Convolution Attack on Frequency Hopping by Full-Duplex Radios

Harshan Jagadeesh and Yih-Chun Hu

***Abstract*—In this paper, we propose a new adversarial attack on frequency-hopping-based wireless communication between two users, namely Alice and Bob. In this attack, the adversary referred to as Eve, instantaneously modifies the transmitted signal by Alice before forwarding it to Bob within the symbol period. We show that this attack forces Bob to incorporate Eve's signal in the decoding process; otherwise, treating it as noise would further degrade the performance akin to jamming. Through this attack, we show that Eve can convert a slow-fading channel between Alice and Bob to a rapid-fading one by modifying every transmitted symbol independently. As a result, neither pilot-assisted coherent detection techniques nor blind-detection methods are directly applicable as countermeasures. As potential mitigation strategies, we explore the applicability of frequency hopping along with ON–OFF keying (OOK) and binary frequency-shift keying (BFSK) as modulation schemes. In the case of OOK, the attacker attempts to introduce deep fades on the tone carrying the information bit, whereas in the case of BFSK, the attacker pours comparable energy levels on the tones carrying bit-0 and bit-1, thereby degrading the performance. Based on extensive analyses and experimental results, we show that when using OOK, Bob must be equipped with a large number of receive antennas to reliably detect Alice's signal, and when using BFSK, Alice and Bob must agree upon a secret key to randomize the location of the tones carrying the bits, in addition to randomizing the carrier frequency of communication.**

***Index Terms*—Jamming, frequency-hopping, cognitive radio, convolution attack, wireless security.**

I. Introduction

JAMMING is a well known adversarial attack on wireless communication [1]–[5] wherein the attacker overpowers the communication between a transmitter and a receiver by injecting high-powered noise signals. Standard ways to mitigate jamming include frequency-hopping (FH) [6], [7] and direct sequence spread spectrum (DSSS) schemes [8]. In the case of DSSS, a narrowband signal is spread across a wide band of frequencies by using a spreading code so that an attacker, which does not possess the spreading code, will have its jamming signal rejected by the receiver. In the case of FH, which is the subject matter of this paper, the transmitter and the receiver synchronously hop across several carrier-frequencies so that the hopping pattern appears non-deterministic to the adversary. As a result, narrowband jamming, i.e., jamming a specific carrier-frequency, cannot guarantee performance degradation due to randomness in the hopping pattern. On the other hand, with wideband jamming, i.e., jamming all the carrier-frequencies, the effective noise power injected on each carrier-frequency would be too weak to induce significant degradation in the performance. Both DSSS and FH are effective under the assumption that the attacker is power-constrained. Citing these benefits, DSSS and FH have found extensive applications in military communication systems, and recently in many cyber-physical systems. While DSSS and FH introduce randomness in the choice of the spreading code and carrier-frequencies, respectively, introducing randomness over spatial orientation of the antennas has also been explored as a viable anti-jamming technique in communication involving highly-directional antennas [9].

With wireless communication being an integral part of most cyber-physical systems, e.g., urban transportation, smart-grid and other IOT systems [10], it is imperative to envision new attacks [11] on such systems and provide suitable countermeasures against them. Over the past decade, wireless communication technology has witnessed enormous progress in bandwidth-efficient physical-layer techniques that have helped wireless devices achieve high data-rate. One of the prominent areas rising in this space is full-duplex communication [15]–[17], wherein a radio device can simultaneously transmit and receive signals in the same frequency band. While efficient hardware- and software-architectures have helped full-duplex radios to achieve near-perfect self-interference cancellation, there have been concurrent developments in hardware implementation for low-latency processing of radio frequency (RF) signals [23] in the field of systems security. Aggregating the latest developments in the above areas, we believe that next-generation cyber-physical systems ought to assume strong attack models that employ state-of-the-art wireless techniques.

A. Motivation

In this paper, we are interested in threat models arising out of full-duplex radios that operate as hidden relays between a transmitter and a receiver, as depicted in Fig. 1. Loosely speaking, this threat comes under the well known framework of *man-in-the-middle attacks*, wherein the attacker can manipulate the transmitted symbols before they reach the legitimate receiver. Although instantaneous modification of transmitted symbols has been

Manuscript received May 17, 2018; revised November 25, 2018 and January 19, 2019; accepted March 4, 2019. Date of publication March 28, 2019; date of current version June 18, 2019. This work was supported by the Indigenous 5G Test Bed project from the Department of Telecommunications, Ministry of Communications, New Delhi, India. The review of this paper was coordinated by Prof. R. Q. Hu. *(Corresponding author: J. Harshan.)*

H. Jagadeesh is with the Indian Institute of Technology Delhi, New Delhi 110016, India (e-mail: jharshan@ee.iitd.ac.in).

Y.-C. Hu is with the University of Illinois Urbana-Champaign, Champaign, IL 61820 USA (e-mail: yihchun@illinois.edu).

Digital Object Identifier 10.1109/TVT.2019.2908008

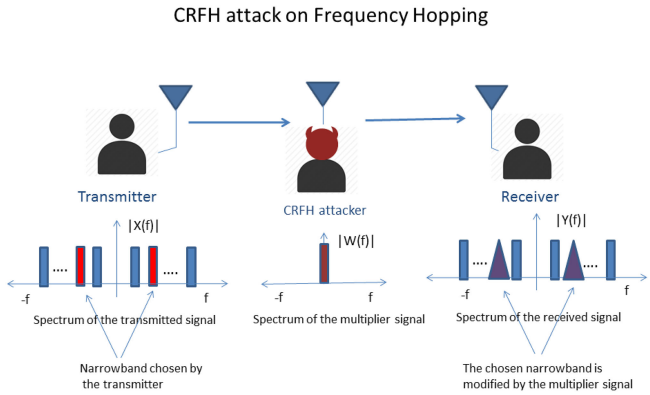

Fig. 1. Under the framework of Cognitive Radio from Hell (CRFH), the attacker can modify the signal in any narrowband chosen by the two users despite not knowing the hopping pattern. In the above figure, $X(f)$, $W(f)$, and $Y(f)$, respectively, denote the Fourier transform of the transmitted passband signal, attacker's random signal, and the received passband signal.

addressed to mitigate interference in wireless networks [12], [13], [22], such ideas have not been studied as a threat to wireless security. An important question to answer along that direction is: *Are the current-day wireless systems resilient to instantaneous manipulation of transmitted symbols in the air?* From the standpoint of practicality, major challenges to instantaneous modification include (i) additional processing-delay and (ii) additional path-delay, introduced by the attacker. The processing-delay constraint restricts the attacker not to make dynamic decisions based on baseband signal processing of the received signals. On the other hand, the path-delay constraint resulting from the attacker's position restricts it to be appropriately placed so that the forwarded components reach the receiver well within the delay of one symbol-period relative to the signals received from the main path. In a nutshell, if the above two constraints are respected, then, in principle, it is possible for the modified signals to arrive at the legitimate receiver within the symbol-period. We refer to such an attacker as Cognitive Radio from Hell (CRFH). The proposed adversarial model comes under the class of correlated jamming [14] wherein the jammer has full or partial information about the transmitter's signals.

B. CRFH Attacks on Frequency-Hopping

Our discussion in the preceding section indicates that the processing-delay and the path-delay constraints may preclude the attacker from executing instantaneous modification on wideband communication due to small symbol-periods. However, on narrowband communication systems, such as FH (wherein the bandwidth around the chosen carrier-frequency is small), the attacker can potentially execute instantaneous modification "in the air" due to relatively large symbol-periods compared to the path-delay on the main path. This has motivated us to study the effect of CRFH attacks on FH systems. Particularly, in the context of FH, we note that instantaneous modification of symbols is crucial to degrade the error-performance at Bob, otherwise, any unintentional delay introduced by the attacker, will result in a delay of one symbol-period or more. This allows the legitimate receiver to evade the attack by hopping to the next carrier-frequency before the delayed components arrive. Thus, to enforce degraded performance from instantaneous modification, the CRFH attacker on FH must respect the delay constraints on instantaneous modification.

C. Related Work

To help translate the idea of CRFH attack to practice, recent advances in the field of full-duplex radios [15]–[20] have shown that radios can be designed to cancel their self-interference while instantaneously forwarding the transmitted signals. In particular, [21] has showcased the possibility of building radios with the capability of instantaneous processing and relaying. Recently, [22] has demonstrated the effectiveness of instantaneous modification by full-duplex radios to achieve co-existence in interference channels. Also, [23] has showed that radio-frequency signals can be processed and retransmitted in the analogue domain with a delay of few nano-seconds.

The notion of modifying symbols in the air is also known under the framework of reactive jamming [24], which refers to the process of targeting selected packets in the air as it allows the attacker to destroy specific packets and yet go undetected. The authors of [25] have studied the feasibility of reactive jamming by designing and implementing a reactive jammer against 802.15.4 networks. Through the use of Universal Software Radio Peripherals (USRPs), [25] has demonstrated jamming attack with reaction time of the order of microseconds in indoor environments. In [26], the authors have addressed reactive jamming attacks where the adversary is capable of picking packets based on real-time classification of packets at the physical-layer. They have also proposed countermeasures to prevent real-time packet classification based on both cryptographic as well as physical-layer ideas. In [27], the authors have proposed a technique to detect reactive jammers on DSSS. The basic idea is to use statistics on attack-free packets and then identify packets attacked from those lost due to bad channel condition. In [28], reactive jamming on Orthogonal Frequency Division Multiplexing (OFDM) is considered, and an effective countermeasure based on Multiple-Input Multiple-Output (MIMO) systems has been proposed. Overall, inspired by the above works, particularly that of [21] and [23], we believe that it is imperative for existing cyber-physical systems to envision attacks that could arise out of full-duplex radios capable of instantaneous modification of transmitted symbols.

D. Contributions

The contributions of this paper are summarized below:

- We introduce a new adversarial attack, referred to as the convolution attack (CA), on FH based wireless communication. In this attack, the adversary, which is strategically positioned between the transmitter and the receiver, instantaneously multiplies the received passband signal by a random baseband signal, and then forwards it to the receiver within the symbol-period. Subsequently, the forwarded signals will combine with the signals directly received from the transmitter, thereby modifying the information symbols *in the air*. One of the highlights of the attack is that the attacker is able to perturb the transmitted symbols

despite not knowing the active narrowband of communication. We show that the proposed attack forces the legitimate receiver to incorporate the forwarded signals in the decoding process; otherwise, discarding them as noise is shown to result in consequences akin to jamming. (see Section III). We also show that the CA forces the equivalent channel between the legitimate users to experience frequency-selectivity and rapid-fading, in such a way that neither pilot-based coherent detection techniques, nor traditional non-coherent and differential encoding/decoding detection techniques can mitigate the attack.

- As a countermeasure against CA, we study the performance of an FH system with non-coherent On-Off Keying (OOK) as the underlying modulation scheme (see Section IV). This mitigation strategy, although a traditional communication scheme, is tailor-made to handle the threat model because switching-off the transmission forbids the attacker from perturbing the communication, while switching-on the transmission helps the receiver to collect energy despite the attack. With large number of antennas at the receiver, we show that the receiver can opportunistically use the attacker's signal to its advantage to gather more energy for detection (see Section IV-A). We show that OOK is an effective countermeasure if the attacker executes the convolution attack on both the pilot symbols and the data symbols with the same attack parameters; this is because the threshold for energy detection is computed using the received energy distributions on the pilot symbols. However, if the attacker decides to selectively attack only the data symbols and not the pilots, then OOK is no longer an effective countermeasure.
- As a second countermeasure against CA, we study the performance of non-coherent Binary Frequency Shift Keying (BFSK), a widely used modulation scheme with FH in military application. In this form of CA, the adversary instantaneously modifies the signal "in the air" so that the receiver witnesses comparable energy levels on the tones carrying bit-0 and bit-1. As a result, this attack significantly degrades the error performance at the receiver when it uses threshold-based energy detection (see Section V). One the fundamental causes for this attack is that although the carrier-frequency is randomly hopped based on a shared secret-key between the legitimate users, the locations of the tones carrying bit-0 and bit-1 are deterministic upto one bit randomness when the attacker observes the signal in the air. We first show that this form of CA, when appropriately executed, introduces error-floor behaviour in the error performance. Subsequently, we propose a mitigation strategy, referred to as Enhanced BFSK, wherein unlike the standard frequency-hopping technique, the tones carrying bit-1 and bit-0 are also randomized based on an additional secret-key shared between the legitimate users. As a consequence, upon observing the transmitted signal in the air, the attacker continues to have uncertainty about the location of tone carrying the complementary bit, thereby forcing it to execute wideband jamming. Unlike the case of OOK, we show that BFSK is resilient even if the attacker selectively executes the CA on the data symbols and not on the pilots; this is because BFSK detection does not rely on the distribution of received energy on the pilots.

Henceforth, throughout the paper, we refer to the transmitter, the receiver, and the attacker as Alice, Bob and Eve, respectively. To model a power-constrained attacker, we assume that Eve has θ times more energy than Alice, i.e., $E_{Eve} = \theta E_{Alice}$, for some $\theta >> 1$. This implies that as Alice increases her energy to improve the performance, Eve can also proportionately increase her energy. Furthermore, out of E_{Eve}, Eve may use only a fraction of it, say $E_{Eve,C} = \alpha E_{Eve}$, for some $0 \leq \alpha \leq 1$, on the CA. Thus, the key attack parameters of this paper are $\theta >> 1$ and $0 \leq \alpha \leq 1$.

II. Convolution Attack on Frequency-Hopping

Consider an FH based amplitude-modulated communication scheme between Alice and Bob, wherein the carrier-frequency f_c of the transmitted narrowband signal is randomly chosen from one of the N tones, denoted by the set $\mathcal{F} = \{f_1, f_2, \ldots, f_N\}$. Let Alice use a root raised cosine (RRC) waveform [8], denoted by $g(t)$, as the baseband signal of bandwidth W Hz and symbol rate T seconds. Furthermore, let $\{x_k = x_{I,k} + \imath x_{Q,k} \mid k = 0, 1, 2, \ldots\}$, with $\imath = \sqrt{-1}$, denote the sequence of complex symbols, where x_k takes value from a 2-dimensional finite complex constellation, e.g., quadrature amplitude modulation. The corresponding train of baseband signals is given by

$$s_b(t) = \sum_k \sqrt{E_{Alice}} x_k g(t - kT), \tag{1}$$

where E_{Alice} is the average transmit energy by Alice assuming that x_k and $g(t)$ are appropriately normalized. After modulating $s_b(t)$ on carrier-frequency $f_c \in \mathcal{F}$, the transmitted passband signal is of the form

$$s(t) = \mathcal{R}\left(s_b(t) e^{2\pi \imath f_c t}\right). \tag{2}$$

where $\mathcal{R}(\cdot)$ denotes the real part of a complex number. The set $\mathcal{F}$ is chosen such that $|f_i - f_{i+1}| > W$, for $1 \leq i \leq N-1$, thereby leaving sufficient guard-band to mitigate inter-carrier interference. Alice employs a carrier-frequency $f_c \in \mathcal{F}$ for $T_{hop} = mT$ seconds, for some integer $m > 0$, before hopping to another value in $\mathcal{F}$. Meanwhile, Bob synchronously hops across the same sequence of carrier-frequencies every T_{hop} seconds, as the hopping pattern is generated using a shared secret key. Throughout the paper, we use small values of m by assuming that Alice and Bob are capable of quickly switching the carrier-frequencies with minimal losses due to transients in the transmit and receive RRC filters. Otherwise, with $m >> 1$, a sophisticated attacker can sense the narrowband of communication and subsequently inject jamming energy on the detected band, akin to traditional jamming. Thus, small values of m helps the legitimate users to mitigate standard jamming attacks on frequency-hopping. The discrete-time version of the received baseband signal at Bob is given by

$$y_k(f_c) = \sqrt{E_{Alice}} h_k^{(AB)}(f_c) x_k + n_k^{(B)}(f_c), \tag{3}$$

for $k = 0, 1, \ldots, m-1$, where $h_k^{(AB)}(f_c)$ is the complex channel gain on the tone f_c, and $n_k^{(B)}(f_c)$ is the additive noise at Bob, distributed as $\mathcal{CN}(0, \sigma_{Bob}^2)$. A complex random variable

$g \sim \mathcal{CN}(0, \sigma^2)$ is said to be circularly symmetric Gaussian distributed when the real and imaginary components of g are Gaussian and i.i.d. with mean 0 and variance $\frac{\sigma^2}{2}$. We assume that the channel $h_k^{(AB)}(f_c)$ remains fixed within the hopping interval, i.e., $h_k^{(AB)}(f_c) = h^{(AB)}(f_c), 0 \leq k \leq m-1$. For brevity, henceforth, we drop the reference to the carrier-frequency f_c from the channel model in (3).

We assume that Eve is positioned somewhere between Alice and Bob, and she is not aware of the secret key used to generate the hopping pattern. At any point in time, due to the non-deterministic hopping pattern, Eve cannot successfully guess the *active* carrier-frequency with probability one, and therefore narrowband jamming on a random carrier-frequency in $\mathcal{F}$ does not guarantee degraded error performance.

Keeping in view practical hurdles in executing wideband jamming by a power-constrained attacker, we envision a new attack, referred to as the *convolution attack*, which is as depicted in Fig. 1. We assume that Eve is capable of receiving and transmitting signals in the entire wideband covering all the N carrier-frequencies. Through the CA, we show that Eve can modify the transmitted narrowband signal despite not knowing the active carrier-frequency. We draw our inspiration from the fact that analogue processing of narrowband signals is feasible in negligible amount of time [23]. In the proposed attack, Eve multiples the received passband signal with a random baseband signal, denoted by $w(t)$, in the analogue domain, and then forwards it to Bob. This multiplication operation in the time-domain is equivalent to convolving the Fourier transform of the received signal with that of the random signal. Because of this operation, Eve can modify the narrowband signal without knowing the carrier-frequency. Subsequently, this modified version of the signal is added to the signal arriving directly from Alice, thus corrupting the overall received signal in the narrowband of interest. We make the following assumptions for executing the CA: (i) Negligible processing-delay at Eve, (ii) Negligible path-delay through Eve, and (iii) Full-duplex architecture with perfect cancellation at Eve.

In the next subsection, we mathematically describe how the forwarded signals from Eve affect the received signal at Bob.

A. Signal Model With Convolution Attack

Since Eve does not know the active carrier-frequency, she receives signals in the entire band, covering all the N carrier-frequencies. Specifically, the received signal is given by

$$r(t) = \sum_i a_i^{(AE)} s\left(t - \tau_i^{(AE)}\right) + z(t),$$

where i denotes the i-th multipath component from Alice to Eve, and $a_i^{(AE)}$ and $\tau_i^{(AE)}$, respectively denote the corresponding amplitude and delay associated with the multipath component. Once Alice and Bob are locked onto a carrier-frequency, we assume that the rest of the $N-1$ narrowbands are unused by other users in the network, and therefore, the non-signal component of $r(t)$ constitutes only the additive noise at Eve. In general, when the N narrowbands are shared among several users in the network, the received signal $r(t)$ also constitutes interference from other users. Although Eve receives over a wide band of frequencies, we assume that the channel from Alice to Eve is frequency-flat over the active narrowband. Upon receiving $r(t)$, Eve multiplies it by a real random signal $w(t)$ (of unit average-energy over the symbol-period), and then transmits

$$e(t) = \sqrt{\alpha\theta} r(t) w(t), \tag{4}$$

where $\sqrt{\alpha\theta}$ is the gain introduced by Eve for some $\theta >> 1$ and $0 \leq \alpha \leq 1$. The product operation $r(t)w(t)$ can be viewed as a way of introducing Doppler shifts to the passband signal by various frequency components of $w(t)$. With $e(t)$ transmitted from Eve, the received signal at Bob is given by

$$y(t) = \sum_j b_j^{(EB)} e(t - \tau_j^{(EB)} - t_p) + \sum_q c_q^{(AB)} s(t - \tau_q^{(AB)}) + n(t), \tag{5}$$

where the first part is contributed by Eve, the second part comes directly from Alice, and the last part $n(t)$ is the ambient noise generated at Bob's receiver. In (5), $b_j^{(EB)}$ and $\tau_j^{(EB)}$, respectively denote the amplitude and the delay associated with the j-th multipath component from Eve to Bob. Similarly, $c_q^{(AB)}$ and $\tau_q^{(AB)}$, respectively denote the amplitude and the delay associated with the q-th multipath component from Alice to Bob. Also, note that t_p is the processing-delay introduced by Eve when multiplying the two signals. Among the multipath components from Alice to Bob, let τ_f^{AB} denote the first significant multipath component. Similarly, among the multipath components from Alice to Eve, and Eve to Bob, let τ_f^{AE} and τ_f^{EB} denote the first significant multipath components, respectively. In the proposed attack, Eve positions herself such that the following condition on delay is satisfied:

$$\tau_f^{(AB)} < \tau_f^{(AE)} + t_p + \tau_f^{(EB)} < \tau_f^{(AB)} + T. \tag{6}$$

If the timing constraint in (6) is satisfied, then it is straightforward to verify that Eve's signal $w(t)$ can modify the current symbol in the air. After downconverting the received signal $y(t)$ from the carrier-frequency $f_c \in \mathcal{F}$, and then sampling and filtering, we obtain the discrete-time version of the baseband received signal, given by

$$y_k = \sqrt{E_{Alice}} h_k^{(AB)} x_k + \sum_{l=0}^{L_k - 1} h_{k,l}^{(AEB)} \sqrt{\alpha\theta E_{Alice}} x_{k-l} + \sqrt{\alpha\theta} n_k^{(EB)} + n_k^{(B)}, \tag{7}$$

for $k = 0, 1, \ldots, m-1$, where $\{h_{k,l}^{(AEB)} \mid 1 \leq l \leq L_k\}$ are the complex channels contributed by Eve, $n_k^{(EB)}$ is the noise component forwarded by Eve, and $n_k^{(B)}$ is the additive noise at Bob. The channel contributed by Eve is possibly frequency-selective, where the number of taps of the channel, denoted by L_k, depends on the chosen waveform $w(t)$. Intuitively, as depicted in Fig. 1, although the channel from Alice to Eve, and Eve to Bob are frequency-flat within a narrowband of W Hz, the convolution operation in the frequency domain can disrupt the frequency-flat structure, thereby giving rise to a frequency-selective channel.

Observe that Eve is not injecting noise into the narrowband of interest, instead she is instantaneously modifying the transmitted symbols by a random quantity, which is some complex function

of (i) the channel from Alice to Eve, (ii) the signal $w(t)$, and (iii) the channel from Eve to Bob. If the timing constraint in (6) is not satisfied, then the signal forwarded by the attacker does not modify the current symbol in the air, instead it reaches Bob in the subsequent symbol-periods. This implies that $h_{k,0}^{(AEB)} = 0$ in (7). Although this form of attack continues to affect the signal-to-noise-ratio of subsequent symbols, the current symbol in the air does not get modified. A straightforward way for Alice and Bob to evade this attack is by locking to a given carrier-frequency for just one symbol before hopping to another carrier-frequency in $\mathcal{F}$. Thus, satisfying the timing constraint in (6) is crucial for Eve to execute the CA when the legitimate users have the potential to hop carrier-frequencies with $m = 1$.

III. Challenges in Mitigating Convolution Attack

Without the attack, i.e., $h_{k,l}^{(AEB)} = 0, \forall k, l$, the complex channel $h_k^{(AB)}$ is determined only by the environment. Importantly, the coherence-time of the channel $h_k^{(AB)}$ is determined only by the relative velocity of the surrounding objects in the environment. However, with attack, an additional signal component $\sum_{l=0}^{L_k-1} h_{k,l}^{(AEB)} x_{k-l}$ is added to the received signal at Bob as shown in (7). A naive way to handle this additional term is by considering it as noise. However, this will naturally lower the signal-to-noise-ratio (SINR), and degrade the error performance when Eve's power is dominant. Instead, since the additional component contains useful information, it is prudent for Bob to treat it as the signal term in the decoding process. After incorporating Eve's signals in the decoding process, Bob is forced to view an equivalent channel model, given by

$$\sqrt{E_{Alice}} h_k^{(AB)} x_k + \sum_{l=0}^{L_k-1} h_{k,l}^{(AEB)} \sqrt{\alpha\theta E_{Alice}} x_{k-l}. \qquad (8)$$

Although Eve is contributing additional signal power into the system, Bob is unsure of how to use this additional power as it may rapidly change every symbol. We now summarize the major changes introduced in the channel model when Eve executes CA with significant power compared to that at Alice: (i) Since $w(t)$ can be arbitrarily chosen by Eve, the equivalent channel can be frequency-selective despite using narrowband for communication. (ii) Unlike in traditional channels, the delay-spread of the equivalent frequency-selective channel may change each symbol since $w(t)$ could be composed of arbitrary segment of signals every T seconds, and finally, (iii) the coherence-time of the equivalent channel can also be controlled by Eve, to the extent that the channel seen across two successive symbols can be uncorrelated. It is worth emphasizing that Eve is able to force abrupt variations in two fundamental characteristics of the channel, namely: frequency-selectivity and Doppler-spread. To bring in these variations, it is necessary for Eve to spend significant power compared to Alice, otherwise the characteristics of the true wireless channel will continue to dominate, and as a result the attack will be ineffective, as shown in (9) at the bottom of this page.

From the model in (8), it seems that Alice and Bob can circumvent the CA by employing encoding and decoding mechanisms that do not rely on the knowledge of channel state information (CSI), such as differential-encoding methods and blind detection techniques [29], [30]. However, these methods work under the assumption that some statistics of the channel remain constant for several blocks, and are also known at the receiver. In the case of CA, these techniques are not directly applicable as $w(t)$ is completely controlled by Eve. In the case of frequency-selective equivalent channel, the delayed components are contributed only by Eve as the main channel is frequency-flat due to the narrowband assumption. A straightforward way to handle frequency-selectivity is by using OFDM as the modulation scheme. However, the idea of OFDM modulation requires the channel realizations to be fixed for at least one OFDM symbol, and this assumption can also be violated by Eve. Therefore, OFDM is not applicable in this attack scenario.

A. Impact of Convolution Attack

To showcase the impact of CA, we consider a Binary Phase Shift Keying (BPSK) signalling scheme at Alice aided by coherent maximum-likelihood detection at Bob. We present the error-performance of this scheme under the following attacks: (i) *Narrowband jamming (NJ)*: Eve executes narrowband jamming by injecting noise of energy $E_{eve} = \theta E_{Alice}$, with $\theta = 9$, on one of the $N = 1024$ bands with uniform distribution, (ii) *Wideband Jamming (WJ)*: Eve executes wideband jamming by uniformly dividing its energy $E_{eve} = \theta E_{Alice}$, with $\theta = 9$, across the $N = 1024$ narrowbands, and (iii) *Convolution attack (CA)*: Eve executes CA to result in a rapid-fading frequency-flat equivalent channel, with $\alpha = 1$ and $\theta = 9$. The equivalent channel on each carrier, denoted by $\sqrt{E_{Alice}} h_k^{(AB)} + \sqrt{E_{Alice}\alpha\theta} h_k^{(AEB)}$, changes rapidly to force error-floor behaviour on coherent maximum-likelihood detection. For the experiments, we use $\sigma_{Bob}^2 = 1$ and $\sigma_{Eve}^2 = 0.01$. In Fig. 2, we plot the bit-error-rate (BER) curves of the above schemes against $\frac{E_b}{N_0} = \frac{E_{Alice}}{2\sigma_{Bob}^2}$ when Bob is equipped with $N_r = 2$ and $N_r = 10$ receive antennas. The plots show that neither narrowband jamming nor wideband jamming is effective in degrading the error-performance at Bob, whereas CA can force severe BER degradation at an attack-ignorant Bob. Thus, even with large values of N, it is important for Alice and Bob to identify CA, and then mitigate it by employing an appropriate countermeasure.

IV. Convolution Attack on FH Based On-Off Keying

We study an FH system with non-coherent On-Off Keying (OOK) as the modulation scheme. In this strategy, Alice communicates bit-1 by transmitting a signal of energy E_{Alice} (referred

$$y_k = \begin{cases} \sqrt{E_{Alice}} h_k^{(AB)} + \sqrt{\alpha\theta E_{Alice}} h_k^{(AEB)} + \sqrt{\alpha\theta} n_k^{(EB)} + n_k^{(B)}, & \text{if } b_k = 1 \\ \sqrt{\alpha\theta} n_k^{(EB)} + n_k^{(B)}, & \text{Otherwise} \end{cases} \qquad (9)$$

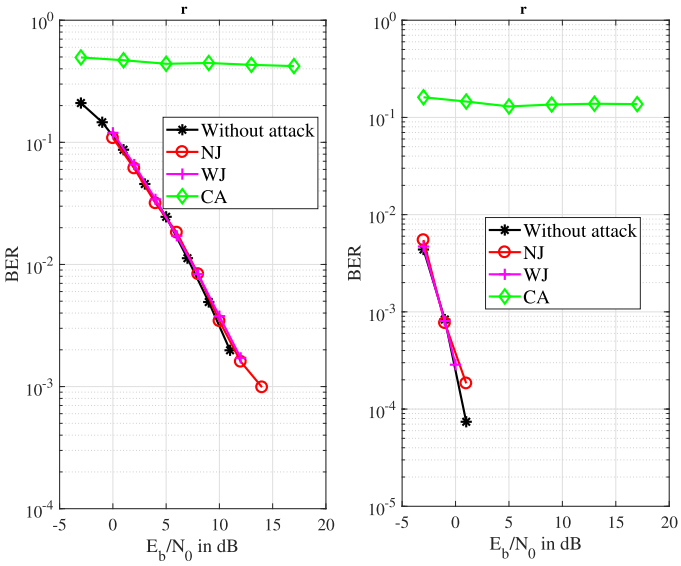

Fig. 2. Impact of CA, Narrowband Jamming and Wideband Jamming on an FH-based communication with $N = 1024$ carrier frequencies. Binary Phase Shift Keying (BPSK) signalling scheme is used at Alice aided by coherent maximum-likelihood detection at Bob.

to as ON state), and bit-0 by switching-off the communication (referred to as OFF state). For exposition, let b_k denote the bit transmitted at the k-th time instant. To communicate b_k, Alice encodes it as

$$x_k = \begin{cases} 1, & \text{if } b_k = 1; \\ 0, & \text{otherwise}, \end{cases} \tag{10}$$

before transmitting x_k on the carrier-frequency $f_k \in \mathcal{F}$. From the nature of the attack, it is clear that Eve forwards only the noise component in the active narrowband when Alice switches-off her transmitter. However, when Alice transmits bit-1, Eve forwards significant signal power in the active narrowband. With this signal design, Bob can distinguish bit-1 and bit-0 by measuring the received energy on each symbol without the knowledge of the channel. In the rest of this paper, we assume that Eve uses $w(t)$ which results in a frequency-flat equivalent channel at Bob. For the frequency-selective case, Alice and Bob may handle it by locking onto a carrier-frequency f_c only for one symbol, i.e., $m = 1$, so that Bob may continue to listen to the preceding set of carrier-frequencies for the delayed components. Our inferences on the attack-strategies and countermeasures are only based on the frequency-flat equivalent channel model. Since the users can handle frequency-selectivity by hopping across the carrier-frequencies for one symbol, we do not expect significant deviations in the inferences with the frequency-selective case.

Applying OOK on the frequency-flat model, the received symbol at Bob is given in (9) , where $\sqrt{\alpha\theta}$ is the gain applied by Eve on its received signal. Based on the nature of operations at Eve, we model the complex channel $h_k^{(AEB)}$ as $h_k^{(AEB)} \triangleq h_k^{(AE)} w_k h_k^{(EB)}$, where $h_k^{(AE)}$ is the channel from Alice to Eve, distributed as $\mathcal{CN}(0,1)$, $h_k^{(EB)}$ is the channel from Eve to Bob, distributed as $\mathcal{CN}(0,1)$, and w_k is a complex random variable of mean zero and unit variance obtained from the waveform $w(t)$. The forwarded additive noise from Eve is $n_k^{(EB)} \triangleq h_k^{(EB)} w_k n_k^{(E)}$, where $n_k^{(B)}$ is distributed as $\mathcal{CN}(0, \sigma_{Eve}^2)$. Henceforth, we denote $\alpha\theta E_{Alice}$ as $E_{Eve,C}$, which is the additional signal energy contributed by Eve through CA.

At the receiver side, Bob decodes to an estimate of b_k, denoted by $\hat{b}_k$, based on the following rule:

$$\hat{b}_k = \begin{cases} 1, & \text{if } |y_k|^2 > E_{th}; \\ 0, & \text{Otherwise.} \end{cases}, \tag{11}$$

where E_{th} is an appropriately designed threshold chosen based on the noise component in (9). One of the challenges in designing OOK against the CA is the derivation of the threshold E_{th}, as fading characteristics of $h_k^{(AB)}$ and $h_k^{(AEB)}$ have to be considered. We address the choice of E_{th} in Section IV-C.

When decoding OOK, Bob faces two types of error events: (i) $\hat{b}_k = 1$ when $b_k = 0$, and (ii) $\hat{b}_k = 0$ when $b_k = 1$. While the former event may occur when the threshold E_{th} is lower than the noise components jointly contributed by Eve and Bob, the latter event captures the case when Eve attempts to force the effective channel $\sqrt{E_{Alice}} h_k^{(AB)} + \sqrt{\alpha\theta E_{Alice}} h_k^{(AEB)}$ to deep fade, i.e., $|y_k|^2 \leq E_{th}$. We represent the associated probability as $P_{1\to 0}^{(attack)}$. In the following section, we propose a mitigation strategy by Bob to reduce $P_{1\to 0}^{(attack)}$.

A. Mitigation Strategy: Large Number of Receive Antennas

In the case of CA, since $w(t)$ is completely controlled by Eve, the distribution of the equivalent channel can be changed to affect $P_{1\to 0}^{(attack)}$ provided $E_{Eve,C} >> E_{Alice}$. However, on the defense-side, since the two users hop across a wide range of narrowbands, Eve cannot learn the narrowband, and therefore, she cannot drive the equivalent channel $\sqrt{E_{Alice}} h_k^{(AB)} + \sqrt{E_{Eve,C}} h_k^{(AEB)}$ to deep fade with probability one. As a defense mechanism to counter Eve's strategy, Bob should collect energy from as many independent paths as possible. One such bandwidth-efficient way is to employ multiple receive antennas at Bob. This way, the probability that Eve can drive all the independent channels simultaneously to deep fade can be reduced. If we use N_r to denote the number of receive antennas at Bob, without additive-noise at Eve and Bob, the total signal energy collected across N_r antennas is given by

$$R_{N_r,k}^{(attack)} \triangleq \sum_{j=1}^{N_r} \left| \sqrt{E_{Alice}} h_{k,j}^{(AB)} + \sqrt{E_{Eve,C}} h_k^{(AE)} w_k h_{k,j}^{(EB)} \right|^2, \tag{12}$$

where $h_{k,j}^{(AB)}$ and $h_{k,j}^{(EB)}$ denote the equivalent channels seen by the j-th antenna of Bob on the k-th symbol. In the event of no attack, we have $w_k = 0$, and $R_{N_r,k}^{(no-attack)}$, given by

$$R_{N_r,k}^{(no-attack)} \triangleq \sum_{j=1}^{N_r} \left| \sqrt{E_{Alice}} h_{k,j}^{(AB)} \right|^2, \tag{13}$$

is Chi-square distributed with degrees of freedom $2N_r$. However, with attack, the error-performance depends on the distribution of $R_{N_r,k}^{(attack)}$ given in (12), which in turn depends on the distribution of w_k. When N_r is large, the following proposition

shows that Eve's additional energy can be used to Bob's advantage to accumulate more energy. Although this result seems to suggest that CA is aiding Bob to improve the error-performance, it is important to note that this relative improvement is with respect to non-coherent OOK, which is already sub-optimal compared to coherent ML detection techniques.

Proposition 1. Let $R_\Delta \triangleq R_{N_r,k}^{(attack)} - R_{N_r,k}^{(no-attack)}$, where $R_{N_r,k}^{(attack)}$ and $R_{N_r,k}^{(attack)}$ are as given in (12) and (13), respectively. For a small $\epsilon > 0$, there exists $\bar{N}_r$ such that for all $N_r \geq \bar{N}_r$, we have

$$\text{Prob}\left(\frac{R_\Delta}{N_r} > -\epsilon\right) > 1 - \epsilon. \tag{19}$$

Proof. We start by expanding $R_{N_r,k}^{(attack)}$ as in (14), shown at the bottom of this page, where $\sum_{j=1}^{N_r} |\sqrt{E_{Alice}} h_{k,j}^{(AB)}|^2$ is the energy accumulated at Bob without the attack. As a result, Prob$(\frac{R_\Delta}{N_r} > -\epsilon)$ can be written as shown in (15) at the bottom of this page. Since $\sum_{j=1}^{N_r} |\sqrt{E_{Eve,C}} h_k^{(AE)} w_k h_{k,j}^{(EB)}|^2$ is strictly non-negative, the probability in (15) is lower-bounded by (16), shown at the bottom of this page. This is because we are only considering the events when

$$\frac{1}{N_r}\sum_{j=1}^{N_r}\left(\sqrt{E_{Alice}E_{Eve,C}}\, 2\mathcal{R}\left(h_{k,j}^{*(AB)} h_k^{(AE)} w_k h_{k,j}^{(EB)}\right)\right)$$

is bounded in the interval $(-\epsilon, \epsilon)$. Furthermore, the random variables $\{\mathcal{R}(h_{k,j}^{*(AB)} h_k^{(AE)} w_k h_{k,j}^{(EB)}) \mid 1 \leq j \leq N_r\}$ are i.i.d. with mean zero since $h_k^{(AE)}$ and w_k are constants. As a result, we rewrite (16) as shown in (17) at the bottom of this page. Finally, applying weak law of large numbers [32, Ch. 3] on (17) we get (18), shown at the bottom of this page, for sufficiently large $N_r \geq \bar{N}_r$. This completes the proof.

With massive MIMO in contention for next-generation networks (e.g., 5G), base-stations equipped with hundreds of antennas are likely to be deployed in practice [31]. This implies that Proposition 1 is useful when base-station plays the role of Bob and a UE (user-equipment) plays the role of Alice.

While the above proposition shows the advantage of employing large number of receive antennas to combat the CA, in the rest of this section, we present numerical results to understand the cumulative distribution function (CDF) of $R_{N_r,k}^{(attack)}$ when N_r is not large. To generate the numerical results, we assume that the channels $h_{k,j}^{(AB)}, h_k^{(AE)}$ and $h_{k,j}^{(EB)}$ are i.i.d., and are distributed as $\mathcal{CN}(0,1)$. We also assume that w_k is distributed as $\mathcal{CN}(0,1)$. When the transmitted bit is 1, let $E_{total} = E_{Alice} + E_{Eve,C}$ be the average received energy at every antenna of Bob, out of which, $E_{Eve,C}$ be the signal energy contributed by Eve. We define

$$\eta \triangleq \frac{E_{Eve,C}}{E_{total}} \times 100, \tag{20}$$

as the percentage of average energy contributed by Eve when the transmitted bit is 1. In Fig. 3, we plot the CDFs of the random variable $\frac{R_{N_r,k}^{(attack)}}{N_r}$ when w_k is Gaussian distributed. For computing the CDFs, we use $E_{total} = 1$. The plots in Fig. 3 show that as N_r increases, the CDFs shift towards right, thereby driving the cross-over probability to lower values.

$$E_{bit-1} = \sum_{j=1}^{N_r}\left|\sqrt{E_{Alice}} h_{k,j}^{(AB)} + \sqrt{E_{Eve,C}} h_k^{(AE)} w_k h_{k,j}^{(EB)} + \sqrt{\alpha\theta} n_{k,j}^{(EB)} + n_{k,j}^{(B)}\right|^2 \tag{21}$$

$$\tilde{E}_{bit-1} = \sum_{j=1}^{N_r}\left|\sqrt{E_{Alice}} h_{k,j}^{(AB)} + \sqrt{E_{Eve,C}} \tilde{h}_{k,j}^{(AEB)} + \sqrt{\alpha\theta} \tilde{n}_{k,j}^{(EB)} + n_{k,j}^{(B)}\right|^2 \tag{22}$$

$$R_{N_r,k}^{(attack)} = \sum_{j=1}^{N_r}\left(\left|\sqrt{E_{Alice}} h_{k,j}^{(AB)}\right|^2 + \left|\sqrt{E_{Eve,C}} h_k^{(AE)} w_k h_{k,j}^{(EB)}\right|^2\right) + \sum_{j=1}^{N_r}\left(\sqrt{E_{Alice}E_{Eve,C}}\, 2\mathcal{R}\left(h_{k,j}^{*(AB)} h_k^{(AE)} w_k h_{k,j}^{(EB)}\right)\right) \tag{14}$$

$$\text{Prob}\left(\frac{R_\Delta}{N_r} > -\epsilon\right) = \text{Prob}\left(\left(\frac{1}{N_r}\left(\sum_{j=1}^{N_r}\left|\sqrt{E_{Eve,C}} h_k^{(AE)} w_k h_{k,j}^{(EB)}\right|^2 + \sum_{j=1}^{N_r}\left(\sqrt{E_{Eve,C}E_{Alice}}\, 2\mathcal{R}\left(h_{k,j}^{*(AB)} h_k^{(AE)} w_k h_{k,j}^{(EB)}\right)\right)\right)\right) > -\epsilon\right) \tag{15}$$

$$\text{Prob}\left(\frac{R_\Delta}{N_r} > -\epsilon\right) \geq \text{Prob}\left(\left|\frac{1}{N_r}\sum_{j=1}^{N_r}\left(\sqrt{E_{Alice}E_{Eve,C}}\, 2\mathcal{R}\left(h_{k,j}^{*(AB)} h_k^{(AE)} w_k h_{k,j}^{(EB)}\right)\right)\right| < \epsilon\right) \tag{16}$$

$$= \text{Prob}\left(\left|\left(\frac{1}{N_r}\sum_{j=1}^{N_r}\left(\sqrt{E_{Alice}E_{Eve,C}}\, 2\mathcal{R}\left(h_{k,j}^{*(AB)} h_k^{(AE)} w_k h_{k,j}^{(EB)}\right)\right)\right) - 0\right| < \epsilon\right) \tag{17}$$

$$> 1 - \epsilon. \tag{18}$$

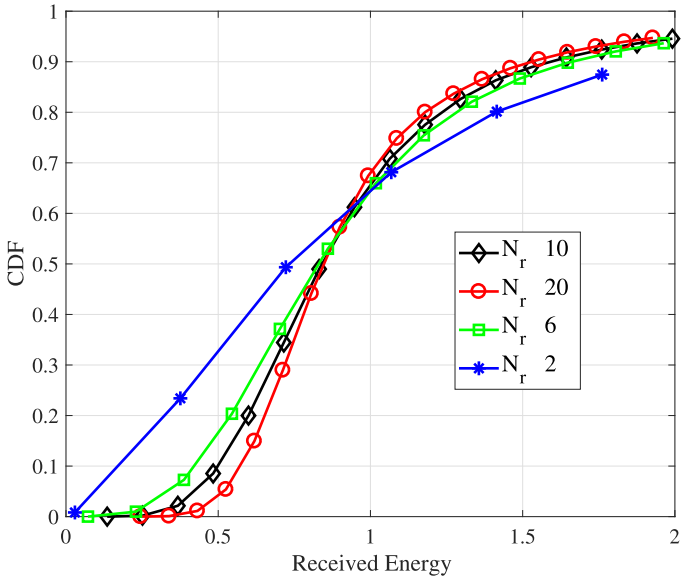

Fig. 3. CDFs of the average received energy across N_r antennas at Bob. The parameter η, as given in (20), denotes the percentage of energy contributed by Eve at Bob. The plots show that multiple receive antennas at Bob helps to reduce the attack effect.

$$\tilde{E}_{bit-0} = \sum_{j=1}^{N_r} \left| \sqrt{\alpha\theta}\tilde{n}_{k,j}^{(EB)} + n_{k,j}^{(B)} \right|^2 \tag{23}$$

B. Effect of Multiple Antennas at Eve

We acknowledge that Bob's trick to garner energy for detection comes from using multiple antennas. To keep the comparison fair, we study the effect of CA when Eve is also equipped with multiple antennas. Considering $N_r = 1$, the total energy at Bob without additive noise at Alice and Bob is given by

$$\left| \sqrt{E_{Alice}} h_k^{(AB)} + \sum_{l=1}^{N_e} \left(\sqrt{\frac{\alpha\theta E_{Alice}}{N_e}} \right) h_{k,l}^{(EB)} h_{k,l}^{(AE)} w_{k,l} \right|^2, \tag{24}$$

where N_e denotes the number of antennas at Eve, $w_{k,l}$, which is distributed as $\mathcal{CN}(0,1)$, is the scalar used at the l-th antenna of Eve, $h_{k,l}^{(EB)}$ is the channel from the l-th antenna at Eve to Bob, and $h_{k,l}^{(AE)}$ is the channel from Alice to the l-th antenna at Eve. In the case of single antenna at Eve, the energy at Bob is

$$\left| \sqrt{E_{Alice}} h_k^{(AB)} + \sqrt{\alpha\theta E_{Alice}} h_{k,1}^{(EB)} h_{k,1}^{(AE)} w_{k,1} \right|^2 \tag{25}$$

where the main difference between (24) and (25) is the distribution of the random variables

$$\sum_{l=1}^{N_e} \frac{1}{\sqrt{N_e}} h_{k,l}^{(EB)} w_{k,l} h_{k,l}^{(AE)} \tag{26}$$

with $N_e > 1$ and with $N_e = 1$. With $N_e > 1$, since (26) is the sum of product of three independent Gaussian random variables, we have observed that the CDF of $|\sum_{l=1}^{N_e} \frac{1}{\sqrt{N_e}} h_{k,l}^{(EB)} w_{k,l} h_{k,l}^{(AE)}|^2$ grows much slower than that of $|h_{k,1}^{(EB)} w_{k,1} h_{k,1}^{(AE)}|^2$, as shown in Fig. 4. As a result, for a given E_{th}, the probability of decoding bit-1 as bit-0 decreases when multiple antennas are used at Eve.

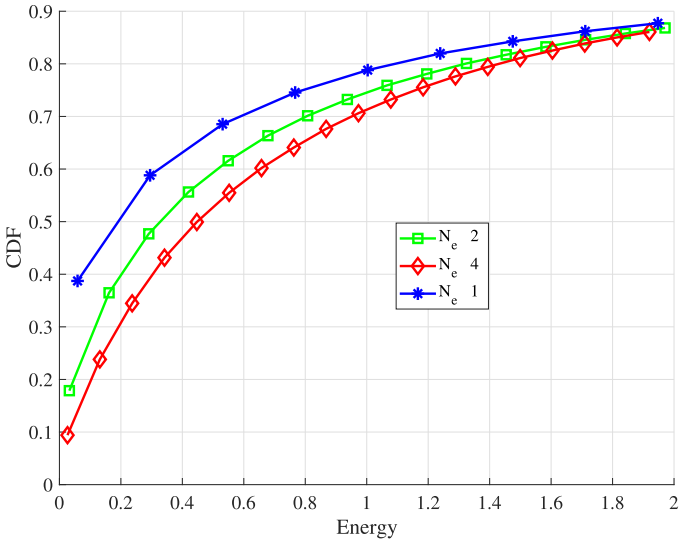

Fig. 4. CDFs of $|\cdot|^2$ of random variables in (26), where $|\cdot|$ denotes the absolute value of a complex number. The plots indicate that using multiple antennas at Eve changes the energy distribution at Bob.

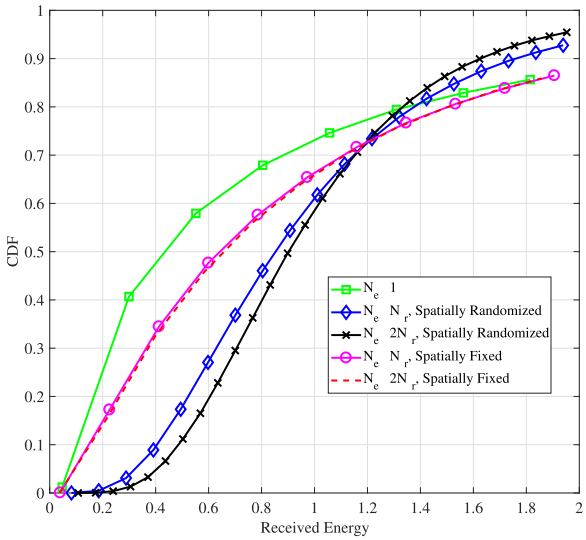

Fig. 5. Comparison of CDFs of the average received energy across N_r antennas at Bob for various strategies employed at Eve. For the results, we fix $N_r = 10$ and $\eta = 90\%$. The number of antennas at Eve is denoted by N_e. The plots highlight that it is better for Eve to equip only one antenna in order increase the attack effect.

Furthermore, we compute the CDFs of the received energy across the N_r antennas at Bob when $N_r \geq 1$ and Eve uses the following strategies: (i) single-antenna, (ii) multiple-antenna with spatially randomized waveforms - $\{w_{k,l} \mid 1 \leq l \leq N_e\}$ are independent, and (iii) multiple-antenna with spatially fixed waveforms - $\{w_{k,l} = w_k \mid 1 \leq l \leq N_e\}$. To give advantage to Eve, we have also considered the case when $N_e = 2N_r$. The CDFs, which are presented in Fig. 5, highlight that employing multiple

antennas at Eve does not aggravate the attack effect as multiple antennas assists Bob in receiving more energy than the single-antenna case. Due to lack of closed-form expressions on the CDFs of energy collected at Bob, we do not have concrete theoretical insights on this argument. Nevertheless, based on the simulation results, we advocate the use of single antenna at Eve and multiple antennas at Bob. In Section IV-D, we also present the BER performance of OOK with and without multiple antennas at Eve to reinforce this observation.

C. Design of Threshold E_{th}

Having studied the energy distributions during the ON state of OOK, we now address the computation of E_{th} in (11) to optimize the error-performance at Bob. With CA, the signal energy collected across N_r antennas during the ON state is given by (21) , where $h_{k,j}^{(AB)}$ and $h_{k,j}^{(EB)}$ denote the equivalent channels seen by the j-th antenna of Bob on the k-th symbol. Similarly, energy collected during the OFF state is

$$E_{bit-0} = \sum_{j=1}^{N_r} \left| \sqrt{\alpha\theta} n_{k,j}^{(EB)} + n_{k,j}^{(B)} \right|^2. \tag{27}$$

To determine the optimal threshold we need to solve

$$E_{th}^* = \arg min_{E_{th}} \text{Prob}(E_{bit-1} \leq E_{th}) + \text{Prob}(E_{bit-0} > E_{th}), \tag{28}$$

which in turn requires Bob to measure the Probability Density Functions (PDFs) on E_{bit-1} and E_{bit-0}. Towards that direction, we assume that Bob can learn the distributions empirically using pilots, which are periodically transmitted by Alice. Note that the persistent nature of the CRFH attack helps in measuring the energy distributions with attack, otherwise, Bob is forced to employ threshold values based on the energy distribution of $\sqrt{E_{Alice}} h_k^{(AB)}$, which in turn degrades the error-performance under convolution attack. From E_{bit-1} and E_{bit-0}, we observe that $\{h_k^{(AE)} w_k h_{k,j}^{(EB)} \mid 1 \leq j \leq N_r\}$ are uncorrelated but not necessarily independent. Similarly, the random variables $\{n_{k,j}^{(EB)} \mid 1 \leq j \leq N_r\}$ are also uncorrelated but not independent. Due to challenges in obtaining the closed-form expressions on the PDFs of E_{bit-1} and E_{bit-0}, we approximate $\{h_k^{(AE)} w_k h_{k,j}^{(EB)} \mid 1 \leq j \leq N_r\}$ to be statistically independent and Gaussian distributed as $\mathcal{CN}(0,1)$, and then arrive at a sub-optimal solution. Similarly, $\{n_{k,j}^{(EB)} \mid 1 \leq j \leq N_r\}$ is also assumed i.i.d., where each $n_{k,j}^{(EB)}$ is distributed as $\mathcal{CN}(0, \sigma_{Eve}^2)$. Using such approximations, the corresponding versions of received energy are given by (22) and (23), where $\tilde{h}_{k,j}^{(AEB)}$ and $\tilde{n}_{k,j}^{(EB)}$ are Gaussian distributed. We immediately note that $\tilde{E}_{bit-1}$ can be written as

$$\tilde{E}_{bit-1} = \frac{1}{2}(E_{Alice} + E_{Alice}\alpha\theta + \alpha\theta\sigma_{Eve}^2 + \sigma_{Bob}^2)\chi_1$$

where χ_1 is Chi-square distributed with degrees of freedom $2N_r$. Similarly, $\tilde{E}_{bit-0}$ can be written as

$$\tilde{E}_{bit-0} = \frac{1}{2}\left(\alpha\theta\sigma_{Eve}^2 + \sigma_{Bob}^2\right)\chi_2$$

where χ_2 is also a Chi-square distributed random variable with degrees of freedom $2N_r$. With this, the approximate solution, henceforth denoted as $\tilde{E}_{th}^*$, is computed as in (29), shown at the bottom of the page, wherein $\gamma(\cdot,\cdot)$ is the lower incomplete gamma function. Unlike the optimal solution in (28), the solution in (29) can be obtained using numerical methods on incomplete gamma function.

D. Error-Performance of OOK Against Convolution Attack

In this section, we present simulation results on the error-performance of OOK against the CA. To carry out the experiments, we assume that the channels $\{h_{k,j}^{(AB)}(f_c) \mid f_c \in \mathcal{F}\}$ across the N narrowbands are statistically independent and distributed as $\mathcal{CN}(0,1)$. Similarly, the sets of channels $\{h_k^{(AE)}(f_c) \mid f_c \in \mathcal{F}\}$ and $\{h_{k,j}^{(EB)}(f_c) \mid f_c \in \mathcal{F}\}$ are also i.i.d. across the N narrowbands, and are distributed as $\mathcal{CN}(0,1)$.

To showcase the effect of CA, we present the error-performance of the non-coherent OOK scheme along with the schemes discussed in Section III-A, namely, (i) Narrowband jamming (NJ), and (ii) the CA, on binary phase shift keying (BPSK) with coherent maximum-likelihood detection at Bob. In Fig. 6, we plot the BER curves of the above schemes against $\frac{E_b}{N_0} = \frac{E_{Alice}}{2\sigma_{Bob}^2}$ for $N_r = 2$ and $N_r = 10$. For CA on OOK, we use two different threshold values for energy detection, namely: E_{th}^* in (28), and $\tilde{E}_{th}^*$ in (29), which are computed based on the attack parameters. The plots show that the Gaussian approximation to compute $\tilde{E}_{th}^*$ does not result in significant loss in the error-performance. Moreover, the error-performance of OOK is better than that of coherent modulation method under the CA. Similar to the results in Fig. 6, we also present the BER curves of OOK with $N = 1024$ in Fig. 7. The plots highlight that it is important for Alice and Bob to identify the CA, and then mitigate it by employing OOK based strategy.

Finally, in Fig. 8, we present the error-performance of OOK when Eve is equipped with multiple antennas, and when $\theta = 9, \alpha = 100\%$ and $N = 1024$. Similar to the observations in Section IV-B, Fig. 8 confirms that multiple antennas at Eve does not aggravate the attack effect. For the simulations, the threshold values for energy detection are computed based on the energy distribution during the ON and the OFF states similar to the one in (28).

$$\begin{aligned}\tilde{E}_{th}^* &= \arg min_{E_{th}} \text{Prob}\left(\chi_1 \leq \frac{2E_{th}}{E_{Alice} + E_{Alice}\alpha\theta + \alpha\theta\sigma_{Eve}^2 + \sigma_{Bob}^2}\right) + \text{Prob}\left(\chi_2 > \frac{2E_{th}}{\alpha\theta\sigma_{Eve}^2 + \sigma_{Bob}^2}\right) \\ &= \arg min_{E_{th}} \gamma\left(N_r, \frac{E_{th}}{E_{Alice} + E_{Alice}\alpha\theta\sigma_{Eve}^2 + \alpha\theta + \sigma_{Bob}^2}\right) - \gamma\left(N_r, \frac{E_{th}}{\alpha\theta\sigma_{Eve}^2 + \sigma_{Bob}^2}\right)\end{aligned} \tag{29}$$

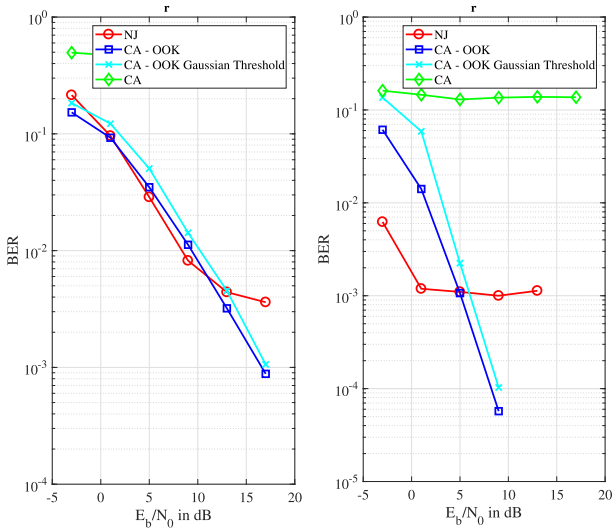

Fig. 6. Error-performance of OOK against convolution attack (CA) on an FH system with $N = 128$. Since the attack is persistent, Bob measures the energy distributions during the attack to design the threshold E^*_{th}. The choice of $\tilde{E}^*_{th}$, which is based on Gaussian approximation marginally degrades the performance compared to that when using the optimal value E^*_{th}.

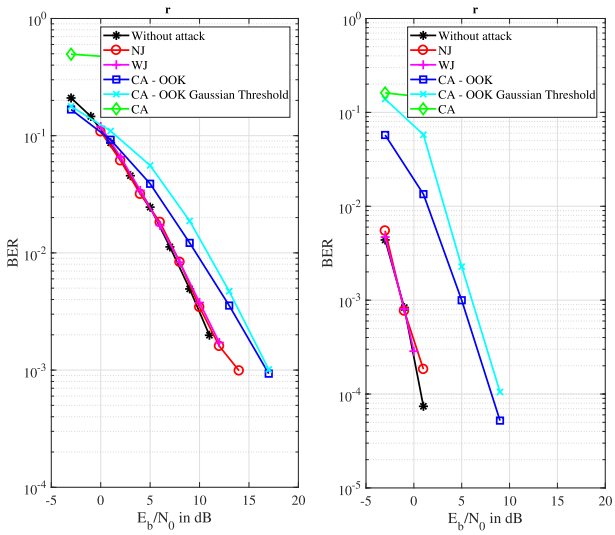

Fig. 7. Error-performance of OOK against convolution attack (CA) on an FH system with $N = 1024$. Since the attack is persistent, Bob measures the energy distributions during the attack to design the thresholds E^*_{th} and $\tilde{E}^*_{th}$.

Remark 1. The error-performance of OOK, as presented in Fig. 6 and Fig. 7, captures the best-case results from the perspective of Alice and Bob. This is attributed to the assumption that Eve executes the convolution attack persistently on both the pilot symbols and the data symbols with the same parameters α and θ. However, when Eve selectively attacks only the data symbols, then the corresponding estimate of the threshold will be suboptimal, which in turn will result in degraded performance.

E. Limitations of OOK Against Wideband Jamming

In this section, we explore the idea of changing Eve's strategy to wideband jamming (WJ) once Alice and Bob switch to

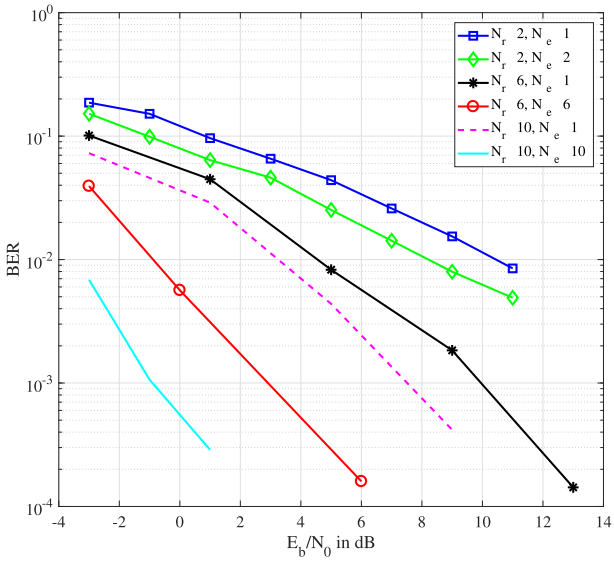

Fig. 8. Error-performance of OOK against CA when Eve is equipped with multiple antennas. The plots show that the best attack strategy for Eve is to mount just one antenna.

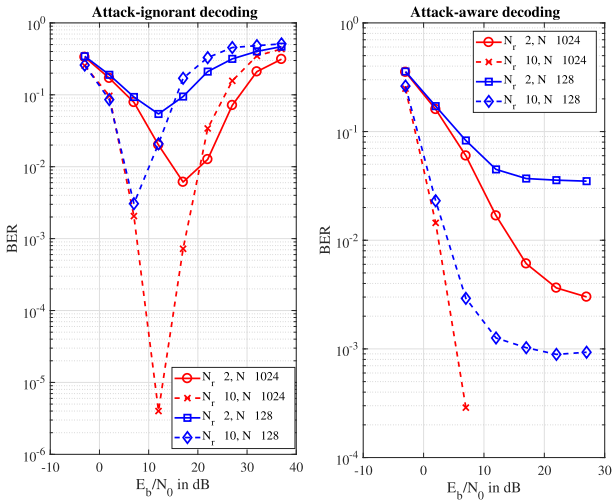

Fig. 9. Error-performance of OOK against wideband jamming on an FH system with $N = 128$ and $N = 1024$. We use $\theta = 9$ to generate the results.

OOK in response to CA. In WJ, Eve uniformly divides her energy $E_{Eve} = \theta E_{Alice}$ across the N narrowbands. The rationale behind this switch is to exploit lower threshold values used for energy detection, thereby forcing Bob to decode bit-0 as bit-1. We first capture the consequence of an attack-ignorant detection in Fig. 9 (left-side), which shows the BER performance of OOK when E_{th} is optimized based on E_{Alice} and σ^2_{Bob}. Since E_{th} is chosen based on E_{Alice}, and E_{Alice} is much lower than E_{Eve}, BER increases with large values of jamming energy; this is mainly contributed by the error event of decoding bit-0 as bit-1. In the attack-aware case, Bob measures the jamming energy using the pilots, and then takes it into account when designing E_{th} (this is possible due to the persistent nature of the attack). The error-performance of such a strategy is also presented in Fig. 9 (right-side), which shows that unlike the case of

attack-ignorant detection, the BER experiences error-floor behaviour when E_b/N_o is large; this is because the threshold value linearly increases with E_{Alice}, thereby saturating the probability of decoding bit-0 as bit-1, and vice versa. In summary, although OOK mitigates CA, a combination of CA followed by WJ can result in degraded error-performance at Bob when E_b/N_o is large.

V. Convolution Attack on FH Based Frequency Shift Keying

In this section, we study the impact of CA on Binary-FSK (BFSK) based FH scheme as an alternate countermeasure. We have chosen BFSK as the modulation scheme as most military and commercial frequency hopping systems use frequency shift keying. Unlike the generic attack in Section II, the objective of CRFH in this case is to create confusion at Bob when decoding the BFSK modulated symbols. In this attack, Eve uses an appropriate baseband signal $w(t)$ to forward a frequency-shifted version of the received passband signal so that the tones carrying bit-0 and bit-1 have comparable energy levels at Bob.

A. Signal Model for BFSK Without Attack

At Alice, bit-1 is transmitted by using the carrier-frequency $f_c+\beta$, and bit-0 is transmitted by using the carrier-frequency $f_c-\beta$, for some $f_c \in \mathcal{F}$ (given in Section II). We assume that $0<\beta<\frac{\Delta}{2}$, where Δ is the spacing between adjacent carrier-frequencies. We use $b_k \in \{0,1\}$ to denote the bit transmitted at the k-th symbol-period, and $\bar{b}_k$ to denote the complement of b_k. To communicate b_k, Alice transmits the tone f_k, given by

$$f_k = \begin{cases} f_c+\beta, & \text{if } b_k=1, \\ f_c-\beta, & \text{otherwise}, \end{cases} \tag{30}$$

where f_c is chosen based on the shared secret-key between Alice and Bob. Overall, the total set of tones used by Alice and Bob is $\mathcal{T}=\{f_i+\beta, f_i-\beta, \mid i=1,2,\ldots,N\}$. In this model, we assume $N_e=1$ and $N_r=1$.

Without any attack, the received complex-baseband symbols at Bob are of the form

$$y_{k,main} = \sqrt{E_{Alice}}h_k^{(AB)} + n_{k,main}^{(B)}, \tag{31}$$

$$y_{k,side} = n_{k,side}^{(B)}, \tag{32}$$

where $y_{k,main}$ and $y_{k,side}$ are the symbols received on the tones $f_c+\beta$ and $f_c-\beta$ depending on b_k. When bit-1 is transmitted, $y_{k,main}$ and $y_{k,side}$ correspond to the symbols on the tones $f_c+\beta$ and $f_c-\beta$, respectively. Similarly, when bit-0 is transmitted, $y_{k,main}$ and $y_{k,side}$ correspond to the symbols on the tones $f_c-\beta$ and $f_c+\beta$, respectively. Here, the additive white Gaussian noise (AWGN) components $n_{k,main}^{(B)}$ and $n_{k,side}^{(B)}$ are i.i.d. as $\mathcal{CN}(0,\sigma_{Bob}^2)$. Stitching the above together, the received symbols on the tones $f_c+\beta$ and $f_c-\beta$ are given by

$$y_k(f_c+\beta) = \begin{cases} y_{k,main}, & \text{if } b_k=1; \\ y_{k,side}, & \text{otherwise.} \end{cases} \tag{33}$$

$$y_k(f_c-\beta) = \begin{cases} y_{k,main}, & \text{if } b_k=0; \\ y_{k,side}, & \text{otherwise.} \end{cases} \tag{34}$$

In (33) and (34), we have assumed that the two tones $f_c-\beta$ and $f_c+\beta$ experience identical channel realization (assuming a large coherence-bandwidth).

B. Signal Model for BFSK With Attack

With CA, we assume that Eve has the knowledge of β, and she chooses the waveform $w(t)$ so that some energy is added on the received tone $f_k \in \mathcal{T}$ and also on the side-tones $f_k+2\beta$ and $f_k-2\beta$. Note that Eve does not know whether f_k is $f_c+\beta$ or $f_c-\beta$, for some f_c. Therefore, she uniformly divides her energy on both the side-tones $f_k+2\beta$ and $f_k-2\beta$ so that the attack is successful irrespective of the transmitted bit. Assuming frequency-flat equivalent channel at Bob, the received symbols under the CA are given by

$$\begin{aligned} y_{k,main} &= \sqrt{E_{Alice}}h_k^{(AB)} + \sqrt{\alpha\theta E_{Alice}}h_{k,main}^{(AEB)} \\ &\quad + \sqrt{\alpha\theta}n_k^{(EB)} + n_{k,main}^{(B)}, \end{aligned} \tag{35}$$

$$\begin{aligned} y_{k,side} &= \sqrt{\frac{(1-\alpha)\theta E_{Alice}}{2}}h_{k,side}^{(AEB)} \\ &\quad + \sqrt{\frac{(1-\alpha)\theta}{2}}n_k^{(EB)} + n_{k,side}^{(B)}, \end{aligned} \tag{36}$$

where $\sqrt{\alpha\theta}$ and $\sqrt{\frac{(1-\alpha)}{2}\theta}$ are the gains applied by Eve on the received tone and on either of the side-tones, respectively. Based on the nature of operations at Eve, we model the complex channels $h_{k,main}^{(AEB)}$ and $h_{k,side}^{(AEB)}$ as

$$h_{k,main}^{(AEB)} \triangleq h_k^{(AE)}w_k h_k^{(EB)} \text{ and } h_{k,side}^{(AEB)} \triangleq h_k^{(AE)}u_k h_k^{(EB)},$$

respectively, where $h_k^{(AE)}$ is the channel from Alice to Eve, distributed as $\mathcal{CN}(0,1)$, $h_k^{(EB)}$ is the channel from Eve to Bob, distributed as $\mathcal{CN}(0,1)$, and w_k and u_k are the statistically independent random variables obtained from the waveform $w(t)$. Similarly, the forwarded AWGN components from Eve are $n_{k,main}^{(EB)} \triangleq h_k^{(EB)}w_k n_k^{(E)}$ and $n_{k,side}^{(EB)} \triangleq h_k^{(EB)}u_k n_k^{(E)}$, where $n_k^{(E)}$ is distributed as $\mathcal{CN}(0,\sigma_E^2)$. Henceforth, we denote $\alpha\theta E_{Alice}$ and $\frac{(1-\alpha)}{2}\theta E_{Alice}$ as $E_{Eve,main}$ and $E_{Eve,side}$, respectively.

To decode the information bits, Bob uses non-coherent energy detection rule given by

$$\hat{b}_k = \begin{cases} 1, & \text{if } |y_k(f_c+\beta)|^2 > |y_k(f_c-\beta)|^2; \\ 0, & \text{0therwise.} \end{cases} \tag{37}$$

where $\hat{b}_k$ denotes the estimate of b_k, and $y_k(f_c+\beta)$ and $y_k(f_c-\beta)$ are as given in (33) and (34), respectively.

C. Events Affecting Error-Performance at Bob

In the CA, Eve can vary her energy levels $E_{Eve,main}$ and $E_{Eve,side}$ so that the energy levels of the main channel $\sqrt{E_{Alice}}h_k^{(AB)} + \sqrt{E_{Eve,main}}h_{k,main}^{(AEB)}$ and the side channel $\sqrt{E_{Eve,side}}h_{k,side}^{(AEB)}$ are close enough to create confusion at Bob. Since Alice and Bob hop across a wide range of narrowbands, Eve cannot learn the narrowband instantaneously, and

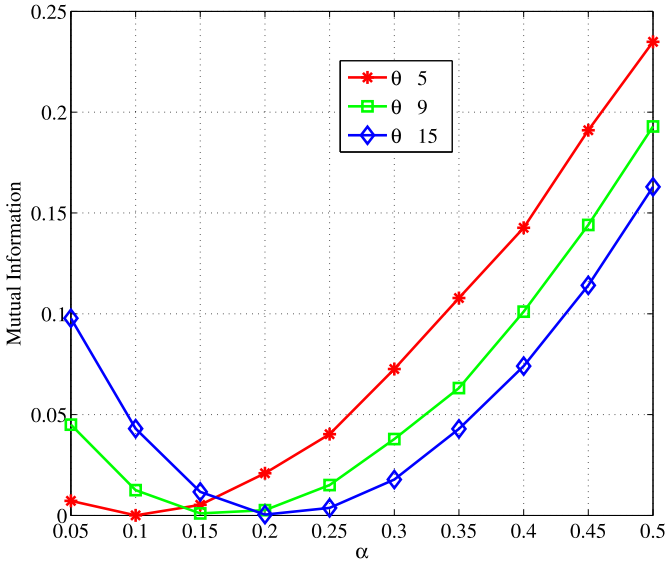

Fig. 10. Numerically computed values of α that maximize the impact of the attack. The best attack strategy is to pour higher energy on the side channels as the main channel already contains energy contributed by Alice.

therefore she cannot force the channel realizations to a specific value with probability one. However, she can change the distribution of the received energy on the tones $f_c + \beta$ and $f_c - \beta$ at Bob by varying the value of α. Along that direction, an interesting question is: *What is the optimal value of α that degrades the error-performance at Bob?*

We now discuss the right choice of the parameter α from the attacker's perspective. With no additive-noise at Eve and Bob, the received energy on the tone chosen by Alice is

$$E_{main} = E_{Alice} \left| h_k^{(AB)} + \sqrt{\alpha\theta} h_k^{(AE)} w_k h_k^{(EB)} \right|^2. \quad (38)$$

Similarly, the received energy on the complementary tone is

$$E_{side} = E_{Alice} \left| \sqrt{\frac{1-\alpha}{2}\theta} h_k^{(AE)} u_k h_k^{(EB)} \right|^2. \quad (39)$$

Since E_{main} and E_{side} are random variables, the objective of the attacker is to choose α such that

$$p_{cross} \triangleq \text{Prob}(E_{main} > E_{side}) = \frac{1}{2}.$$

In other words, the objective is to drive the mutual information $I(b_k; \hat{b}_k) = 1 - H(p_{cross}) = 0$, where $H(\cdot)$ is the entropy function. We have empirically computed the mutual information values $I(b_k; \hat{b}_k)$ against various values of α over an ensemble of realizations of the random variables $h_k^{(AB)}$, $h_k^{(AE)}$, $h_k^{(EB)}$, w_k and u_k. To generate the numerical results, we use $E_{Alice} = 1$ and $\theta = 5, 9, 15$. We assume that w_k and u_k are independent and distributed as $\mathcal{CN}(0, 1)$. The computed mutual information values are presented in Fig. 10 as a function of α for several values of θ. The plots suggest that the attack impact can be maximized by choosing $\alpha = 0.1, 0.15, 0.2$ for $\theta = 5, 9, 15$, respectively. Note that larger value of α decreases the cross-over probability, thereby increasing the mutual information of the channel. Similarly, values of α lower than the above optimal values increases the cross-over probability more than 0.5, using which the receiver can achieve cross-over probability less than 0.5 by flipping the decoded bits on each symbol.

Since the density functions on E_{main} and E_{side} are not analytically tractable, the following theorem provides closed-form expressions on sub-optimal values of α by approximating $h_{k,main}^{(AEB)}$ and $h_{k,side}^{(AEB)}$ to be Gaussian distributed.

$$\mathbb{E}_{|h_{side}^{(AEB)}|^2} \left(\text{Prob} \left(E_{main} > \left(\frac{1-\alpha}{2} \right) \theta |h_{side}^{(AEB)}|^2 \right) \right) = \frac{2 + 2\alpha\theta}{2 + \alpha\theta + \theta} \quad (40)$$

Theorem 1. Under the assumption that $h_{k,main}^{(AEB)}$ and $h_{k,side}^{(AEB)}$ are statistically independent complex Gaussian random variables, with $\sigma_{Eve}^2 = \sigma_{Bob}^2 = 0$, the optimal value of α (denoted by α^*) which minimizes the mutual information $I(b_k; \bar{b}_k)$ is $\frac{\theta-2}{2\theta}$.

Proof. In (38) and (39), the variables w_k and u_k are statistically independent with zero mean and unit variance. We note that the random variables $h_k^{(AE)} u_k h_k^{(EB)}$ and $h_k^{(AE)} w_k h_k^{(EB)}$ are uncorrelated but not statistically independent. Furthermore, since the distribution on the product of the three Gaussian random variables is not tractable, we seek to obtain α by assuming that $h_k^{(AE)} u_k h_k^{(EB)}$ and $h_k^{(AE)} w_k h_k^{(EB)}$ are Gaussian distributed and statistically independent. We need to choose α such that $\text{Prob}(E_{main} > E_{side}) = 0.5$. From (38) and (39), we note that E_{Alice} is a common factor in both E_{main} and E_{side}, and therefore, without loss of generality, we assume $E_{Alice} = 1$. In the rest of this proof, we compute $\text{Prob}(E_{main} > E_{side})$ as a function of α and θ, and subsequently obtain α that achieves cross-over probability 0.5. First, we compute $\text{Prob}(E_{main} > E_{side} = e_{side})$, where e_{side} is a realization of the random variable E_{side}. Since E_{main} is exponential distributed with mean $(1 + \alpha\theta)$, the above probability can be written as

$$\text{Prob}(E_{main} > E_{side} = e_{side}) = e^{\frac{-e_{side}}{1+\alpha\theta}}.$$

Replacing e_{side} by $\frac{1-\alpha}{2}\theta |h_{side}^{(AEB)}|^2$, we have

$$\text{Prob} \left(E_{main} > \left(\frac{1-\alpha}{2} \right) \theta |h_{side}^{(AEB)}|^2 \right) = e^{\frac{-((\frac{1-\alpha}{2})\theta |h_{side}^{(AEB)}|^2)}{1+\alpha\theta}}.$$

Finally, since $|h_{side}^{(AEB)}|^2$ is also exponentially distributed, we take the average of the above expression with respect to $|h_{side}^{(AEB)}|^2$ to obtain (40). In order to obtain the above probability to be 0.5, the variable α^* must satisfy the constraint $\alpha^* = \frac{\theta-2}{2\theta}$.

D. Simulation Results

In this section, we demonstrate the error-performance of BFSK based FH under CA. To carry out the experiments, we assume that the channels $\{h_{k,j}^{(AB)}(f_c) \mid f_c \in \mathcal{F}\}$ across the N narrowbands are statistically independent and distributed as $\mathcal{CN}(0, 1)$. Similarly, $\{h_k^{(AE)}(f_c) \mid f_c \in \mathcal{F}\}$ and $\{h_{k,j}^{(EB)}(f_c) \mid f_c \in \mathcal{F}\}$ are also i.i.d. as $\mathcal{CN}(0, 1)$ across the N narrowbands.

To showcase the effect of CA, we present the error-performance of: (i) *BFSK based FH without attack* and (ii) *BFSK*

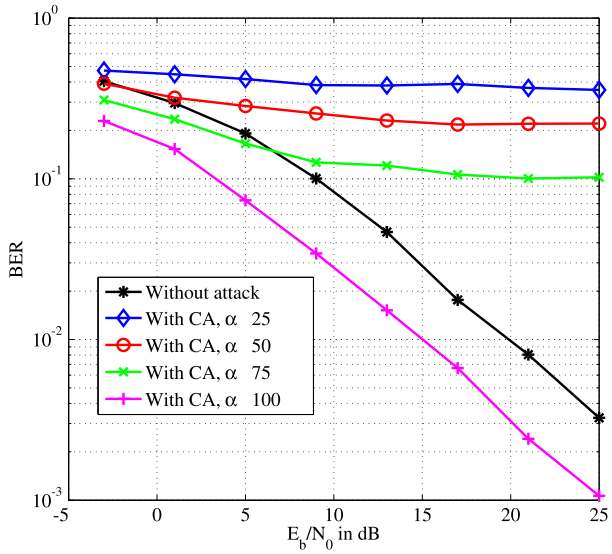

Fig. 11. Error-performance of BFSK against CA for various values of α. In the CA, α fraction of total energy at Eve is spent on received carrier-frequency f_k, $\frac{1-\alpha}{2}$ fraction each on $f_k + 2\beta$ and $f_k - 2\beta$. Interestingly, $\alpha = 100\%$ outperforms the no-attack case as Eve's signals help Bob in decoding.

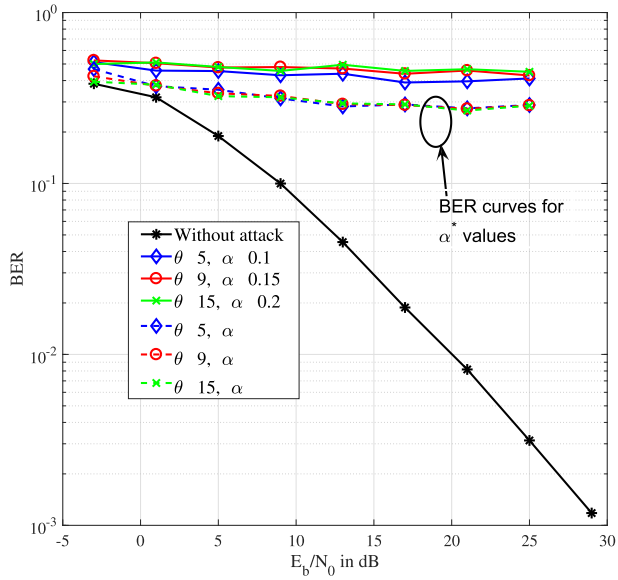

Fig. 12. Error-performance of BFSK against CA when α is computed using Gaussian assumptions on $h_{k,main}^{(AEB)}$ and $h_{k,side}^{(AEB)}$.

based FH with CA. In the latter scheme, Eve executes the CA with various values of α. Specifically, α fraction of the total energy at Eve is used for corrupting the main channel, while $\frac{1-\alpha}{2}$ fraction of it is used to introduce additional energy on either of the side-tones. We use $\theta = 9$, i.e., as Alice increases E_{Alice}, Eve also increases E_{Eve} proportionately. For the AWGN, we use $\sigma^2_{Bob} = 1$ and $\sigma^2_{Eve} = 0.01$. In Fig. 11, we plot the BER curves of the above two schemes against $\frac{E_b}{N_0} = \frac{E_{Alice}}{\sigma^2_{Bob}}$. The plots confirm our observations from the previous section that it is a better strategy for Eve to use α that ensures comparable energy levels on the two tones $f_c + \beta$ and $f_c - \beta$. In Fig. 12, we also plot the BER when closed-form expression on α^* (from Theorem 1) is used. The plots show that although these values of α are not optimal, they continue to result in degraded error-performance at Bob.

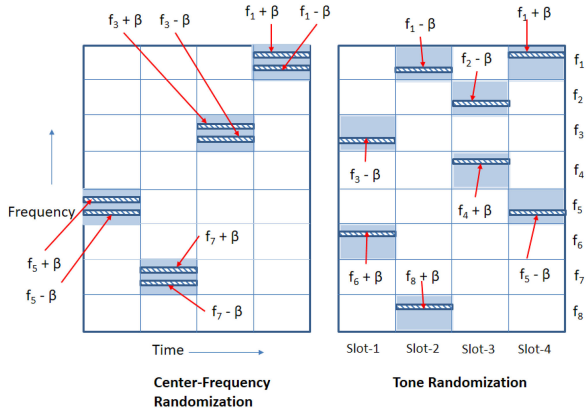

Fig. 13. Pictorial representation of traditional BFSK (left-side) and enhanced BFSK (right-side) with eight carrier-frequencies and four time-slots. With EBFSK, tone randomization helps in mitigating the CA on BFSK based FH.

E. Mitigation Strategy: Enhanced BFSK

In the existing BFSK based FH scheme, randomness is applied on the choice of the carrier-frequency $f_c \in \mathcal{F}$ but not on the choice of the tones $f_c + \beta$ and $f_c - \beta$. This implies, given f_k at Eve, the tone on which bit-$\bar{b}_k$ is encoded is deterministic upto 1 bit of randomness, and this weakness is specifically exploited by Eve during the CA. Therefore, from the legitimate users' perspective, they must obfuscate the location of the tones $f_c + \beta$ and $f_c - \beta$. This way, Eve cannot introduce significant energy on the tone that carries bit-$\bar{b}_k$. To achieve this mitigation strategy, we enable Alice and Bob to share a secret-key using which the random positions of the side-tones are determined. As a consequence, Eve cannot learn their locations. Meanwhile, Bob's strategy is to observe the appropriate pair of tones, and then apply non-coherent energy detection to decode the information bits.

We refer to the proposed mitigation strategy as Enhanced BFSK (EBFSK), wherein a pair of tones is randomly chosen from the set $\mathcal{T}$ based on a secret-key, and one of them is used to communicate bit-1 and the other for bit-0. Since this selection is based on a shared-key, Bob observes the symbols on the chosen tones, and then decodes the information based on the received energy. To illustrate the above idea, we use the example depicted in Fig. 13. As shown on the left-hand side of Fig. 13, traditional BFSK based FH randomizes only the carrier-frequencies, while keeping the side-tones fixed. On the other hand, the EBFSK scheme randomizes the side-tones as shown on the right-hand side of Fig. 13. For instance, in time-slot 4, bit-1 can be encoded on the tone $f_5 - \beta$ and bit-0 can be encoded on the tone $f_1 + \beta$. With that mapping, when the attacker instantaneously receives the signal on $f_5 - \beta$, she does not know the location of the other tone which carries bit-0. As a result, executing the CA given in Section V does not guarantee degradation of error-performance at Bob.

TABLE I
CONVOLUTION ATTACK ON OOK AND BFSK

Features	On-Off Keying	Binary Frequency Shift Keying
Attack objective	Introduce deep fades	Introduce comparable energy levels on tones carrying bit-0 and bit-1
Defense	Use large number of receive antennas at Bob	Use frequency-hopping with tone randomization
Shared keys	Needed for frequency hopping	Needed for tone randomization in addition to frequency-hopping
Wideband Jamming	Error-floor behaviour at high SNR	Error-floor behaviour at high SNR
Generalization to higher-order modulation	Not effective	Fffective
Measurement of energy distribution at Bob	Needed to design E^*_{th}	Not needed
Pilot contamination by Eve	Degrades the performance	Resilient to pilot contamination

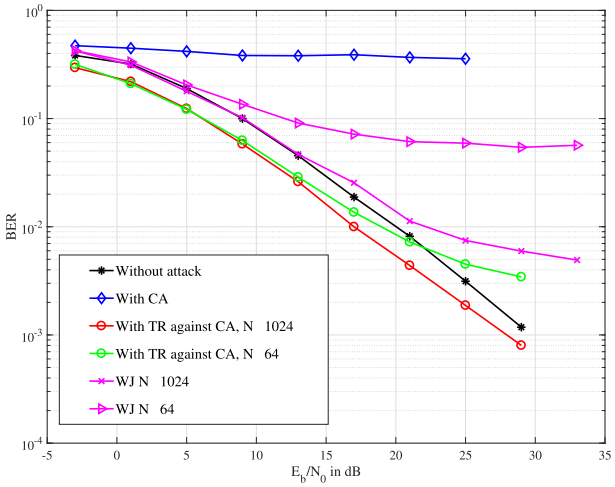

Fig. 14. Error-performance of enhanced BFSK with tone randomization (TR) against CA with $\alpha = 0.25$. With EBFSK, tone randomization helps in mitigating the CA on FH.

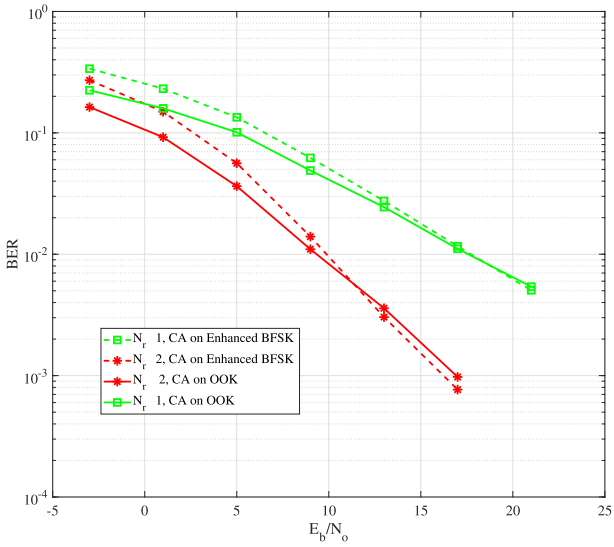

Fig. 15. Error-performance of OOK and BFSK against corresponding variants of CA on an FH system with $N = 1024$.

To demonstrate the impact of tone randomization, we present the error-performance of: (i) *CA on traditional FH based BFSK*: BFSK based FH is employed at Alice, wherein only the carrier-frequencies are subject to randomization. (ii) *CA on Enhanced BFSK*: BFSK based FH is employed at Alice, wherein all the $2N$ tones of $\mathcal{T}$ are subject to randomization. For the above two schemes, CA is executed as described in Section V with $\alpha = 25\%$. In Fig. 14, we plot the uncoded BER curves of the above schemes with $N = 64$ and $N = 1024$. The plots show that tone randomization assists the legitimate users in mitigating the CA. They also reinforce the point that larger value of N helps in mitigating the CA. This is because, given the tone for bit-b_k, the probability that either $f_k + 2\beta$ or $f_k - 2\beta$ is used for bit-$\bar{b}_k$ is $\frac{1}{2N-1}$. In contrast, the error-performance of traditional FH under CA does not depend on N as the tones carrying bit-$\bar{b}_k$ is deterministic upto 1 bit randomness.

We now discuss a possible counter-strategy by Eve to overcome the idea of tone randomization. In this strategy, Eve distributes all her energy $E_{Eve} = \theta E_{Alice}$ on wideband jamming. In Fig. 14, we also present the BER performance of EBFSK against wideband jamming when $\theta = 9$ for $N = 64$ and $N = 1024$. The plots show that the error-performance degrades as E_b/N_o increases, and the degree of degradation depends on the value of N. Similar to OOK signalling scheme, BER of BFSK experiences error-floor behaviour with increased jamming energy; this is because equal energy is injected on tones carrying bit-0 and bit-1.

VI. DISCUSSION

We have proposed convolution attacks (CA) on FH based wireless communication by full-duplex radios. We have shown that the CA can convert a slow-fading channel between the transmitter and the receiver to a rapid fading one, thereby forbidding the users to apply amplitude-modulation based signalling schemes. Subsequently, we have studied (i) FH-based OOK and (ii) FH-based BFSK, as countermeasures to mitigate the CA.

In this concluding section, we discuss some important advantages and disadvantages of the proposed countermeasures, as listed in Table I. First, we compare the error-performance of the proposed countermeasures against the corresponding variants of CA when $N = 1024$. We have used $N_r = 1, 2$ at Bob, and $N_e = 1$ at Eve. For the OOK scheme, Eve executes the CA with $\alpha = 1$ and $\theta = 9$, whereas Bob employs non-coherent energy detection to recover the bits. The threshold values for energy detection are computed using the measured energy distributions during the ON and the OFF states. For the BFSK scheme, Eve uses $\alpha = 0.15$ and $\theta = 9$ so that Bob witnesses comparable energy levels on both the tones. As a countermeasure, Alice and Bob employ EBFSK wherein the tones carrying bit-0 and bit-1 are randomized. When comparing the two schemes, we note that BFSK has lower spectral-efficiency than OOK. To keep the comparison fair, the average transmit energy of the OOK scheme is increased so as to keep the energy per bit constant between the two schemes. We have presented the BER performance of the two schemes in Fig. 15, which shows that the OOK scheme

marginally outperforms BFSK at lower values of E_b/N_o under the attack, whereas the performance of the two schemes are approximately same when E_b/N_o is high. In a nutshell, both OOK and BFSK experience similar error-performance against the CA with the exception that (i) BFSK has higher-overhead than OOK as it needs additional shared-key to randomize the tones carrying bit-1 and bit-0, and (ii) OOK requires Bob to measure the energy distributions to determine the optimal threshold E^*_{th}, whereas BFSK does not. As a result, if the CRFH attacker does not attack the pilot symbols, then BFSK continues to be effective, whereas OOK may fail due to mismatch between the estimated threshold value and the true energy distributions during the attack.

When generalizing OOK to higher-order modulations, we believe that M-PAM (Pulse Amplitude Modulation) variant of OOK for $M > 2$, will result in degraded error-performance against CA. This is because, while symbol 0 can be detected at Bob, distinguishing non-zero symbols will be a challenge as fading is completely controlled by Eve. However, when generalizing BFSK, we believe that both the attack as well as the countermeasure can be generalized to higher-order FSK.

A. Directions for Future Research

For future work, we are interested in studying the impact of convolution attack when the full-duplex radio at Eve experiences imperfect self-interference cancellation. With this constraint, we envisage memory property being introduced by the attacker since the forwarded symbol at a given time-instant will affect the subsequent symbols due to the leakage effect.

REFERENCES

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[2] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Commun. Surv. Tut.*, vol. 11, no. 4, pp. 42–56, Oct.–Dec. 2009.

[3] J. T. Chiang and Y. Hu, "Dynamic jamming mitigation for wireless broadcast networks," in *Proc. IEEE Conf. Comput. Commun.*, Phoenix, AZ, USA, 2008, pp. 1211–1219.

[4] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. 6th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2005, pp. 46–57.

[5] S. D'Oro, E. Ekici, and S. Palazzo, "Optimal power allocation and scheduling under jamming attacks," *IEEE/ACM Trans. Netw.*, vol. 25, no. 3, pp. 1310–1323, Jun. 2017.

[6] K. Pelechrinis, C. Koufogiannakis, and S. V. Krishnamurthy, "Gaming the jammer: Is frequency hopping effective?" in *Proc. 7th Int. Symp. Model. Optim. Mobile, Ad Hoc, Wireless Netw.*, Seoul, South Korea, 2009, pp. 1–10.

[7] K. Pelechrinis, C. Koufogiannakis, and S. V. Krishnamurthy, "On the efficacy of frequency hopping in coping with jamming attacks in 802.11 networks," *IEEE Trans. Wireless Commun.*, vol. 9, no. 10, pp. 3258–3271, Oct. 2010.

[8] J. Proakis, *Digital Communications*, 3rd ed. New York, NY, USA: McGraw-Hill, 1995.

[9] J. T. Chiang and Y.-C. Hu, "JIM-Beam: Jamming-resilient wireless flooding based on spatial randomness," in *Proc. IEEE Mil. Commun. Conf.*, 2013, pp. 464–469.

[10] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 4, pp. 586–602, Oct.–Dec. 2017.

[11] J. Harshan and Y.-C. Hu, "Cognitive radio from hell: Flipping attack on direct-sequence spread spectrum," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Barcelona, Spain, Apr. 2018, pp. 1–6.

[12] Z. K. M. Ho and E. A. Jorswieck, "Instantaneous relaying: Optimal strategies and interference neutralization," *IEEE Trans. Signal Process.*, vol. 60, no. 12, pp. 6655–6668, Dec. 2012.

[13] Q. Wang, Y. Dong, J. Zhao, N. Li, J. Qian, and B. Liu, "Instantaneous relaying: Feasibility conditions for interference neutralization," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1370–1373, Aug. 2015.

[14] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2119–2123, Sep. 2004.

[15] M. Duarte and A. Sabharwal, "Full-duplex wireless communications using off-the-shelf radios: Feasibility and first results," in *Proc. 44th Asilomar Conf. Signals, Syst. Comput.*, Pacific Grove, CA, USA, 2010, pp. 1558–1562.

[16] J. I. Choi, M. Jain, K. Srinivasan, P. Levis, and S. Katti, "Achieving single channel, full duplex wireless communication," in *Proc. 16th Annu. Int. Conf. Mobile Comput. Netw.*, 2010, pp. 1–12.

[17] M. Jain *et al.*, "Practical, real-time, full duplex wireless," in *Proc. 17th ACM Annu. Int. Conf. Mobile Comput. Netw.*, 2011, pp. 301–312.

[18] J. Zhou *et al.*, "Integrated full duplex radios," *IEEE Commun. Mag.*, vol. 55, no. 4, pp. 142–151, Apr. 2017.

[19] M. S. Amjad, H. Nawaz, K. Ozsoy, O. Gurbuz, and I. Tekin, "A low-complexity full-duplex radio implementation with a single antenna," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2206–2218, Mar. 2018.

[20] M. Amjad, F. Akhtar, M. H. Rehmani, M. Reisslein, and T. Umer, "Full-duplex communication in cognitive radio networks: A survey," *IEEE Commun. Surv. Tut.*, vol. 19, no. 4, pp. 2158–2191, Oct.–Dec. 2017.

[21] D. Bharadia and S. Katti, "FastForward: Fast and constructive full duplex relays," *ACM SIGCOMM Comput. Commun.*, vol. 44, no. 4, pp. 199–210, 2014.

[22] F. Ahsan and M. Uppal, "Stalkers: A physical-layer solution towards co-existence with WiFi," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Barcelona, Spain, Apr. 2018, pp. 1–6.

[23] K. B. Rasmussen and S. Capkun, "Realization of RF distance bounding," in *Proc. USENIX Secur. Symp.*, 2010, pp. 389–401.

[24] S. Fang, Y. Liu, and P. Ning, "Wireless communications under broadband reactive jamming attacks," *IEEE Trans. Depend. Secure Comput.*, vol. 13, no. 3, pp. 394–408, Jun. 2016.

[25] M. Wilhelm *et al.*, "Short paper: Reactive jamming in wireless networks: How realistic is the threat?" in *Proc. 4th ACM Conf. Wireless Netw. Secur.*, 2011, pp. 47–52.

[26] A. Proano and L. Lazos, "Packet-hiding methods for preventing selective jamming attacks," *IEEE Trans. Depend. Secure Comput.*, vol. 9, no. 1, pp. 101–114, Feb. 2012.

[27] M. Spuhler, D. Giustiniano, V. Lenders, M. Wilhelm, and J. B. Schmitt, "Detection of reactive jamming in DSSS-based wireless communications," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1593–1603, Mar. 2014.

[28] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, "MIMO-based jamming resilient communication in wireless networks," in *Proc. IEEE Conf. Comput. Commun.*, Toronto, ON, Canada, 2014, pp. 2697–2706.

[29] X. Ma, G. B. Giannakis, and B. Lu, "Block differential encoding for rapidly fading channels," *IEEE Trans. Commun.*, vol. 52, no. 3, pp. 416–425, Mar. 2004.

[30] M. K. Tsatsanis and G. B. Giannakis, "Equalization of rapidly fading channels: Self-recovering methods," *IEEE Trans. Commun.*, vol. 44, no. 5, pp. 619–630, May 1996.

[31] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, Feb. 2014.

[32] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ, USA: Wiley, 2006.