international journals and conferences, and a book Optimal Coverage in Wireless Sensor Networks (Springer, 2020) (with D.-Z. Du). He has served on Program and Organization Committees of numerous leading wireless and networking conferences, including IEEE INFOCOM, from 2008 to 2023, the PC Track Chair of IEEE ICDCS 2019, the Workshop Chair of IEEE ICDCS 2023 and the ACM MobiHoc, from 2008 to 2009, and over 148 international conferences. He has received numerous awards, including the IEEE Chester W. Sall Memorial Award, in 2018, the KIISE Gaheon Research Award, in 2011, the LG Yonam Foundation Overseas Faculty Member Award, in 2007, and the Best Teaching Award from Korea University, in 2005, 2009, and 2021. In 2019, his project “BackPlugged: Wearable-optimized Ultra Low-Power Wi-Fi Networking with Plugged-in Backscatter Radio” was selected for 100 Outstanding National Research and Development Achievements by the Ministry of Science and ICT (MSIT), South Korea. He is the 2022 President-Elect (the 2023 President) of the Korean Institute of Information Scientists and Engineers (KIIEEE). He is a fellow of the Korean Academy of Science and Technology (KAST).