PHY-Layer Resiliency in OFDM Communications: A Tutorial

Chowdhury Shahriar, *Student Member, IEEE*, Matt La Pan, *Student Member, IEEE*, Marc Lichtman, *Student Member, IEEE*, T. Charles Clancy, *Senior Member, IEEE*, Robert McGwier, *Senior Member, IEEE*, Ravi Tandon, *Member, IEEE*, Shabnam Sodagari, *Senior Member, IEEE*, and Jeffrey H. Reed, *Fellow, IEEE*

***Abstract*—This tutorial paper addresses the physical layer security concerns and resiliency of Orthogonal Frequency Division Multiplexing (OFDM) communications; the de facto air-interface of most modern wireless broadband standards including 3GPP Long Term Evolution (LTE) and WiMAX. The paper starts with a brief introduction to the OFDM waveform and then reviews the robustness of the existing OFDM waveform in the presence of noise, multipath fading, and interference. The paper then moves on to build comprehensive adversarial models against OFDM waveforms. Robustness of OFDM is first investigated under AWGN noise and noise-like jamming attack scenarios, then under uncorrelated yet colored interferences from modulated sources (both intentional and unintentional). Finally, the paper explores some of the more recent developments in the field of energy efficient correlated jamming attacks that can disrupt communication severely by exploiting the knowledge of the target waveform structure. Potential countermeasures against such jamming attacks are presented, in an attempt to make a robust and resilient OFDM waveform.**

***Index Terms*—Jamming, anti-jamming, security, robustness, OFDM, MIMO, LTE, WiMAX, TV white space.**

I. Introduction

MODERN wireless broadband communication systems require extremely high throughput using a limited bandwidth, to accommodate the ever increasing mobile data demand. Orthogonal Frequency Division Multiplexing (OFDM) modulation technique and associated Orthogonal Frequency Division Multiple Access (OFDMA) channel access mechanism have become a major element in modern wireless broadband communication systems. This is due to OFDM's spectral efficiency, achievable data rates, and robustness in multipath fading environments. Wireless Local Area Network (WLAN) technologies based on the IEEE 802.11a, 802.11g, 802.11n, 802.11ac, and 802.11ad standards all use OFDM. It is also used in Wireless Metropolitan Area Network (WMAN) technologies based on the IEEE 802.16d, 802.16e, and 802.16m standards. In addition, Long Term Evolution (LTE), the leading cellular broadband technology, relies on OFDM for its air-interface.

Manuscript received November 8, 2013; revised May 12, 2014; accepted July 7, 2014. Date of publication August 20, 2014; date of current version March 13, 2015.

The authors are with the Bradley Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg, VA 24061 USA.

Digital Object Identifier 10.1109/COMST.2014.2349883

In recent years, the Federal Communications Commission (FCC) has freed up the 700 MHz band (running from 698–806 MHz) as a result of the *Digital Television* transition and made it available for both commercial wireless and public safety communications [1]. The FCC has allocated portions of the 700 MHz band (24 MHz bandwidth) to establish a nationwide, interoperable wireless broadband communications network that will benefit state and local public safety users. FCC then auctioned licenses to use the remaining 700 MHz band for commercial mobile broadband services for smartphones, and other mobile devices. An important element of the 700 MHz public safety spectrum is the establishment of a framework for a 700 MHz public safety/private partnership between the licensee for one of the commercial spectrum blocks and the licensee for the public safety broadband spectrum [2]. Presence of multiple networks will require careful planning and may often become subject of interference from each other. On top of that, both dedicated public safety spectrum and public safety/private partnership shared commercial spectrum blocks may become targets of malicious adversaries, making it even more important to look into the security issues of OFDM.

While OFDM is often celebrated for its robust performance in noise, fading channel and uncorrelated interference, it has been shown that the current implementations of OFDM are susceptible to a variety of signal jamming attacks [3]–[7]. In fact, the United States military prohibits the use of Wireless MAN in such hostile environments [8], prompting development of specific transmission security extensions to the standard [9] for such scenarios.

In this tutorial paper we have explored the resiliency of OFDM under various adversaries that a OFDM-based communication system may encounter. We began with barrage (or broadband or wideband) jamming attack on OFDM, where the adversary attempts to jam entire band of OFDM waveform with noise-like signal. Barrage jamming is the simplest and most intuitive of all the conventional jamming attacks and is also the optimum one when *a priori* knowledge about the target is unavailable [10]. Therefore, barrage jamming is used as the baseline for all the analysis presented in this paper.

Immediately after introducing barrage jamming, we move on to explore next conventional jamming attacks category called partial-band jamming. In partial-band jamming attack, adversaries attempt flood part of a wideband systems with noise-like signals. Next we look into unintentional interferences that an OFDM system may encounter from other communication

systems that are operating in the same or adjacent bands. Then, we move onto explore the resiliency of OFDM systems under sophisticated correlated jamming attacks. In these kind of jamming attacks, adversaries exploits the knowledge about the OFDM waveform to tailor jamming waveform. They are not only power efficient, but also capable of causing complete disruption of communications. Here we explore synchronization attacks, equalization attacks and control channel attacks against OFDM systems.

One of the most important prerequisites for communicating using OFDM is synchronization between the transmitter and the receiver. Both timing and frequency synchronization are necessary to avoid intersymbol interference (ISI), as well as intercarrier interference (ICI) and loss of orthogonality among OFDM subcarriers. This synchronization is usually performed using predetermined training symbols transmitted each frame [11]–[13]. These symbols are a potentially critical target for OFDM jamming. We will discuss a number of potential threats and security concerns for OFDM synchronization.

In OFDM, the channel impulse response is estimated and equalized using known symbols, called pilot tones [14]. Various efficient jamming attacks which target these pilot tones of OFDM systems have been derived in [3]. These attacks seek to manipulate information used by the equalization algorithm, to cause errors to a significant number of symbols. The two attacks detailed are pilot jamming, where attack values are independent and identically distributed (i.i.d.), and pilot nulling, where pilot values are assumed to be known and inverted to cause destructive interference. While this is one aspect of OFDM which must be improved, it is not the only area of weakness to a sophisticated adversarial attack.

At last, we investigate control channel attacks on OFDM-based systems. When targeting a specific communications protocol, an efficient jamming attack can be realized by interfering with one subsystem of that protocol. This subsystem can take the form of a physical channel or physical signal; several of which are present in OFDM-based protocols. As long as the subsystem is vital to the operation of the link, and the jamming signal is received at a high enough jammer-to-signal ratio (J/S), denial of service (DOS) is inflicted. Example physical layer subsystems include Hybrid Automatic Repeat Request (HARQ) acknowledgments, random access requests, and control channels. By targeting a subsystem that is sparse in both time and frequency (with respect to the entire downlink or uplink signal), an adversary can achieve a low duty cycle, low bandwidth, and low power jamming attack.

We have also briefly discussed about the threats and security issues of Single Carrier Frequency Division Multiple Access (SC-FDMA), which is an important variant of OFDM. SC-FDMA can be viewed as DFT-spread OFDMA [15]. SC-FDMA has been adopted as the air-interference for the uplink of the LTE and LTE-A systems.

The remainder of this paper is organized as follows. Section II establishes motivation of the paper. Section III discusses brief literature review. Section IV details the OFDM system including synchronization, channel estimation, and equalization. Section V categorizes adversarial models against OFDM systems. Section VI describes robustness of the OFDM waveform. Section VII details noise jamming attacks. Section VIII discusses communication disruption from intentional and unintentional interferences. Section IX introduces the synchronization jamming attack and possible mitigation strategies. Section X introduces the equalization jamming attack and possible countermeasures. Section XI proposes control channel attacks and possible mitigation strategies. Section XII concludes.

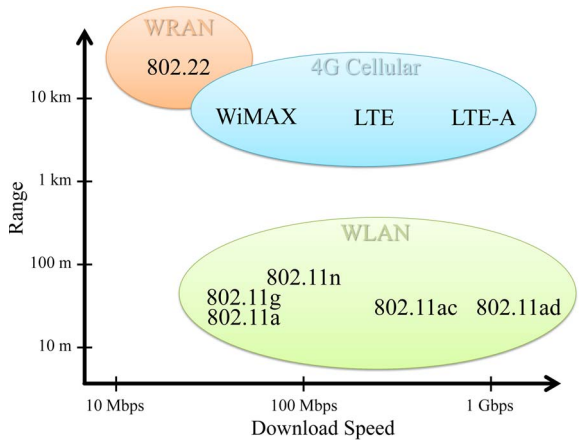

Fig. 1. OFDM-based wireless broadband technologies, mapped according to typical range and data rate.

II. Motivation

The OFDM modulation and associated OFDMA multiple access technique have become the primary technologies used by the latest wireless broadband standards; both fixed and mobile. Fixed wireless broadband over a short distance is provided by Wi-Fi, which uses OFDM in versions IEEE 802.11a, 802.11g, 802.11n, and 802.11ac. For fixed wireless broadband over long distance, the IEEE 802.22 standard describes an OFDM-based Wireless Regional Area Network (WRAN) which utilizes white spaces in the TV frequency bands. In terms of cellular technologies, the most recent generation of mobile broadband standards include LTE, LTE-Advanced and WiMAX. Fig. 1 illustrates OFDM-based technologies used to provide wireless broadband over a variety of distances.

LTE is well on its way to becoming the primary commercial standard for mobile wireless broadband. LTE is gaining popularity all over the world because of its high speed communications at a rapidly reducing cost. The LTE standard is extensive, and is in a state of continuing improvement by the Third Generation Partnership Project (3GPP). Releases 10 and higher of LTE correspond to the LTE-Advanced technology, which includes additional capabilities such as coordinated multipoint transmission and reception (CoMP), carrier aggregation, self-organizing networks (SON), and more advanced multiple-input and multiple-output (MIMO) schemes.

In addition to commercial use, LTE is the chosen technology for the United States' nationwide public safety network known as FirstNet, which is currently under development. The FirstNet network will consist of dedicated LTE infrastructure in the 700 MHz band. In locations where dedicated infrastructure does not yet exist or is congested, FirstNet devices will fall

back on commercial LTE networks. The use of LTE in FirstNet is an example of how LTE will play a role in mission-critical communications, which is why we should consider the security and information assurance aspects of LTE. The OFDM attacks discussed in Sections IX–XI can all be applied to the LTE downlink and/or uplink signals.

III. Literature Review

In this paper we are investigating the resiliency of OFDM communication systems; therefore, it is an integral part of this research to explore various adversaries that OFDM systems may encounter. The coverage is not all-inclusive; however, most of the common approaches are discussed here.

As mentioned earlier, barrage jamming is the simplest of all jamming attacks. A number of papers is available where research is conducted on OFDM system under barrage jamming attack [3], [16]–[18]. A noteworthy mention would be [16], where Lou *et al.* derived the bit error rate (BER) of OFDM under barrage jamming attack. A jamming game on OFDM setting is explored by Renna *et al.* in [17]. Another major class of noise jamming attack on OFDM is the partial-band jamming, in which part of a wideband system is jammed intentionally [16], [18]–[23]. In [18], [22]–[28] the impact of noise jamming on OFDM-based broadband standards (e.g., Wi-Fi and WiMAX) are explored.

There has been considerable research on OFDM synchronization in the past twenty years. Classical synchronization methods are presented in [11]–[13]. In addition, there are a plethora of other methods—some of them specialized, slightly modified, or system specific—examples of which are presented in [29]–[33]. Previous research encompasses both symbol timing acquisition as well as carrier frequency offset estimation due to the fact that they can be performed jointly or separately.

While there has been research conducted on robustness of OFDM synchronization algorithms [29]–[39], the majority of this work has been conducted under the assumption of uncorrelated or narrowband interference. Some of these works also include interference detection and mitigation strategies. Recently, specific adversarial signals were introduced [4], [5] which are highly correlated and designed with the intent of disrupting the OFDM system during the synchronization stage. In this paper, we focus on jamming attacks that prevent a receiver employing OFDM from ever acquiring the proper symbol timing estimate. This work is based on the symbol timing and carrier frequency offset estimation algorithm designed by Schmidl and Cox [11], which is the maximum likelihood detector for OFDM, and because of its optimality it is widely used in commercial systems based on OFDM, the WiMAX standard being the most recognizable instance.

In OFDM, the channel impulse response is estimated and equalized using known symbols, called pilot tones [14], [40], [41]. Clancy *et al.* [42] discussed possibility of jamming the channel estimation procedure as an efficient type of attack. It is suggested that targeting the channel sounding or accuracy of channel state information (CSI) estimation not only requires less power, but also more efficient than barrage jamming. Following [42], jamming of channel estimation and equalization are studied for SISO-OFDM communications [3], [6] and MIMO-OFDM channels [43], [44]. The impact of jamming pilots tones and disrupting equalization process of OFDM systems can also be found in [27], [45]–[48].

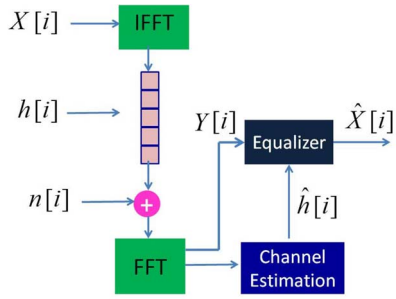

Fig. 2. System diagram for an OFDM transmitter and receiver subject to a multipath channel.

Literature related to control channel jamming attacks on modern wireless broadband technologies is limited. The authors of [7] investigate the extent to which LTE is vulnerable to intentional jamming, by analyzing the components of the LTE downlink and uplink signals. This includes the jamming vulnerability of each control channel in LTE. A survey of the security of LTE availability is given in [49]. The authors of [50] analyze PHY and MAC layer vulnerabilities in WiMAX. While all of these papers focus on the specific PHY and MAC layer channels within each technology, they indirectly analyze the types of attacks described in Section XI of this paper (e.g. the random access channel attack and the resource allocation attack).

IV. OFDM Systems

The block diagram of the overall OFDM transceiver and channel model used in this paper is shown in Fig. 2. Symbol X_i is estimated by $\hat{X}_i$ by measuring received symbol Y_i and channel estimate $\hat{H}_i$. Specifically,

$$Y_i = H_i X_i + n_i \tag{1}$$

where H_i is the channel frequency response and n_i is i.i.d. AWGN with distribution $\mathcal{N}(0, \sigma_n^2)$ [3].

A. Transceiver

In an OFDM system, many narrowband signals are multiplexed in the frequency-domain (FD), converted to the time-domain (TD) and finally transmitted. At the appropriate sampling time, the corresponding discrete-time OFDM symbol at the transmitter can be expressed as

$$x_i[n] = \text{IFFT}\{X_i[k]\} = \sum_{k=0}^{N-1} X_i[k] e^{j\frac{2\pi kn}{N}} \quad n \leq N-1 \tag{2}$$

where $0 \leq k$ (kth subcarrier) and N is the number of subcarriers.

At the receiver, time-domain received signals are fed to the FFT block to be converted back to the FD for equalization and demodulation, and can be expressed as

$$Y_i[k] = \text{FFT}\{y_i[n]\} = \sum_{n=0}^{N-1} y_i[n] e^{-j\frac{2\pi kn}{N}}. \tag{3}$$

B. Synchronization

There are a number of classic OFDM synchronization algorithms [11]–[13], [29]–[33]. In general, these algorithms rely on the correlation between a training symbol and some copy of itself to perform timing acquisition and carrier frequency offset estimation. The similarity of these algorithms means that most of the security concerns and potential jamming attacks reviewed in this work are applicable to each of these algorithms, as is described later in this work. However, for the sake of brevity, the topics covered in this paper are described and outlined mathematically in reference to [11] for reasons previously described in Section I.

The synchronization method proposed in [11] has three main stages—symbol timing estimation, fine carrier frequency offset estimation and correction, and coarse carrier frequency offset estimation. This algorithm is based on the use of specific *preamble* symbols, transmitted at the beginning of every frame. Due to the nature of this synchronization algorithm, the preamble symbols have a very specific structure.

It is important to note the structure of these symbols and the reasoning behind the structuring. The first symbol is constructed from a pseudo-random (PN) sequence of in-phase/quadtrature (IQ) symbols in the frequency domain which is half the length of the number of subcarriers used. To mitigate interference with other users, as well as to avoid distortion from frequency down conversion, a guard band of empty subcarriers is used on both the upper and lower frequency edges of each OFDM symbol.

This symbol can be constructed by either populating every other subcarrier in the frequency domain before taking the IFFT to create the time domain OFDM symbol, or by taking a half-length IFFT of the PN sequence then repeating the symbol twice in time. Once the time domain symbol is created, the cyclic prefix is appended in the time domain.

The second preamble symbol is constructed from a PN sequence the length of all of the subcarriers. Each of the subcarriers is populated in the frequency domain, so that there is no repetition of the symbol in the time domain. The IFFT of the PN sequence is taken and the cyclic prefix is generated in the time domain, as in the previous symbol. The first and second symbol are essentially glued together in time and transmitted as one preamble.

Timing recovery is performed using only the first symbol, but frequency recovery employs the differential PN sequence of the subcarriers that the first and second symbols both use. This sequence is just the division of the PN sequence on the corresponding frequencies from half of the second symbol (even or odd), and the PN sequence from the first symbol. It therefore has the length of half of the number of subcarriers used, and is the rotation on each of the IQ symbols from the first PN sequence to the second. The structure of the preamble and this last PN sequence make up the knowledge that the receiver has about the preamble symbol. This will allow the receiver to both detect the preamble symbol and determine the timing and frequency offset between with the transmitter.

The first step in the synchronization process is the estimation of symbol timing, performed on the complex baseband samples of the RF down converted signal. A sliding window of L samples is used to search from the preamble, where L is equal to the length of half of the first preamble symbol excluding the cyclic prefix. Two terms are computed for timing estimation. The first according to

$$P(d) = \sum_{m=0}^{L-1} \left(r_{d+m}^{*} r_{d+m+L} \right) \tag{4}$$

and the second according to

$$R(d) = \sum_{m=0}^{L-1} |r_{d+m+L}|^2 \tag{5}$$

where d is the time index which corresponds to the first sample taken in the window and r is the length-L vector of received symbols. These two terms are used to compute the timing metric $M(d)$ according to

$$M(d) = \frac{|P(d)|^2}{R(d)^2} \tag{6}$$

whose maximum value determines the symbol timing. Once this is performed, the receiver will need to correct for the carrier frequency error between the transmitter and the receiver.

Carrier frequency offset estimation is the final step of the synchronization process. There are actually two sub-stages within frequency correction. The first is fine frequency correction and the second is coarse frequency correction. The fine frequency correction Δf is estimated using

$$\Delta f = \text{angle}\left(P(d)\right) / \pi T \tag{7}$$

where T is the period of a single preamble symbol without its cyclic prefix and d is taken from anywhere along the timing metric plateau.

This term provides the fractional frequency offset only. The symbols can then be multiplied by a complex exponential to correct for the fine frequency error. In the frequency domain this represents the subcarriers being properly aligned in to bins.

The coarse frequency error estimation is the final step in the synchronization process, and finally employs the use of the second preamble symbol and the differentially modulated PN sequence. First, FFTs—the length of the symbol period without the cyclic prefix—of each of the symbols are taken. A coarse frequency metric is then computed to determine the number of bins that the symbols are shifted in either direction.

$$B(g) = \frac{\left| \sum_{k \in \mathcal{X}} x_{1,k+2g}^{*} v_k x_{2,k+2g}^{*} \right|^2}{2\left(\sum_{k \in X} |x_{2,k}|^2 \right)^2}. \tag{8}$$

For this equation, the set $\mathcal{X}$ represents all of the subcarrier bins which are occupied by both preamble symbols (either even or odd). The term g spans the range of the possible frequency offsets (there must be some bounds on the frequency errors between the transmitter and receiver). The point $g_{\max}$ at which

the function $B(\cdot)$ is maximized represents the coarse frequency offset. The overall frequency offset is

$$\hat{\Delta f} = \text{angle}\left(P(d)\right)/\pi T + 2g_{\max}/T. \tag{9}$$

Once the overall frequency offset between the transmitter and the receiver has been determined, the signal acquisition process is complete and symbols can be demodulated.

C. Channel Estimation and Equalization

In OFDM, equal power and equally spaced pilot tones are inserted in the signal to estimate and equalize the channel's frequency response at the receiver for optimum performance [51]. If $\{k_1, k_2, \ldots, k_n\}$ are the locations of the pilot tones, then the channel's frequency response at the pilot tone location [6]

$$\hat{H}_{k_i} = \frac{Y_{k_i}}{p_i} = \frac{H_{k_i}p_i + n_{k_i}}{p_i} = H_{k_i} + \frac{n_{k_i}}{p_i}. \tag{10}$$

If the pilot tones p_i are unit energy, then channel frequency response error at the pilot tones are the additive noises. The receiver interpolates between these pilot tones to estimate the intermediate values of the channel frequency response [52]. For linear interpolation, where $k_j < i < k_{j+1}$, the estimated channel frequency response

$$\hat{H}_i = \frac{\hat{H}_{k_j}(k_{j+1} - i) + \hat{H}_{k_{j+1}}(i - k_j)}{k_{j+1} - k_j} \tag{11}$$

where $\hat{H}_i$ is the least squares (LS) estimate of the channel H_i.

Equalization of channel effect is performed after estimating the channel frequency response $\hat{H}_i$ by

$$\hat{X}_i = \frac{Y_i}{\hat{H}_i} = \frac{X_i H_i}{H_i + \epsilon_i} + \frac{n_i}{H_i + \epsilon_i}$$

where ϵ_i is the overall error of channel estimation. When jamming signal is present, the equalized signal becomes

$$\hat{X}_i = \frac{X_i H_i}{H_i + \epsilon_i} + \frac{J_i G_i}{H_i + \epsilon_i} + \frac{n_i}{H_i + \epsilon_i}. \tag{12}$$

Note that one can model the overall channel estimation error ϵ_i in terms of interpolation error ϵ_i^n due to additive noise at pilot tones, and approximation error ϵ_i^a due to approximating channel's frequency response function using finite numbers of pilot tones. Fig. 3 shows both of these errors graphically.

1) Channel Noise Error: Additive noise at pilot tones propagates during linear interpolation. The error during interpolation due to noise can be expressed as [3]

$$\epsilon_i^n = \frac{1}{k_{j+1} - k_j}\left(\frac{n_{k_j}}{p_j}(k_{j+1} - i) + \frac{n_{k_{j+1}}}{p_{j+1}}(i - k_j)\right). \tag{13}$$

If the pilot tones are unit-power, then this additive noise error has following distribution

$$\epsilon_i^n \sim \mathcal{N}\left(0, \left(\frac{k_j^2 + k_{j+1}^2 + 2i\,(i - k_j - k_{j+1})}{(k_{j+1} - k_j)^2}\right)\sigma_n^2\right). \tag{14}$$

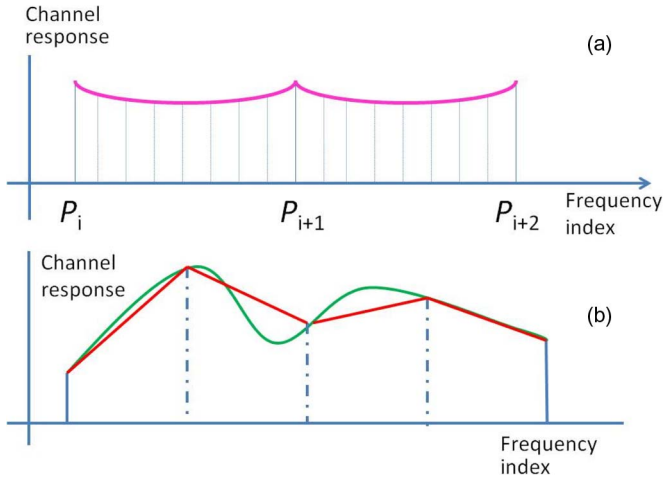

Fig. 3. Overall channel estimation error is the result of two sources of errors: (a) channel noise error—error that emerges due to noise at pilot tones that propagates during interpolation, and (b) channel approximation error—error that is created due to using finite number of points to approximate a function (in this case, the wireless channel).

2) Channel Approximation Error: Use of finite points to approximate a function causes error. If linear interpolation is used to approximate two known values at other points, then the point-wise error is bounded as [53], [54]

$$|\epsilon_i^a(x_1, x_0)| \leq \left[\frac{1}{8}\max_{x_0 \leq x \leq x_1}|h''(x)|\right](x_1 - x_0)^2. \tag{15}$$

For equidistance pilots, space $d = (x_{i+1} - x_i)$ is deterministic with mean equal to d and approximation error $\epsilon_i^a \cong Kd^2$, where $K = (1/8)\max_{x_0 \leq x \leq x_1}|h''(x)| = constant$ for $x_0 \leq x \leq x_1$. This expression for the approximation error is important as it relates the distance between two adjacent pilots with approximation error, and therefore can be used during waveform design.

V. Adversarial Model

In this section we discuss the intention, capabilities and goal of hostile interferences (also known as jamming). Fig. 4 shows the system diagram of an OFDM transmitter-receiver pair (target), which is subject to jamming by the adversary.

It is assumed that the individual subcarrier channels are each a flat-faded Rayleigh fading channel where individual OFDM subcarriers have a channel bandwidth less than the coherence bandwidth of the channel. Let x_i be the transmitted signal and y_i be the received signal. Then, in the presence of a jammer $j_i[n]$, a narrowband flat-fading system can be modeled as

$$y_i[n] = h_i[n] * x_i[n] + g_i[n] * j_i[n] + w_i[n], \tag{16}$$

where h_i and g_i are channel impulse response of transmitted signal and jammer's signal respectively, and w_i is independent and identically distributed (i.i.d.) additive white Gaussian noise (AWGN) with distribution $\mathcal{N}(0, \sigma_n^2)$.

Typically jammers seeks to disrupt communications, and have a variety of strategies that they are capable of. Some

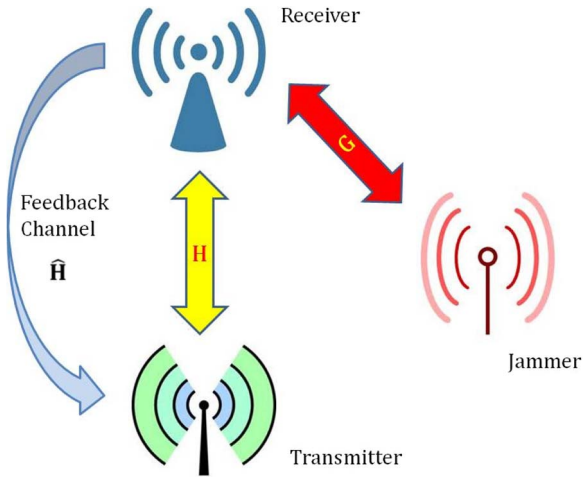

Fig. 4. System diagram for an OFDM transmitter-receiver pair subject to jamming attack; where H is the channel between transmitter and receiver and G is the channel between target receiver and jammer.

techniques are more effective and efficient than others, and a successful strategy depends on the particular type of target employed. We classify the attacks into one of the following categories: i.i.d. noise, colored interference, and jamming that is correlated with the target signal. Unintentional interferences from other communicating nodes often degrade communication as well, which is also a subject in this discussion. We also discuss protocol-aware jamming, which uses prior knowledge of the protocol in use to increase effectiveness. This can be thought of as a subset of correlated jamming. This coverage of jamming strategies is not all-inclusive; however, most of the common approaches are discussed here.

A. Noise Jamming

The first category is noise jamming. Noise jamming attacks are the simplest of all the jamming attacks that one can envision. In noise jamming, the jamming carrier signal is modulated with a random noise waveform with the intent to disrupt the communication waveform by injecting noise into the receiver. The noise is generally assumed to be Gaussian. Broadband noise (BBN) jamming, partial-band noise (PBN) jamming (including single-tone and multi-tone noise), and chirp (a.k.a. sweep) jamming are within this category [55]. BBN jamming simply jams the entire OFDM waveform by placing i.i.d. Gaussian noise energy across the entire frequency spectrum used by the target signal(s). It is also called full band jamming and sometimes called barrage jamming. Throughout this paper the noise threat from BBN is treated as the basis of comparison for the sake of analysis. Unlike BBN jamming, PBN jamming could apply to a non-agile jammer where the jamming signals occupy a portion of the target's entire signal. Details of the noise jamming are discussed in Section VII.

B. Interference Jamming

Interference attacks are ones that are structured (colored), but not synchronized to target signal. This category encompasses anything that is not purely constant. As interference jamming attacks are not dependent on the target signal, they are therefore much easier to execute because one does not need to observe and obtain any level of synchronization with the target signal. For example, the adversary may intentionally start its own communication in the band where the target is operating. Such transmission can interfere with the target and therefore, degrade/disrupt the targets ability to communicate. One can observe similar interference from unintentional interference from co-channel and/or adjacent channel communications. For example, baby monitors at 700 MHz or the TV channel 51 next to 700 MHz may cause unintentional colored interference to OFDM-based waveforms in 700 MHz band [2]. Details of interference jamming are discussed in Section VIII.

C. Correlated Jamming

Correlated jamming attacks are very serious and capable of causing damage to OFDM transmissions using minimal power. These attacks are typically very sophisticated and can involve detailed synchronization and knowledge of the target signal, to increase effectiveness. A simple example of correlated jamming involves only transmitting a jamming signal when there is energy on the channel. Commercial waveforms are designed with specific structures such as reference signals to perform symbol timing estimation, pilot tones to estimate and equalize channel effects, and control channels to embedded various control information. Such waveforms are susceptible to the threat of correlated jamming. Recently, pilot tone based OFDM jamming was introduced [3], where the jammer seeks to jam pilot tones to jeopardize equalization. OFDM synchronization jamming attacks are introduced in [4], [5], where the adversary either jams the acquisition signal or misguides the target receiver to synchronize into erroneous time and frequency. Different kinds of correlated jamming attacks are discussed in detail in Sections IX–XI.

A subset of correlated jamming is known as *Protocol-Aware Jamming* [56], in which the jammer has prior knowledge of the protocol used by the target(s), and exploits this knowledge to increase jamming effectiveness. For example, if a jammer knows the target signal is a Wi-Fi signal, then it could transmit periodic pulses with a period equal to the IEEE 802.11 Extended Interframe Space (EIFS). This strategy has been shown to lead to an effective jamming attack using an extremely low duty cycle [57]. The concept of protocol-aware jamming can be applied to most of the jamming techniques discussed throughout this paper.

We have showed a high-level classification of various jamming attacks in Table I. Note that Barrage jamming is also a kind of noise jamming attack. Since it is the simplest one and considered as the base of all jamming in absence of any knowledge about the signal, we have included it as independent one. The table shows various jamming attacks and the complexity of generating each types of jamming and their effectiveness. The complexity of generating each types of jamming and their effectiveness will be discussed in details in coming sections.

TABLE I
HIGH-LEVEL CLASSIFICATION OF JAMMING ATTACKS

Attack	Complexity	Effectiveness
Barrage Jamming	Very Low	Low
Noise Jamming	Low	Low
Interference	Low	Low
Correlated Jamming		
– Synchronization Attack	High	High
– Equalization Attack	High	High
– Control Channel Attack	High	High

VI. ROBUSTNESS OF OFDM

One of the key strengths of OFDM is its ability to handle multipath propagation. It is capable of combating multipath fading with greater robustness and less complexity. ISI caused by multipath propagation is less of a problem with OFDM because low data rates are carried by each carrier. Since low symbol rate modulation schemes (i.e., where the symbols are relatively long compared to the channel time characteristics) suffer less from ISI, it is advantageous to transmit a large number of low-rate streams in parallel instead of a single high-rate stream. Since the duration of each symbol is long, it is feasible to insert a guard interval (GI) between the symbols. Using a cyclic prefix (CP) greater than the coherence bandwidth during the GI ensures eliminating most ISI. However, it comes at the price of spectral efficiency [40], [41].

OFDM system, due to avoidance of ISI, can easily adapt to severe channel conditions without the need for complex channel equalization algorithms being employed [40], [41]. For example, frequency-selective fading caused by multipath propagation can be considered as constant (flat) over an OFDM sub-channel if the sub-channel is sufficiently narrow-banded. This makes frequency domain equalization possible at the receiver, which is simpler than the time domain equalization used in conventional single-carrier modulation.

OFDM waveforms are also resilient when combating narrowband co-channel interference (CCI). As an OFDM waveform is composed of many narrowband tones, a narrowband interferer can degrade only a limited portion of the signal, leaving the rest of the subcarriers intact. In addition, wireless broadband standards such as LTE include adaptive rate modulation, which allows subcarriers under poor conditions to fall back to a lower order modulation scheme, such as QPSK [58].

Unfortunately, the typical OFDM system has a smaller subcarrier spacing, which can be vulnerable to *Doppler* shift observed in high mobility situations. *Doppler* shift can cause significant ICI. Luckily, ICI mitigation strategies can compensate to a certain extent. Another notable drawback of OFDM is its sensitivity to timing and frequency synchronization; a mismatch at the receiver can cause serious ICI and ISI [58].

VII. NOISE JAMMING ATTACKS

In this section we briefly discuss conventional noise jamming attacks on OFDM, such as barrage jamming, partial band jamming, single-tone jamming and multi-tone jamming.

A. Barrage Jamming

Barrage jamming (a.k.a. broadband noise jamming) is the simplest kind of jamming attack in which the jammer jams the entire bandwidth occupied by the subcarriers of an OFDM signal. It has been shown game theoretically and information theoretically to be the optimal jamming strategy in the absence of any knowledge of the target signal [10].

Barrage jamming involves transmitting AWGN in an effort to increase the noise floor; thus degrading the target's received Signal-to-Noise Ratio (SNR). As a result, σ_n^2, and consequently both noise n_i and noise error ϵ_i^n increases significantly, degrading the SNR. Barrage jamming is typically used as the baseline when evaluating other kinds of jamming attacks.

B. Partial Band Jamming

In partial-band noise (PBN) jamming, a certain fraction of the occupied bandwidth is jammed with additive Gaussian noise. If the jamming power is constant, then the performance of the PBN depends on the fraction between jamming bandwidth and signal bandwidth. The jammer-to-signal power ratio (JSR) given by (P_{PBN}/P_{Sig}) and the jammer-to-signal bandwidth fraction ratio (JFR), $\rho = W_{PBN}/W_{Sig} \leq 1$, are important values when considering PBN jamming. P_{PBN} is the jamming power, P_{Sig} is the target signal power, W_{PBN} is the jamming signal bandwidth, and W_{Sig} is the target signal bandwidth [16]. The PSD of the PBN is [16]

$$PSD_{PBN} = \frac{P_{Sig}}{\rho} = \frac{P_{PBN}}{W_{Sig}}.\frac{W_{Sig}}{W_{PBN}} = \frac{P_{PBN}}{W_{PBN}}. \quad (17)$$

In PBN, the target signal has two frequency bands - i) a jammed band and ii) an unjammed band. If the average PSD of PBN is N_{PBN}, then the effective PSD of PBN in the jammed bands becomes (N_{PBN}/ρ). Taking this in consideration, we can get the BER for QPSK modulated OFDM system under PBN as [16], [40]

$$P_b(\rho) = \rho.\mathbf{Q}\left(\sqrt{\frac{2E_b}{N_0 + \frac{N_{PBN}}{\rho}}}\right) + (1-\rho).\mathbf{Q}\left(\sqrt{\frac{2E_b}{N_0}}\right). \quad (18)$$

1) Single-Tone Jamming: Single-tone jamming (STJ) is a special kind of partial-band jamming where a single high powered tone is transmitted to jam the system of interest. This tone can be of any form and shape. However, the most common ones are impulse, rectangular and AWGN shape.

For OFDM, a single-tone jammer is considered to be the one that jams a single subcarrier. The time-domain single-tone jamming signal for OFDM subcarrier is

$$J(t) = A_J \cos(2\pi f_J t) = \sqrt{2J}\cos(2\pi f_J t), \quad (19)$$

where A_J is the amplitude of jamming tone, J is the power of the tone, and f_J is the jamming center frequency [16]. STJ is often used to corrupt the target's automatic-gain-control mechanism; indirectly jamming the rest of the subcarriers.

2) Multi-Tone Jamming: Multi-tone jamming (MTJ) is a special kind of partial-band jamming, where multiple equal powered tones in certain frequencies are transmitted to jam the system of interest. As the jammer is power limited, the number of tones is inversely proportional to the power of individual tones. Let J_T be the total jamming power and N_T be the number of tones present in the multi-tone jammer, then the multi-tone jamming power distribution in frequency domain can be expressed as

$$J(k) = \begin{cases} A_k = \frac{J_T}{N_T} & f_L \leq k \leq f_H \\ 0 & \text{otherwise} \end{cases} \quad (20)$$

where A_k represents the amplitude of the k-th frequency bin (or subcarrier in the case of OFDM) and frequency index, $k = \{f_L, f_{L+1}, \ldots f_{H-1}, f_H\}$ [16], [59].

For OFDM, a multi-tone jammer is considered to be the one that jams multiple subcarriers. Every jamming tone can be modeled as

$$J(t) = A_J \sum_{k=1}^{N_T} \cos(2\pi f_k t) = \sqrt{\frac{2J_T}{N_T}} \sum_{k=1}^{N_T} \cos(2\pi f_k t), \quad (21)$$

where A_J is the amplitude of jamming tone, J is the power of the tone, and f_k is the jamming center frequency of k-th subcarrier [59]. MTJ might be used to conserve power while still causing denial of service. Apart from the aforementioned ones, we can find other type of noise jamming attacks such as pulsed and sweeping jamming attack [28].

VIII. Interference Jamming Attacks

Interference attacks are ones that may be structured but are not dependent on the target signal. Alternatively, interference attacks can defined as colored noise where adversaries can have modulated signals that have zero correlation with the target signal, i.e., center frequency of target. Interference can be intentional or unintentional. Intentional interference jamming is much easier to execute because one does not need to observe and obtain any level of synchronization with the target signal. For example, the adversary may intentionally start its own communication in the band where the target is operating. Such transmission can interfere with the target and therefore, degrade/disrupt the targets ability to communicate. In this section we investigate the impact of colored interferences on OFDM systems. While most of the examples provided here involve unintentional interference, we should not forget that adversaries can intentionally use similarly structured signals to cause disruption; especially when they are used against public safety or other mission critical situations.

One source of interference on LTE is TV broadcasting. In [60], [61] the authors discussed the potential interferences between TV white space and DSA-enabled cellular communications. Channel 51 TV broadcasting spectrum, which is next to the lower 700 MHz that 3GPP put into their specification, has received some attention recently [62]. In [62], the authors discuss the interference levels (-40 dBm to -20 dBm) that can impact LTE performance. Based on both lab and field test results, it is found that Channel 51 and E Block signals interfere with Band 12 networks using the B and C blocks and Band 17 devices, and can cause significant degradation of throughput (usually measured in block error rate) in large geographic areas, including urban areas. In addition, E-Block transmissions cause two form of interferences: (1) adjacent channel interference, and (2) reverse intermodulation interference to consumer devices (i.e., LTE-compatible devices) seeking to receive a 5 MHz signal on the C Block or a 10 MHz signal on the B and C Blocks of lower 700 MHz.

There are other cases like this in the records for the Advanced Wireless Services (AWS) band. The FCC plans to reallocate mobile wireless services to 600 MHz spectrum that is currently used for over-the-air broadcast TV services [63], [64]. The impact of 600 MHz TV station interference on the new bands for LTE in the soon-to-be auctioned 600 MHz band is discussed in [63]. A central feature of the FCCs proposed framework is an unusually large duplex gap between the downlink and uplink frequencies combined with the placement of TV stations in that duplex gap. Placing very high power TV stations in the duplex gap would create adjacent channel interference in the 600 MHz devices downlink bands, which could also degrade the receiver performance. Second, the FCCs proposed framework would result in harmonic signals that could interfere with PCS and BRS/EBS mobile downlink spectrum. Third, the FCCs design for uplink spectrum would likely result in co-channel interference caused by TV stations operating in nearby geographic areas.

Another potential category of interference for OFDM could be the various kinds of radars operating nearby. In [65], the authors consider a scenario where low-frequency radars such as Synthetic Aperture Radar (SAR) interferes with the Digital Terrestrial Television (DTT) standard such as DBV-T that employs an OFDM-based waveform. The low-frequency radar operating at VHS (currently) and UHF (in near future) may cause outages to 20% of DVB-T users operating in the 585–806 MHz band (primarily in Europe). The authors concluded with observations that interference from radar can be reduced by flattening the radar spectrum or by increasing FFT size of the channel (which increases the OFDM symbol period). Other notable scenarios where radar interferes with LTE would be weather radar and airport surveillance radar. Both of these radars operate at 2.7–2.9 GHz band which is a proposed band for LTE. The major disturbing trend here is the inequality between radar powers with communication nodes.

Apart from these interferences, OFDM based standards such as LTE may face interference from Tactical Targeting Network Technology (TTNT) proposed by the Defense Advance Research Project Agency (DARPA). The TTNT proposal consists of researching new waveforms for use in air-to-air networks of high-speed aircraft at 1755–1850 MHz which is currently used by commercial cellular users [66]. Even though the Department of Defense (DoD) is planning to relocate TTNT from 1755–1850 MHz to 1755–1850 to 2025–2110 MHz band in ten years, it will remain a clear and present danger for LTE systems operating at nearby bands until then.

IX. Synchronization Jamming Attacks

While the synchronization process described in [11] can be considered robust within *friendly* communications environments, there are many weaknesses to the algorithm were it to be intentionally and intelligently attacked. These jamming strategies allow adversaries to be efficient relative to simple channel whitening. Even based on the importance of timing and frequency recovery alone, a more efficient attack than channel whitening presents itself as whitening only during preamble transmission. Some of the potential weaknesses lie both within the timing recovery and the frequency recovery. It is interesting to note that, while OFDM is much more sensitive to errors in the estimation of carrier frequency offset than symbol timing, there are still various ways in which synchronization could be disrupted by creating error in either value, or possibly both.

It is important to note, however, that the algorithm in [11] can not be utilized in LTE because the primary synchronization signal (PSS) and the secondary synchronization signal (SSS) lack the required structure. While this algorithm cannot be used in LTE systems, most LTE synchronization algorithms are mathematically similar, though slightly less optimal in a maximum likelihood sense. Specifically, most of these algorithms rely on a locally stored reference signal that is used to cross-correlate with the PSS. The algorithm from [11] was chosen because it operates like cross-correlation techniques, but it uses an auto-correlation with a repeating preamble to account for channel response, therefore performing synchronization in a truly maximum likelihood (ML) fashion. While there is no defined synchronization algorithm in the LTE standards, it is still important to mathematically analyze the performance of OFDM synchronization in the presence of adversarial communications. Subsequently, we use this algorithm as a point of reference to show that there are significant security gaps in even the most optimal OFDM synchronization algorithm. Most of the attacks in this paper are directly applicable threats to cross-correlation based algorithms as shown in [67].

A. False Preamble Timing Attack

The main opportunities to efficiently disrupt symbol timing estimation lie within either moving the peak of the timing metric, or destroying it altogether [4]. The first method is to create a new timing metric peak. Based on the knowledge that the jammer has about the preamble, this can either be a retransmission of the preamble, a different preamble symbol altogether or the transmission of the correct preamble at the incorrect time. If the false timing preamble is transmitted at a higher power, then the peak of the overall timing metric will be taken at the wrong place, and can destroy the symbol timing estimation. An example of this attack is shown in Fig. 5, where the false preamble signal is transmitted at a higher power than the true preamble, resulting in timing maximum metric being moved to a false location.

In this case, the attack signal can either be a copy of the preamble sent by the transmitter, or, more generally, can be a preamble symbol constructed with any PN sequence. The only requirement is that the jamming signal be of the preamble form. For the case where the jamming signal is a delayed copy of the preamble and the preamble and jamming symbols do not overlap in time, the timing metric will be dictated by

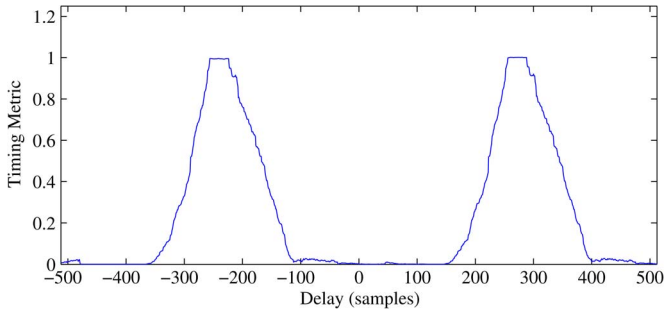

Fig. 5. This plot shows the timing metric over a three symbol window as computed at the receiver. Due to the transmission of the false preamble attack at equal power as the true training symbol, the receiver computes two plateaus and the estimate becomes ambiguous and prone to error.

$$P(d) = R_{y^{(d)}y^{(d)}}(-L) + \alpha^2 R_{y^{(d-N)}y^{(d-N)}}(N). \tag{22}$$

In this case, the timing metric will consist of two plateaus. One will be located at the correct timing peak in terms of the transmitter, and the other will lie at the peak established by the jammer. An example of this is shown in Fig. 5. The dominant peak will be determined by the α term, which corresponds to the SJR in a given scenario.

B. Preamble Nulling Attack

Another method for degrading symbol timing would be to destroy the timing peak altogether. This attack would be carried out by a technique called preamble nulling [4]. This attack would be predicated on the fact that the jammer have perfect knowledge of the preamble as viewed by the receiver. By inverting the preamble symbol in time and transmitting the jamming signal at the correct time, a jammer would effectively be able to destructively interfere with the preamble at the receiver, effectively wiping out the timing metric peak. However, this method is also dependent on the relationship between the channel that the transmitter sees and the channel that the jammer sees. If these channels are the same or similar enough, or if both are known to the jammer, then this attack can be effective.

The analytical impact of this jammer can also be derived using the relationship

$$j(i) = -\alpha \left((k^{-1} * h) * x \right)_i \tag{23}$$

where $\alpha > 0$. Substituting this relationship in to the timing metric equations yields

$$P(d) = \sum_{m=0}^{L-1} (1 - 2\alpha + \alpha^2)(h * x)^*_{d+m}(h * x)_{d+m+L}. \tag{24}$$

The drawback with this attack is that to be effective, it requires that the preamble symbol detected at the receiver be near the noise floor. This means that for a given transmit SNR, the term α must be close to 1 such that the effective SNR of the preamble symbol seen at the receiver is around -30 dB. An illustration of the distortion of the timing metric at -30 dB SNR can be seen in Fig. 6. The proximity of alpha to 1 will

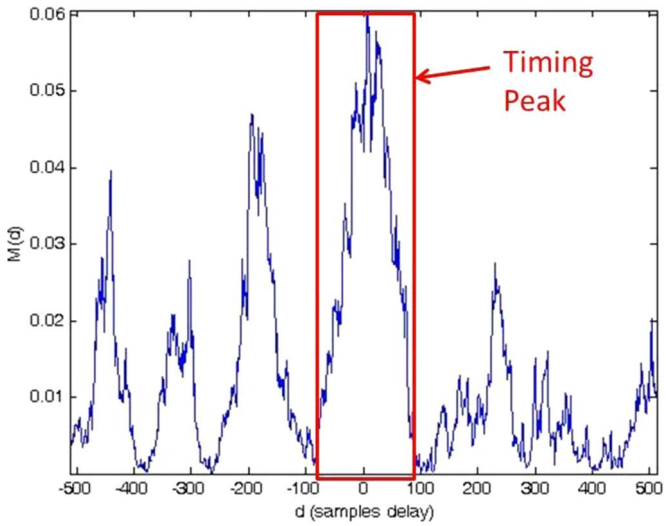

Fig. 6. OFDM timing metric as a result of the preamble nulling attack which has degraded the preamble SNR to −30 dB. The blue portion is the computed timing metric. The red box shows where the true plateau should be, but the other peaks outside of the boundary are due to the noise floor.

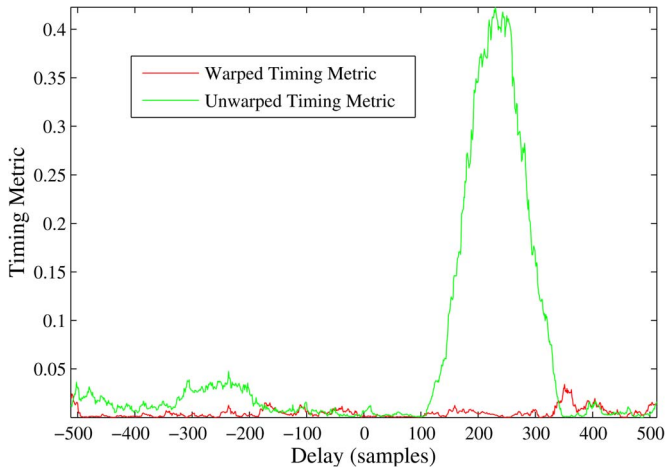

Fig. 7. This plot shows the impact of the preamble warping attack on the symbol timing estimate. The estimate in green is the pure timing metric computation with no attack present; the red shows the metric after the attack is imposed. The preamble warping attack makes the first training symbol resemble any other OFDM symbol by populating all of the available subcarriers as opposed to half.

be therefore determined by the original SNR for the preamble at the receiver. This requirement can be a determining factor of whether or not this attack will be effective.

C. Preamble Warping

Since the timing acquisition relies heavily on the correlation of the two halves of the first preamble symbol, another effective strategy for jamming is to destroy this correlation [4]. This timing attack can be achieved by attacking the frequency domain structure of the preamble. As previously stated, the first preamble symbol can be created either with a half length IFFT and repeating it in the time domain, or by taking a full length IFFT in the frequency domain where every other subcarrier is populated with a PN sequence. These methods are mathematically equivalent, so either one will result in a frequency domain representation where every other FFT bin is empty before the addition of the cyclic prefix. The idea behind the preamble warping attack is to transmit on the unused subcarriers of the preamble symbol to destroy time domain correlation.

Preamble warping essentially transforms the first symbol of the preamble in to a generic preamble symbol, albeit that the PN sequence is still present over one half-set of the subcarriers. By populating the unused subcarriers during timing acquisition, the attack aims to destroy timing correlation, causing the receiver to miss the timing point.

In the warping attack case, the introduction of symbols on to the unused subcarriers creates a new OFDM symbol. Under the same assumptions of channel knowledge, the receiver will now be calculating the timing point according to

$$P(d) = \sum_{m=0}^{L-1} (h * \hat{x})^*_{d+m} (h * \hat{x})_{d+m+L} \tag{25}$$

where $\hat{x} = x + j$ and $\hat{x}$ does not possess the same correlation properties as the intended preamble symbol. This means that the timing metric does not simplify to the autocorrelation function of the OFDM symbol at the zero offset, but rather the autocorrelation function evaluated at L. The following

$$P(d) = R_{\hat{x}^{(d)}\hat{x}^{(d)}}(L) \tag{26}$$

indicates that the timing metric peak will be greatly diminished, as it will correspond to the significantly small offset autocorrelation values of an OFDM symbol as described in [68].

The diminished correlation values of the first preamble symbol do not guarantee destruction of timing acquisition. Due to the fact thatthere is still a small correlation in the offset autocorrelation bins, it would not be expected that this attack would completely destroy timing acquisition. What it does do is diminish the effectiveness of the timing estimator by a significant amount. An example of this can be seen in Fig. 7. Preamble warping accomplishes this with half the power—3 dB savings—of false preamble jamming. This attack would also be particularly effective in low SNR environments where the correlation of the warped preamble is on the order of its noise floor. In addition, this attack could be used in conjunction with a low power false preamble attack to spoof a receiver, causing it to lock on with the jammer.

D. Preamble Phase Warping

OFDM systems begin to suffer noticeable degradations in SNR for frequency offsets that are as little as 1% of the subcarrier spacing [41]. Based on the work done in [34], the degradation in SNR in dB at the receiver based on carrier frequency offset can be expressed as

$$D \approx \frac{10}{3ln(10)} \left(\pi \frac{\Delta F}{F}\right)^2 \frac{E_s}{N_o}. \tag{27}$$

The term ΔF is defined as the frequency offset at the receiver, and the term F signifies the subcarrier or bin spacing in the OFDM symbols. The degradation is proportional to the SNR $= E_s/N_o$ at the receiver. This approximation assumes

that the frequency offset is small relative to the bin spacing. Using the marginal values for E_s/N_o for each of these modulations, it is clear that even slight errors in the fine frequency offset can have a significant impact on the effective SNR of an OFDM symbol at the receiver. This aspect of OFDM illustrates one of the glaring weaknesses of the synchronization process and highlights a definite susceptibility to adversarial signals.

The first of the frequency based synchronization jamming attacks is preamble phase warping [5], which aims to disrupt the frequency offset estimate of the receiver by sending a frequency shifted preamble symbol to the receiver. While it is important to note that this type of attack could be used to change the overall frequency error estimate, another important use of the attack would be to degrade the fine frequency estimate. By altering the fine frequency offset, this jamming attack can prevent the receiver from properly lining up the subcarriers in to frequency bins at the receiver. This results in massive ICI and subsequent degradation of SNR.

This attack can be modeled stochastically based on a random frequency offset over a given range.[1] The frequency offset for any given system within the specified range can be modeled as a continuos random variable with a uniform distribution over the given frequency range. While there may be another distribution which models this offset more closely, a uniform distribution is a sufficient approximation for the purposes of this paper. For the model that we used, both the receiver frequency offset and the phase warp offset are chosen from uniform distributions according to

$$X, Y \sim U(f_{Lo}, f_{Hi}). \tag{28}$$

As previously stated, frequency estimation for OFDM is extremely sensitive, so much so that errors on the order of 1% of a subcarrier spacing can cause significant degradation to the effective SNR at the receiver. In an ideal jamming scenario where the attacker has knowledge of the exact preamble symbol, channel state information and frequency offset estimates, this attack effectively randomizes the frequency estimation within the range of possible offsets.[2]

Assuming that both the receiver frequency offset and warped frequency are approximately equal to their ideally modeled random values, the frequency estimation error converges to

$$e_{RMS} = \sqrt{E[Y^2]} \tag{29}$$

as the sample size becomes sufficiently large. Noting that $E[Y]^2 = 0$ it follows that

$$e_{RMS} = \sqrt{VAR[Y]} = \sigma \tag{30}$$

where σ^2 is the variance of the random variables.

These results indicate that we would expect to see the RMS error for the frequency offset estimate approach the standard deviation of a uniform random variable with a support equal to the possible range of frequency offsets. In short, the ideal phase warping attack basically transforms the receiver frequency offset estimate in to a random variable over the range of possible offsets. This effect will have a dramatic impact on the OFDM synchronization process, the details of which are discussed later in this paper.

[1]The frequency offset error for an OFDM system would have to be constrained within a specific range to not interfere with adjacent channels.

[2]The range of possible frequency offsets is something that would be constrained by the signal standard.

E. Differential Scrambling Attack

The other frequency estimation attack reviewed here is the differential scrambling attack [5]. This attack is designed to disrupt the coarse frequency error estimation at the receiver. The coarse frequency error is simply a subcarrier misalignment at the receiver due to clock frequency discrepancies. The synchronization algorithm uses the phase error in the two halves of the first symbol to determine the fractional portion of the frequency discrepancy, and relies on the differential sequence of the common subcarriers of the first and second preamble symbol to determine the integer valued subcarrier offset. This sequence is determined according to $c_{1,k}$ and $c_{2,k}$ are the PN sequences on the common subcarriers of the first and second preamble symbols. The differential scrambling attack targets this differential sequence and prevents subcarrier alignment by altering the sequence $c_{2,k}$ according to

$$w_k = \sqrt{2}\frac{c_{2,k}}{c_{1,k} + c_{ds,k}}. \tag{31}$$

The attack is carried out by transmitting a constant stream of symbols across the subcarriers used in the first preamble symbol. This attack is similar in structure to the false preamble timing attack proposed in [4]. The idea behind this attack is to distort the amplitude and phase of the received subcarriers in the first preamble symbol, in turn altering the differential sequence at the receiver. The symbols transmitted by the attacker on each subcarrier are constant based on the assumption that the PN sequence of the first preamble symbol is unknown. Assuming the sequence is random and its symbol values are uniformly distributed, transmitting a constant sequence has the same probability of altering the phase at each subcarrier as transmitting a random symbol. Differing this sequence will degrade the performance of the coarse frequency estimation and can result in subcarrier misalignment at the receiver.

F. Simulation

We developed synchronization simulations to test the performance of current synchronization algorithms in the face of symbol timing and frequency attacks. It was assumed that the jammer had knowledge of the exact preamble symbol in the case of the nulling attack, but only knowledge of the structure in the case of the false preamble attack. In the case of the nulling attack, the simulations were performed over a range of effective SNR values seen at the receiver. The false preamble timing attack results were looked at over a range of SJR's in a channel environment with an SNR of 10 dB to isolate the effects of the jamming signal on the symbol timing estimate. The error rate at each value was computed based on an average of 1000 simulations (Figs. 8–11).

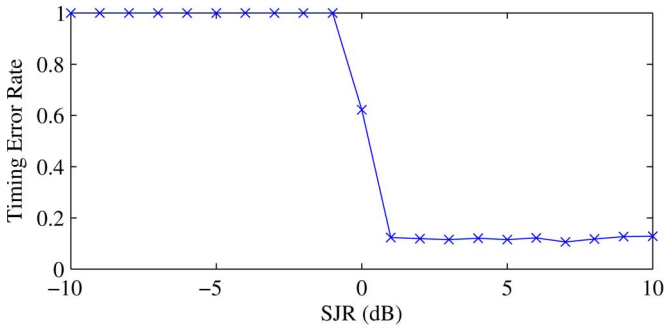

Fig. 8. This plot shows the error rate for the symbol timing estimator as a function of the SJR of the preamble and false preamble attack. The error rate is determined by any estimate taken that falls outside of the symbol timing range. The plot shows that when the signal power for the false preamble is higher than the true preamble, the receiver will lock on to a timing point from the false plateau.

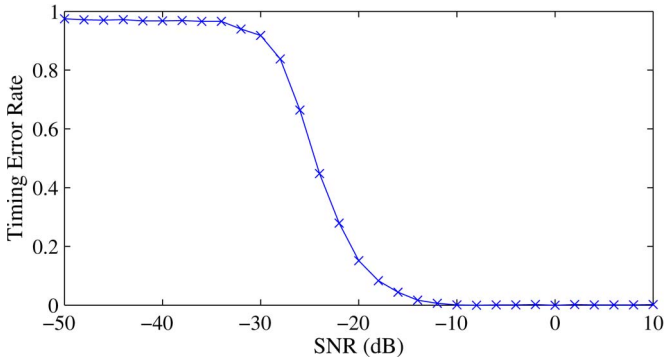

Fig. 9. Symbol timing estimation performance as a function of the SNR at the receiver. The plot shows that the estimator starts to be impacted by noise around −10 dB and is completely lost in the noise floor around −32 dB. This plot also shows how much the preamble nulling attack must degrade the SNR at the receiver to be effective. The level of precision of the attack is determined by the original SNR.

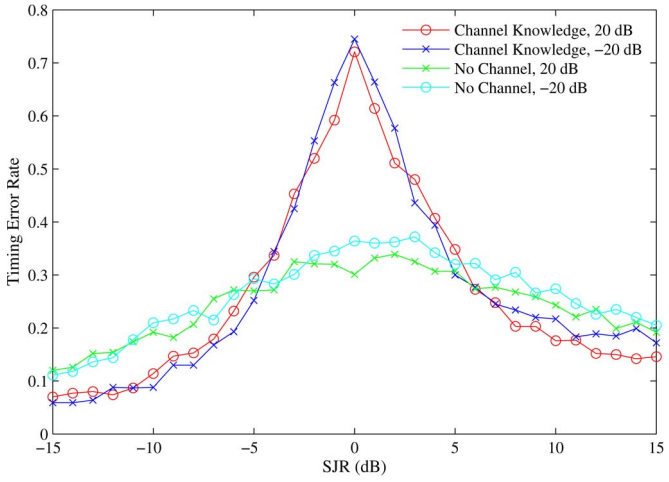

Fig. 10. Symbol timing error rate caused by the preamble warping attack as a function of the SJR at the receiver. The plot shows that this attack is most effective when it has equal power as the preamble at the receiver and channel knowledge. In addition, if the attack is sent at a much higher power than the original preamble, it actually can improve synchronization performance because it becomes a high powered preamble.

G. Attack Comparison

The various attacks presented in this paper have varying degrees of cognition, channel knowledge and complexity, and

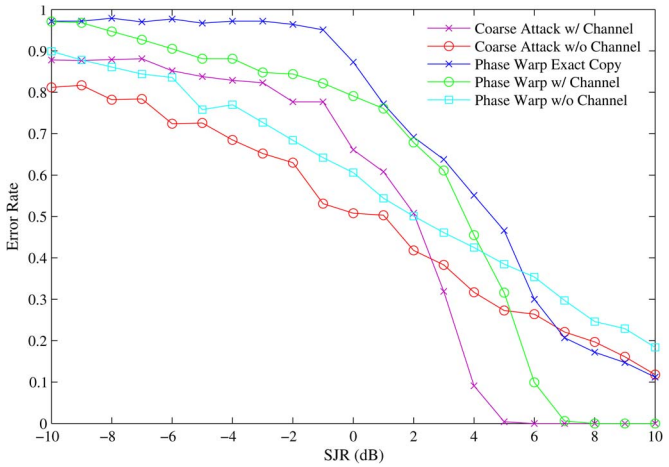

Fig. 11. Frequency offset estimation error of the phase warping and differential scrambling attacks as a function of SJR. The error rates show how effective the attacks are with different levels of cognition about the channel and the training symbols.

therefore varying situational applications. The preamble nulling attack is the most complex of these attacks, requiring exact preamble knowledge, channel estimation and extremely accurate signal generation. On the other hand, the false preamble attack only requires standards knowledge that dictates the structure of the preamble waveform. While this attack is efficient and very effective, it also adds the threat of preamble spoofing, causing the receiver to synchronize with the jammer. The preamble warping attack also demonstrates a significant threat to OFDM synchronization, as it efficiently and significantly reduces preamble timing correlation. This attack could be particularly effective if used in conjunction with other attacks. The preamble phase warping attack can be relatively effective at varying degrees of waveform and channel knowledge, and it is the frequency analog of the false preamble timing attack. The differential scrambling attack requires no channel knowledge, though it is required to be accurate in estimating and scrambling the proper subcarrier frequencies. The effectiveness of each of these jammers is directly tied in to their level of cognition and estimation capabilities.

H. Extension to Cross-Correlation Based Algorithms

As mentioned in Section I, cross-correlation based algorithms similar to [12], [13], [29]–[33] are the most widely implemented in LTE systems. This is because the primary synchronization signal (PSS) and secondary synchronization signal (SSS) lack the required structure to perform synchronization via [11]. However, this does not preclude these algorithms from being vulnerable to the attacks presented here.

An example is a cross-correlation algorithm searching for the timing synchronization point using a reference copy of the training symbols used in the PSS. Any attacker with knowledge of the training symbols used by the system–which are defined in the standard–could perform a false preamble attack to to perform either denial of service or spoofing on a user device. Similarly, all of the attacks reviewed in this work readily extend to cross-correlation based algorithms, except for the preamble warping attack, which relies on the frequency domain

representation of the repeated preamble symbol. But if the same attack were carried out by a jammer that simply inserted tones at the midpoint frequencies of a PSS, then the orthogonality of the tones at the receiver would be destroyed, which massively degrades the effective SNR seen at the receiver, consequently having a similar effect.

The motif of these situations is that existing, correlation based synchronization algorithms are sensitive to correlated interference and therefore must be protected. There are a multitude of methods by which synchronization—the critical and prerequisite process of OFDM systems—can be attacked and ultimately altogether prevented, a portion of which are reviewed in this work. Preventing these types of attacks are critical for developing robust and resilient OFDM systems.

I. SC-FDMA Synchronization Security

SC-FDMA is an important variant of OFDM used for the uplink of LTE and LTE-A [69]. Although the details of SC-FDMA synchronization are outside of the scope of this paper, the process is very similar to OFDM synchronization. The LTE standard, though, leaves control of the timing synchronization of user equipment (UE) with the EnodeB. The carrier frequency offset estimation is performed using a preamble selected by the EnodeB. For this reason, only the syncrhonized attacks reviewed in this paper threaten uplink synchronization in LTE. It is still crucial for uplink demodulation that the EnodeB be able to correctly estimate frequency offset between itself and the receiver, so the attacks discussed here capable of degrading the received SNR of the preamble symbols are significant security concerns for LTE uplink synchronization.

J. Attack Mitigation

The deficiencies of existing OFDM signal acquisition algorithms against adversarial signals leaves plenty of room for future research and improvement. Various alternative synchronization methods have been explored, although there has not been an abundance of research focused on jamming scenarios in particular. There are many possible ways in which the process could be improved. One of these would be to have the transmitter and receiver agree on a specific preamble, or a set of preambles, beforehand to limit attacks against jammers that only have knowledge of the structure of the preamble symbols as opposed to the symbols themselves. Perhaps a more important starting point for improving the robustness of OFDM synchronization would be disguising the preamble. The structure of the preamble is so distinct that it would be obvious to any somewhat intelligent jammer when the transmitter and receiver are trying to synchronize. Even just making the preamble a little bit harder to identify than it is in its current form would be an improvement in robustness.

The preamble structure is based on the need to perform a type of correlation processing between the first and second half of the first symbol to get a timing estimate. Although this process has high processing gain and is effective in mitigating channel effects, it is not the only way to perform timing recovery or frequency recovery for that matter. There are other forms of correlation processing which would not require such an obvious preamble structure to perform signal acquisition. An example of a possible alternative would be to use the Cross Ambiguity Function (CAF) to perform the timing and frequency recovery for OFDM. This form of correlation processing basically computes a timing estimate and a frequency error term the same as the method posed by Schmidl and Cox. But this processing would not require any particular structure to the preamble–other than that it be a valid OFDM symbol. Instead, this method would require that the preamble be known to both the transmitter and the receiver. This is not very different from the current method, in that the receiver must have some prior knowledge about the preamble symbols. This method could greatly increase the degree of difficulty for any potential jammer without explicit knowledge of the preamble symbol being used.

Other strategies to prevent jamming of OFDM synchronization are likely to be found in higher network layers. Disguising the preamble, as well as its location in time and frequency are possible ways to mitigate these types of jamming attacks. Decision based synchronization might also be implemented within the control layers to improve the likelihood of successful acquisition. These methods are advantageous because they do not require the overhaul of the synchronization process in many existing standards.

X. Equalization Jamming Attacks

A. Pilot Jamming Attacks

In pilot jamming, the adversary transmits AWGN signals only on the pilot tone's, in an attempt to raise the pilot tone's noise floor and thus disrupt the equalization process. It can be shown that pilot tone jamming is more power efficient than barrage jamming. Assume an attack where the jammer is synchronized with the target signal through observation of communications between parties in the network. The jammer transmits the signal vector Z_i where $Z_i = 0$ for non-pilot tones, and $Z_i = q_i$ for pilot tones, where q_i is i.i.d. AWGN with distribution $\mathcal{N}(0, \sigma_j^2)$.

Note that for all pilot-based attacks, we assume attack energy is evenly distributed between all pilot subcarriers, for the same reasons that it was determined optimal for pilot energy to be evenly distributed between all pilot subcarriers [51].

The impact is that the error term ϵ_i^J under jamming is dominated by the jammer power, and becomes the linear combination of the jammed energy. For i.i.d. jamming (assuming it has same variance as AWGN), the mean distribution is

$$\epsilon_i^J \sim \mathcal{N}\left(0, \frac{2}{3}\sigma_n^2\right). \tag{32}$$

If the same AWGN sequence is coherently transmitted on all pilots simultaneously, then the noise is not averaged out for linear combinations, and therefore, the noise error distribution that now depends on both jamming and AWGN becomes (assuming unit jamming channel response)

$$\epsilon_i^J \sim \mathcal{N}\left(0, \sigma_n^2\right). \tag{33}$$

Thus it is beneficial to coherently jam pilot tones.

B. Pilot Nulling Attacks

Pilot nulling has more severe consequence on the equalizer than pilot jamming. In this attack, we seek to null the pilot tones. The goal is for $\hat{H}_i$ to be asymptotically close to zero, such that when $\hat{X}_i$ is computed as $\hat{X}_i = (Y_i/\hat{H}_i$, we cause a division by zero that makes $\hat{X}_i$ arbitrarily large.

The underlying assumption here is such that an adversary can estimate the channel between the transmitter and target receiver $\hat{H}_{k_i}$, and his own channel to the target $\hat{G}_{k_i}$. The jammer transmits a signal J, that is defined as

$$J_{k_i} = \left(\frac{\hat{H}_{k_i}}{\hat{G}_{k_i}}\right) e^{j\pi} p_i \tag{34}$$

which is the channel-corrected, π-radian phase shift of the pilot tone.

The received pilot tone signal under nulling attack is then

$$Y_{k_i}^N = H_{k_i} p_i + G_{k_i} \left(\frac{\hat{H}_{k_i}}{\hat{G}_{k_i}}\right) e^{j\pi} p_i + n_{k_i}. \tag{35}$$

If the channel estimates at the jammer are accurate, then we are left with noise only, means this term converges to n_{k_i}. Let this estimate residue term δ_i be defined as

$$\delta_i = H_{k_i} + G_{k_i} \left(\frac{\hat{H}_{k_i}}{\hat{G}_{k_i}}\right) e^{j\pi}. \tag{36}$$

Thus $Y_{k_i}^N = \delta_i p_i + n_{k_i}$ and

$$\hat{H}_{k_i}^N = \delta_i + \frac{n_{k_i}}{p_i}. \tag{37}$$

Let $\overline{\delta}_i$ be the linearly-combined error for non-pilot tones, where $\overline{\delta}_i$ is also Gaussian with distribution $\mathcal{N}(0, \sigma_{\overline{\delta}}^2)$. Hence, the overall channel noise error due to AWGN and residue will be Gaussian as well

$$\epsilon_i^N \sim \mathcal{N}\left(0, \sigma_n^2\right) \tag{38}$$

where $\sigma_n^2 = \sigma_{\overline{\delta}}^2 + 2/3\sigma_n^2$ is combined error variance. While pilot nulling can certainly be effective, it should be noted that obtaining accurate channel information is an extremely difficult task which adds much complexity to the jammer.

C. MIMO-OFDM Channel Sounding Attacks

Recently, another technology advanced hand in hand with OFDM, known as Multiple Input Multiple Output (MIMO). Two major limitations in wireless channels are multipath interference, and the data throughput limitations as a result of Shannon's Law [70]. MIMO employs multiple antennas on the receiver and transmitter to utilize the multipath fading effects to significantly improve the data throughput available on a given channel with its defined bandwidth. Using spatial multiplexing, MIMO technology enables the system to set up multiple data streams on the same subcarriers/symbols, thereby increasing the data capacity of a channel [70], [71].

In many modern broadband standards, MIMO and OFDM are often implemented jointly to achieve high throughput performance [15], [72]–[74]. The MIMO schemes employed in LTE vary slightly between the uplink and downlink to keep the terminal cost low. For the downlink, a configuration of minimum two transmit antennas at the base station and minimum two receive antennas on the mobile terminal are used as baseline. For the uplink from the mobile device to the base station, Multi-User MIMO (MU-MIMO) is recommended [15], [74]. Using this, even though the base station requires multiple antennas, the mobiles only have one transmit antenna and this considerably reduces the cost of the mobile.

Most MIMO systems require a method to estimate and equalize the channel, whether through channel reciprocity or sounding [70]. Like SISO-OFDM, most OFDM-based MIMO waveforms use sounding via OFDM pilot tones. Therefore, a sophisticated jammer can utilize this knowledge to attack the channel sounding symbols of MIMO-OFDM system. Targeting the channel sounding or accuracy of channel state information (CSI) estimation that requires less power while being more efficient than barrage jamming is first introduced in [75], where different types of attacks on the channel sounding process in MIMO channels in low and high SNR regimes and their effects on constellation manipulation have been addressed. Miller *et al.* [76] showed that such attack can be applied to Alamouti space time codes, which are used as a basis of many protocol standards, such as 802.11n [76]. Clancy *et al.* [42] discussed possibility of jamming the channel estimation procedure as an efficient type of attack. Following [42], jamming of channel estimation and equalization were studied for SISO communications [3] and MIMO channels [43], [77]. In [43], [44] jamming of channel sounding symbols for MIMO-OFDM scenario is investigated specifically.

In addition, like SISO pilot nulling [3], *MIMO Singularity Attack* is introduced in [43], which attempts to reduce the rank of the channel gain matrix estimate by the receiver through transmission of specific jamming signals. More specifically, in *MIMO Singularity Attack*, a multi-antenna jammer tries to manipulate pilot tones to skew the channel state information obtained at the receiver. In a way, MIMO-OFDM channel sounding jamming attacks and channel sounding singularity attacks are similar to the pilot jamming attacks and the pilot nulling attacks and have similar effect on the performance. Like pilot nulling attacks, singularity jamming can be more destructive than data jamming attacks such as barrage or pilot jamming. Synchronization missmatch issues related to MIMO channel sounding attack are discussed in [44].

D. Cyclic Prefix Jamming Attacks

In OFDM, a cyclic prefix (CP) is almost always used, which refers to the prefixing of a symbol with a repetition of the end [40], [41]. It is known that frequency-domain equalization (FDE) depends on the CP to take advantage of the DFT operations in frequency domain. The convolution-multiplication property of the DFT states that circular convolution of two signals in time is equivalent to multiplication of two signals in frequency. Circular convolution requires the input sequence

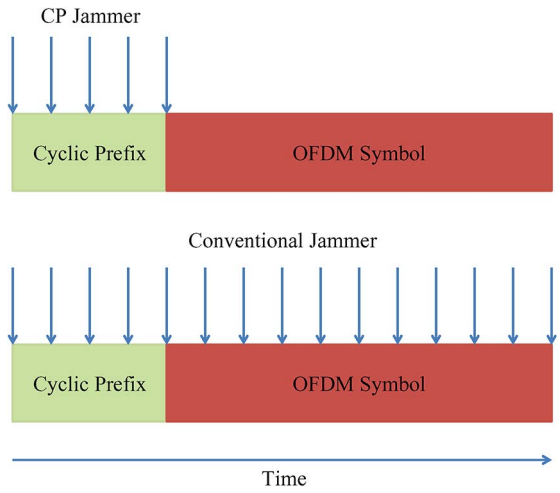

Fig. 12. OFDM signal under jamming attack—jamming only the cyclic prefix (CP) of the OFDM signal (Left) versus jamming on all the subcarriers of the OFDM signal (Right).

to be periodic. In practice, OFDM symbols are made to look like periodic sequences by adding the CP. Therefore, at the receiver, a simple linear equalization can be used to recover the transmitted data symbols. Moreover, the CP serves as a guard interval, which eliminates the interference from the previous symbol and allows for simple frequency-domain processing, which is used for channel estimation [40], [41], [78], [79].

In CP jamming attacks, a low duty cycle jammer selectively targets the CP of the signal. The rationale for CP jamming attack is simple- instead of wasting power to jam the entire signal all the time, jam an important portion of the transmission. If CPs can be degraded, the FDE algorithms simply will not work. In addition, destruction of the CP would result in additional ISI. Moreover, as the CP is used for correcting the symbol-time delay and the carrier frequency offset of the signal by correlating the repeated parts of a symbol, injecting a more concentrated jamming signal in just the CP will knock off the correlation, therefore disrupting the received signal [80]. Fig. 12 shows a CP jamming (left) versus noise jamming model (right) in a typical OFDM symbol.

E. SC-FDMA Equalization Security

Like OFDM/OFDMA, SC-FDMA not only performs channel estimation and equalization in frequency domain, but also uses pilot-symbol assisted (PSA) channel estimation techniques [15]. Therefore, SC-FDMA, in similar way, is prone to the equalization attacks presented in this paper. The impact of pilot jamming on SC-FDMA and a comparative study with OFDM under pilot jamming attack is discussed in [69]. As SC-FDMA is proposed to be used in uplink of LTE (meaning low-power user handsets will be using it), it will require lot less power to jam the equalizer of practical system.

F. Attack Comparison

Barrage jamming and pilot tone jamming achieve similar results, but pilot tone jamming requires significantly less power, since only pilot tones need to be jammed, and the channel noise error ϵ_i^J can be distributed across all subcarriers. Pilot nulling has an even more serious effect. H_i is moved from the denominator to the numerator of the error term, making its impact greater. If the channel estimation error $\hat{\delta}_i$ is small, this term is significant. MIMO-OFDM channel sounding jamming attacks and channel sounding singularity attacks are similar to pilot jamming attacks and pilot nulling attacks and have similar effect on the performance. The effect on bit error rate will be investigated through analysis and simulation in the next sections.

G. Equalization Attack Mitigation

The *pilot nulling* attacks can be avoided by transmitting pilot tones whose values are unknown to the attackers. In the absence of knowledge about pilot tone values, *pilot nulling* becomes as effective as *pilot jamming* that can be avoided by randomizing the pilot locations.

If we assign the pilots randomly, then the distance between two adjacent pilot tones becomes a random variable. Let us define this distance as a random variable X, where $X = (x_{i+1} - x_i)$, and a new random variable Y, where $Y = X^2$. Notice that the random variable Y will have a different distribution than X. So, the approximation error bound of (15) becomes $|E(x_1, x_0)| \leq KY$ [6]. In [6], two strategies for randomization are proposed:

1) Scenario 1—Binned Uniform Distribution: In this case, we assume that two adjacent pilot tones can be located anywhere between subcarriers $(id, (i+1)d)$ (i.e., confined in a binned range of subcarriers). Here, multiplication factor d is the deterministic separation between two adjacent pilot tones used in traditional schemes. Let us consider a scenario where pilot x_i is located at 0th location index, then the pilot tone x_{i+1} will be anywhere within a bin that spreads between 0 to d. So, we can say that the location of pilot tone x_{i+1} has a uniform distribution in $(id, (i+1)d)$.

2) Scenario 2—Unbinned Uniform Distribution: In this case, we assume the pilot tone locations are completely random; not confined in a bin like the previous case. The only restriction that applies here is that there must be a total of N expected number of pilot tones within the entire channel bandwidth, during one OFDM symbol. Such an event can be modeled as Poisson process which ensures the average number of events occurs within a finite interval.

3) Pseudorandom Keystream: The randomization of pilots should be done in such a way that only the legitimate users know the locations in advance, but the attackers do not. This will certainly make joining the network difficult, since new users of the network would not have the necessary information to acquire and equalize the signal. However, it may prove effective in mission critical situations. Any clues given to allow new users would also give information away to adversaries, unless cryptographically protected in some way. One way this can be achieved is by maintaining a truth table containing all possible pseudorandom pilot locations in every legitimate user's receiver. Another approach would be using a pseudorandom keystream generator to specify the locations of the pilot tones. This is seeded by a shared secret key known to members of the network, and an initialization vector changed

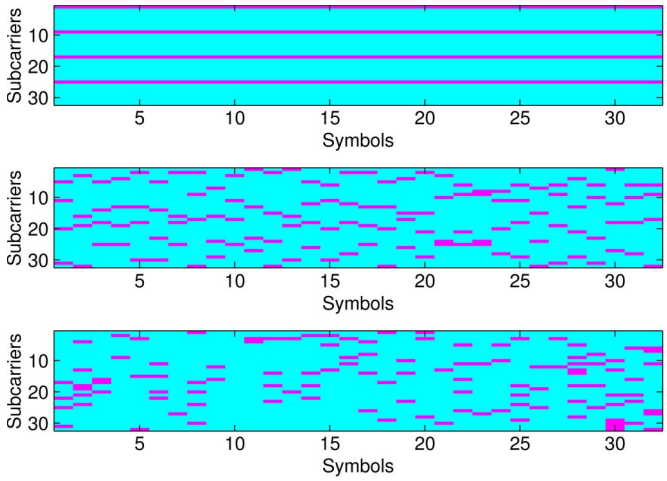

Fig. 13. OFDM time-frequency lattice with three different pilot signal organization schemes: (a) existing equally spaced deterministic but optimum scheme, (b) scheme where pilots are uniformly distributed within a confined bin, and (c) a scheme where pilots are randomly located with location random variable follow exponential distribution.

every frame. Automated key management could be performed at higher protocol layers, but this still requires all devices to be provisioned with the current key to join the network.

H. Performance Analysis

We developed simulation based on the OFDM channel model shown in Fig. 2 to validate the performance of pilot attacks and mitigation via randomization. In the receiver, QPSK modulated data and pilot tones are passed through an IFFT operation and then sent over an 8-tap random channel and finally AWGN is added. The OFDM modulation uses a 256-point FFT with a cyclic prefix length of (1/8). The deterministic OFDM scheme has every 8th subcarrier as a pilot tone. The attack signal is added to the received signal after being passed through a channel with different filter tap coefficients. In the receiver, combined target and jamming signal are received, passed through the FFT, and equalized using the linear interpolation method based on pilot tones. Simulations are executed for 10 000 iterations for different SNRs and SJRs. The channel between the transmitter and target is assumed to be perfectly known to the jammer.

Fig. 13 shows a sample OFDM frame with three different arrangements of pilot tone locations: (a) existing equal spacing (deterministic), (b) uniformly distributed within a bin whose length is equal to the deterministic pilot spacing, and (c) randomly scattered pilot spacing which is exponential distributed.

Now we will look into the performance impact of different pilot location schemes both in the presence and in the absence of jamming attacks, to justify the motivation for randomizing pilot locations. Fig. 14 shows the performance of the three pilot spacing schemes in the absence of pilot tone jamming and in the presence of pilot jamming where the JSR is 0 dB.

In absence of jamming, the deterministic signal has the best bit error rate (BER) performance followed by confined bin and completely random scheme. At 0.2 BER, the deterministic scheme requires 1 dB SNR, confined bin scheme requires 2 dB

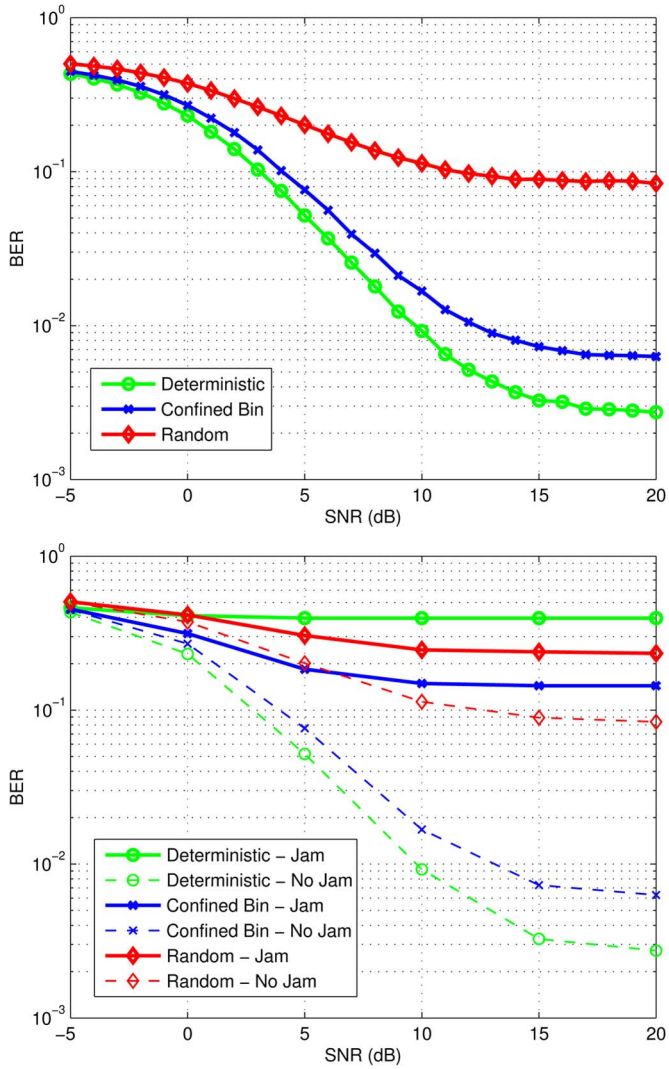

Fig. 14. Bit error rate (BER) performance of the three pilot spacing schemes (i.e., deterministic, confined bin, and random) when there is no jamming signal present in the horizon (Top) and when the target receiver is under pilot jamming attack (Bottom).

SNR, and the random scheme requires 5 dB SNR. This finding is consistent with previous results [51], [52]. In the presence of pilot jamming, at 0.2 BER confined bin scheme requires 5 dB SNR, and completely random scheme requires 10 dB SNR. The benefit of randomizing pilot locations is clearly visible from this figure. In the presence of a pilot jamming, deterministic pilots get jammed and the error due to wrong pilot tone estimation becomes high. To make thing worse, this error further propagates during interpolation and approximation. Both confined bin and random scheme outperform the deterministic one during pilot jamming attack.

Our second objective is to explore the performance behavior pattern for jamming attacks with different strength. In Fig. 15 we compared the performance of three pilot spacing schemes in the presence of pilot jamming by varying the SJR with target signal SNR of 10 dB. At 0 dB JSR, the deterministic scheme's BER is 0.4, confined bin's BER 0.15, and random scheme's BER is 0.25. It can be seen that at high JSR, confined bin performs best. Even the completely random scheme performs

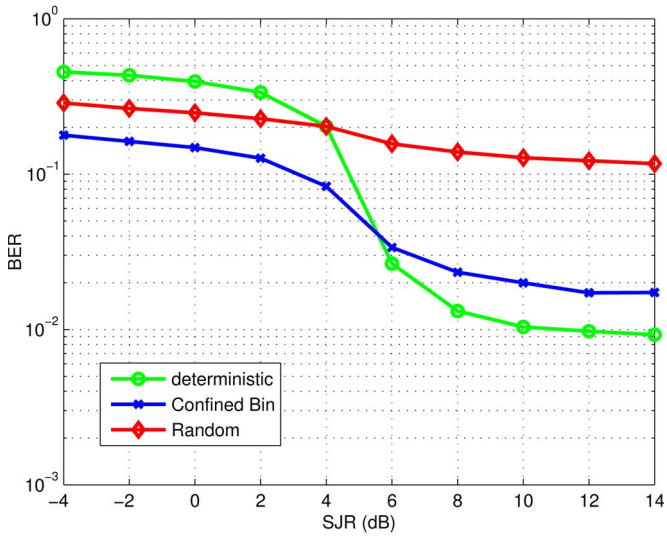

Fig. 15. Bit error rate (BER) performance of three pilot spacing schemes (i.e., deterministic, confined bin, and random) in the presence of pilot jamming and as function of SJR with target signal SNR of 10 dB.

TABLE II
VARIOUS CONTROL CHANNEL ATTACKS

Attack	Features
HARQ Acknowledgement Attack	Corrupt the ARQ mechanism using intentional interference placed on the location of Acknowledgements in time and/or frequency
Random Access Channel Attack	Interfere with the random access channel so that users are unable to initially access a cell
Modulation Indicator Attack	Prevent users from being able to receive information about the modulation scheme used for each block of data
Resource Allocation Attack	Block the base station from indicating which resources are assigned to which user (downlink attack), or prevent users from being able to request a resource grant (uplink attack)

better than the deterministic one. However, at low JSR, the performance pattern is much like the no-jamming case. At -10 dB JSR (equivalent to 10 dB of SJR), the deterministic scheme's BER is 0.01, confined bin's BER 0.02, and completely random scheme's BER is 0.1.

XI. CONTROL CHANNEL ATTACKS

Previously, we have discussed methods of jamming which target a physical layer attribute or mechanism of OFDM. This approach is expected, because jamming is the process of injecting interference at the physical layer. However, in some cases a more effective jamming attack can be realized by targeting a higher layer mechanism. Table II summarizes four of these higher layer mechanisms, which we will discuss further in this section. If it can be determined how the mechanism manifests itself on the physical layer, then a jamming attack is feasible. In wireless broadband technologies such as LTE and WiMAX, this physical layer manifestation is typically in the form of control channels (i.e., physical channels that are not used for data), which are mapped to certain OFDM symbols and subcarriers. For an in depth survey of the physical layer vulnerabilities in LTE we refer the reader to [7], [49], [81], [82], and for physical layer vulnerabilities in WiMAX we refer the reader to [50], [83].

The term Resource Element (RE) is commonly used to refer to a single subcarrier over a single OFDM symbol. The number of bits carried in each RE is determined by the modulation order (e.g., a 16-QAM RE will carry 4 bits of information). OFDM is a unique modulation in that it carries information in both the time and frequency domains. This inherent characteristic of OFDM allows for attacks against components of the signal without the need for time-domain synchronization. Synchronization adds complexity to the jammer, making the attack less likely to be launched by an adversary.

Notation: In this section, $(J/S)_{RE}$ denotes a (J/S) when only taking into account a specific set of REs. $(J/S)_F$ denotes a (J/S) when taking into account the entire frame (every subcarrier across all OFDM symbols) of a downlink or uplink signal. Converting from $(J/S)_{RE}$ to $(J/S)_F$ requires determining the fraction of REs used by the given physical channel, relative to the entire frame.

A. HARQ Acknowledgement Attack

Wireless broadband technologies (i.e., LTE, WiMAX) use an error control mechanism known as Hybrid Automatic Repeat reQuest (HARQ), which combines channel coding (a.k.a. forward error correction) and Automatic Repeat reQuest (ARQ). Although there are multiple ways to incorporate ARQ in an OFDMA system, they all involve the receiving node transmitting either positive or negative acknowledgement indicators back to the sender. These acknowledgements are used to trigger retransmissions in cases where forward error correction does not provide enough redundancy to correct channel errors. This situation may occur after a deep fade, in which a high BER is sustained throughout the frame or sub-frame, and data is lost. For a detailed analysis of HARQ schemes and how they perform in OFDMA systems, we refer the reader to [84].

Acknowledgements sent from the base station (or wireless gateway) to the user are transmitted on a portion of the downlink signal. Acknowledgements are typically represented using single bits (prior to channel coding), indicating positive or negative reception of data. Each acknowledgement must correspond to a chunk of data sent in the past; a common rule is for a given acknowledgement to be associated with data sent during the previous frame.

The objective of the HARQ Acknowledgement Attack is to corrupt the ARQ mechanism using intentional interference by targeting acknowledgement indicators. It is conventional for the acknowledgement indicator to be sent over the channel using a low rate coding scheme (causing high redundancy), but with no additional error checking. The result is an indicator which when corrupted, will feed the radio false information. A corrupted acknowledgement indicator will lead to either an unnecessary retransmission, or a delay in the requested

retransmission. Unnecessary retransmissions will almost surely reduce throughput, while delayed retransmissions increase latency and can hinder quality of service. Both situations can lead to network congestion or failure if enough users are affected. In fact, if certain types of time-sensitive data do not reach their destination in time (e.g., voice over IP data), then the communications link is considered inadequate [85].

The $(J/S)_{RE}$ required to corrupt a given acknowledgement indicator is highly dependent on the modulation and coding scheme used. For the purpose of estimating $(J/S)_{RE}$ we will consider a BER of 0.1, after decoding, to be enough to cause an exceedingly high amount of corrupted acknowledgements. This is just an approximation; a more accurate threshold would require simulation of the modern wireless broadband system or even a real-world testbed. The authors of [86] analyze various turbo coding schemes using in cellular equipment. In each scheme, using BPSK, the BER reaches 0.1 at around 0 to 2 dB of SNR. Although this is a rough estimate, we can use these results to approximate $(J/S)_{RE}$ to be 1 dB. For the purpose of estimating $(J/S)_F$, we will consider a downlink signal which uses 1% of REs for HARQ acknowledgements. The $(J/S)_F$ for this attack would then be around -19 dB. Although this is just an example, it demonstrates the gains associated with targeting a sparse control channel.

The complexity of attack is dependent on how the ARQ acknowledgements are manifested on the physical layer. The REs assigned to acknowledgements are often different for each base station, to reduce inter-cell interference. In these cases, the jammer would have to synchronize with the target base station(s) for this attack to be feasible. The result is a jammer which needs receiving and signal processing capability.

B. Random Access Channel Attack

Random access requests are used in wireless broadband technologies as a method for users to initially access a base station. A random access request is transmitted by a user to indicate that it is present and would like to be allocated channel resources. These requests are typically transmitted in a portion of the uplink bandwidth which is set aside for random access, using a contention-based access scheme [87]. A contention-based approach involves users sharing the same pool of resources without pre-coordination, which means collisions are expected. One method of reducing the impact of collisions is for each user to transmit a sequence randomly chosen from a set of sequences with low cross-correlation. This allows the base station to identify the presence of two or more overlapping random access requests. Once the base station receives the request it will respond with an uplink resource grant, which allocates a certain amount of uplink resources to the user. The user can then use the newly allocated resources to reply to the base station, and exchange more information.

A sequence commonly used for random access requests (a.k.a. random access preambles) is the Zadoff-Chu sequence [88]. An N length Zadoff-Chu sequence is given by

$$x(n) = \exp\left(-j\frac{\pi un(n+1+2q)}{N}\right),\ 0 \le n \le N-1 \quad (39)$$

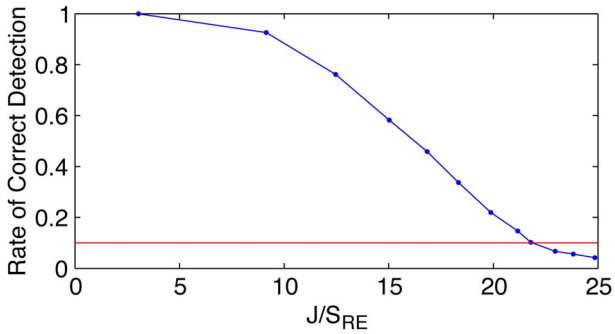

Fig. 16. (J/S) required for a jammer to successfully corrupt a random access channel, in which corruption is defined by a 10% rate of correct signal detection.

where u is the root of the sequence, and q is an offset. Zadoff-Chu sequences are complex valued, and have a constant amplitude of 1. In addition, when N is prime, they have an autocorrelation function that resembles an impulse. This is extremely useful for detection at the base station, as well as ensuring two offset Zadoff-Chu sequences remain orthogonal.

The random access attack is the process of interfering with the portion of the uplink bandwidth, or REs, assigned to random access requests. We will first consider an interferer transmitting AWGN. By flooding the random access channel with enough noise, the base station will struggle with receiving random access requests, thus denying users from initiating communications. The $(J/S)_{RE}$ required to cause a corrupted random access request is based on the amount of noise needed for the base station receiver to have a high probability of detecting any given sequence incorrectly. When this occurs, the base station will reply to the random access request, but the reply will be addressed incorrectly and not parsed by user.

To find the minimum $(J/S)_{RE}$ for the noise-based attack to have a high probability of success, we performed a simulation using Zadoff-Chu sequences as the random access preamble and AWGN interference as the jamming waveform. The sequence is assumed to be demodulated coherently at the receiver, and correlated against all possible sequences. We used a set of 64 different length-853 sequences, and determined the probability of correct detection for a single random access request. All 64 sequences use the same root sequence, but are cyclically shifted by a certain amount. For a more detailed explanation of this type of detection procedure, we refer the reader to [89]. The results of this simulation are shown in Fig. 16. It is observed that a 10% probability of correct detection occurs at roughly 22 dB of $(J/S)_{RE}$. When the entire bandwidth is taken into account, the jammer receives a gain due to the sparse nature of the random access channel, and thus will have a much lower $(J/S)_F$. For example, a random access channel which occupies 10% of the uplink channel resources equates to a $(J/S)_F$ of roughly 12 dB. This $(J/S)_F$ is high when compared to other attacks, leading to the conclusion that transmitting noise on the random access channel is not an effective method for causing denial of service.

We will now investigate the idea of transmitting a randomly selected Zadoff-Chu sequence repeatedly, which can be thought of as spoofing random access requests. In order for

the correlation-based detector to choose the spoofed sequence over the actual sequence(s), the $(J/S)_{RE}$ at the input to the base station's receiver must be greater than or equal to zero, when ignoring channel noise. A small margin of (J/S) could be added if noise is to be taken into account, but as we saw from the previous results, noise does not have a large effect on a length-853 sequence. Using a spoofed sequence which arrives at the receiver 2 dB higher than the actual sequence ($(J/S)_{RE} = 2$ dB), and a random access channel which occupies 10% of the uplink signal, we find that the spoofing form of this attack requires roughly -8 dB of $(J/S)_F$. Although these results are very rough approximations, they demonstrate the difficulty in jamming a long sequence with AWGN.

Similar to the HARQ Acknowledgement Attack, the complexity involved with this form of jamming is highly based on how the target channel is mapped in both time and frequency, and whether this placement is constant or varies by base station. If the channel uses dedicated subcarriers, and the locations of these subcarriers are known by the adversary, then this attack only involves generating and transmitted an RF signal composed of a bogus random access request.

C. Modulation Indicator Attack

As discussed in Section III, one of the benefits of OFDM is that it causes the channel to be split up into a series of subchannels. This allows a wireless system to cope with a fading channel (or other channel impairments) by varying the modulation scheme of each subcarrier independently. For example, subcarriers experiencing good channel conditions could be assigned to use 64-QAM, while those experiencing higher attenuation may fall back to QPSK. Using adaptive modulation is only possible if the receiver sends Channel Quality Indicators (CQIs) back to the transmitter. The transmitter then adjusts the modulation scheme used for each subcarrier, and transmits modulation indicators along with the data. This two-way process typically occurs dozens of times per second, to deal with rapidly changing channel conditions [87]. The modulation indicators in wireless broadband are often combined with other downlink control information and transmitted by the base station on a physical control channel. Although it is theoretically possible for a user to decode the downlink data using all possible modulation schemes, and determine the modulation scheme used through trial and error, we can assume that this approach will not be used in implementations for the sake of complexity.

The modulation indicator attack involves jamming the modulation scheme indicators with the purpose of causing the receiver to incorrectly demodulate data, which will almost surely lead to a higher BER. Although it is possible to jam the CQIs instead of the indicators, this will not necessarily cause denial of service. Corrupted CQIs will lead to either a lower modulation order on a subcarrier which would otherwise be able to handle more, or an excessively high modulation order which will increase the BER on the subcarrier. Although this is still damaging to the overall link, jamming the modulation indicators directly will clearly have a more adverse effect. The $(J/S)_{RE}$ required for a successful modulation indicator attack

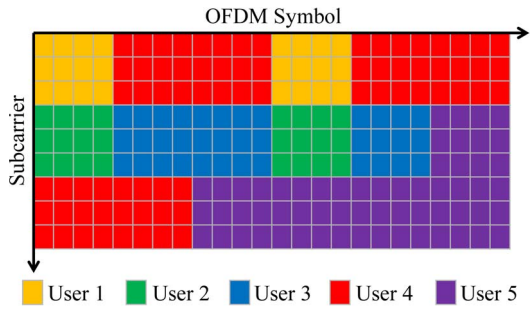

Fig. 17. An OFDM time-frequency lattice, showing an example resource allocation for five users.

is highly based on the modulation and coding scheme used on the control channel which carries the indicator; similar to the ARQ acknowledgement attack. However, unlike the ARQ acknowledgement attack, control channels carrying modulation indicators typically use a Cyclic Redundancy Check (CRC), which is a form of error detection. Therefore, the receiver will know when the information is corrupt, and may decide to not use the information. Assuming the receiver does not attempt blind modulation decoding, as discussed earlier, there are three actions the receiver may take in response to a CRC failure:

1) Use the decoded modulation indicator, even though an error was detected.
2) Use the most recently known modulation scheme.
3) Discard the data.

If enough noise is transmitted on top of the modulation indicators, then the first action will almost surely lead to a high BER. The second action may suffice for a short period of time, but as the channel conditions change, the modulation scheme will also change. If the third action is taken repeatedly, then the user will enter a disconnected state.

D. Resource Allocation Attack

The wireless interface of wireless broadband systems must support a large number of users per base station. Therefore, the available uplink and downlink resources are split between multiple users in both time and frequency. This allocation of resources happens rapidly, due to the low-duty cycle of wireless data traffic (e.g., browsing the web). In addition, the subcarrier allocation is based on the channel conditions seen by each user, so a user experiencing a rapidly changing channel will be reallocated resources fairly often. Fig. 17 shows a portion of signal, over time and frequency, which has been split up to accommodate five users with varying data requirements. Each small block represents a RE. Multiple REs are combined into a group because allocating single REs would add unneeded complexity and reduce throughput (more bits would be needed to exchange allocation information). Typically, the downlink control channel will include information about which users are assigned which subcarriers for a given period of time. This period of time may be as low as 1 millisecond, and the user must receive this information to decode its corresponding data [88]. Because the resource allocation is typically transmitted on the same physical channel as the downlink modulation

TABLE III
SUMMARY OF OFDM THREATS

Attack	Type	Synch. Required	Strength	Weakness
Broadband Noise	Noise	None	Simplest, optimum in absence of waveform knowledge	Power inefficient, impractical for wideband systems
Partial Band Noise	Noise	None	Simple	Power inefficient, less effective
Single-tone	Noise	None	Simple	Power inefficient, less effective
Multi-tone	Noise	None	Simple	Power inefficient, less effective
Interference	Colored	None	Relatively efficient	Less effective, complicated to synthesize, waste of resources
Pilot Jamming	Correlated	Pilot location sych. needed	Power efficient, effective	Sensitive to pilot location
Pilot Nulling	Correlated	Pilot location sych. needed	Power efficient, effective, Denial of Service (DOS)	Sensitive pilot location, obtaining CSI may be difficult
Channel Sounding	Correlated	Pilot location sych. needed	Power efficient, effective, DOS	Sensitive to pilot location, obtaining CSI may be difficult
Cyclic Prefix	Correlated	Frame start timing	Power efficient, effective, DOS	Sensitive to time alignment
Preamble Whitening	Correlated	Loose timing	No waveform synthesis	Power inefficient
False Preamble	Correlated	Loose timing or continuous jamming	Power efficient, spoofing	Preamble format required
Preamble Warping	Correlated	Precise or continuous jamming	Power efficient	Algorithm specific
Preamble Nulling	Correlated	Precise	Complete denial of service	Exact channel state information, synchronization required
Preamble Phase Warping	Correlated	Precise timing	Power efficient, spoofing	Precise timing
Differential Scrambling	Correlated	Precise	Power efficient	Frequency synch. required
HARQ Acknowledgment	Correlated	Timing and knowledge of the Protocol	Efficient, immediate DOS	Finding locations of HARQs may be difficult
Random Access Channel	Correlated	Timing and knowledge of the Protocol	Channel is usually placed statically	Does not cause immediate DOS
Modulation Indicator	Correlated	Timing and knowledge of the Protocol	Efficient	May not cause immediate DOS
Resource Allocation	Correlated	Timing and knowledge of the protocol	Efficient, immediate DOS	Allocations may be multiplexed with other info

indicators, both attacks can be merged into a single attack from the perspective of a physical layer adversary (i.e. jammer). However, for the purpose of analysis, we discuss the two attacks independently.

Corrupting the resource allocation information can quickly cause denial of service, simply because users will not be able to decode any downlink data. As discussed in Section C, the (J/S) required for this attack to succeed is dependent on the given system and configuration.

E. Control Channel Attack Mitigation

The attacks described in this section all have one feature in common; they involve jamming a portion of the uplink or downlink signal which does not contain actual data. Therefore, a possible mitigation strategy would be to include the vulnerable control information in resources which would normally be occupied with data. The redundant control information would only be necessary when there is a communication failure. This is a retroactive approach which would have to be triggered by the detection of an attack, and although it would decrease throughput while active, it is a better alternative to denial of service. Detection of an attack could be as simple as detecting a sudden loss in communications from multiple users. A more complex approach would be monitoring for extra energy on the control channels.

A second mitigation strategy involves randomizing the locations of control channels in both time and frequency, and passing the location information to the user using a shared key. This method would be appropriate for every attack except random access channel jamming, for two reasons. First, the jammer may be able to detect the location in which new users transmit random access requests by sensing the channel. Second, depending on the system, a user who is initially accessing a cell may not have any form of authentication yet, and therefore would not be able to receive encrypted information. Many wireless broadband systems already incorporate a mechanism similar to this strategy, in which the mapping of physical channels is based on the base station ID. This is primary to avoid inter-cell inference, but it also adds complexity to the attacker models described in this section.

We have showed a comprehensive list of all the different types attacks possible against OFDM in Table III.

XII. CONCLUSION

OFDM and its variants such as OFDMA and SC-FDMA have emerged as the primary contender for the air interface of most of the modern wireless broadband communication systems (i.e., LTE, WiMAX, etc). In this tutorial paper, we have discussed the structure of OFDM-based systems, explored potential threats from adversaries, and analyzed the robustness and weakness of practical OFDM-based systems. We have also investigated the conventional jamming attacks and introduced more effective jamming strategies such as synchronization jamming attacks, equalization jamming attacks, and control channel jamming attacks. While going over these energy efficient jamming attacks, we did not limit ourselves in pointing out the loopholes; rather we went on and showed ways to encounter such jamming attacks. We have found that the randomization of reference signals, and pilot locations/values followed by cryptographic techniques for pseudorandom key management can eliminate most of these security threats and create a fairly resilient OFDM waveform that can be deployed in wide range of practical scenarios including commercial, public safety, and military scenarios.

REFERENCES

[1] Connecting America: The National Broadband Plan, 2010.

[2] "FCC band plan on public safety spectrum at 700 MHz," FCC, WT Docket No. 06-150, Aug. 2007.

[3] T. C. Clancy, "Efficient OFDM denial: Pilot jamming and pilot nulling," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2011, pp. 1–5.

[4] M. LaPan, T. C. Clancy, and R. W. McGwier, "Jamming attacks against OFDM timing synchronization and signal acquisition," in *Proc. MILCOM Conf.*, Oct. 2012, pp. 1–7.

[5] M. LaPan, T. C. Clancy, and R. W. McGwier, "Phase warping and differential scrambling attacks against OFDM frequency synchronization," in *Proc. IEEE ICASSP*, May 2013, pp. 2886–2890.

[6] C. Shahriar and T. C. Clancy, "Performance impact of pilot tone randomization to mitigate OFDM jamming attacks," in *Proc. IEEE CCNC*, Jan. 2013, pp. 813–816.

[7] M. Lichtman, J. Reed, T. Clancy, and M. Norton, "Vulnerability of LTE to hostile interference," in *Proc. IEEE GlobalSIP*, Dec. 2013, pp. 285–288.

[8] J. Grimes, "Commercial wireless metropolitan area network (WMAN) systems and technologies," Memo 8–39, Jan. 2009.

[9] T. C. Clancy and T. O'Shea, "Transec mitigation options for wireless metropolitan area networks," in *Proc. IEEE Mil. Commun. Conf.*, Boston, MA, USA, Oct. 2009.

[10] T. Basar, "The Gaussian test channel with an intelligent jammer," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 1, pp. 152–157, Jan. 1983.

[11] T. Schmidl and D. Cox, "Robust frequency and timing synchronization for OFDM," *IEEE Trans. Commun.*, vol. 45, no. 12, pp. 1613–1621, Dec. 1997.

[12] P. Moose, "A technique for orthogonal frequency division multiplexing frequency offset correction," *IEEE Trans. Commun.*, vol. 42, no. 10, pp. 2908–2914, Oct. 1994.

[13] J. van de Beek, "Low-complex frame synchronization in OFDM systems," in *Proc. IEEE ICUPC*, Nov. 1995, pp. 982–986.

[14] M. Ozdemir and H. Arslan, "Channel estimation for wireless OFDM systems," *IEEE Commun. Surveys Tuts.*, vol. 9, no. 2, pp. 18–48, 2007.

[15] E. Dahlman, S. Parkvall, and J. Skold, *4G: LTE/LTE-Advanced for Mobile Broadband*, 1st ed. San Diego, CA, USA: Academic, 2011.

[16] J. Luo, J. Andrian, and C. Zhou, "Bit error rate analysis of jamming for OFDM systems," in *Proc. WTS*, Apr. 2007, pp. 1–8.

[17] F. Renna, N. Laurenti, and Y.-C. Hu, "The jamming game in an OFDM setting," in *Proc. 5th Int. ICST Conf. Perform. Eval. Methodol. VALUETOOLS*, Brussels, Belgium, 2011, pp. 496–505.

[18] D. W. Chi and P. Das, "Effects of jammer and nonlinear amplifiers in MIMO-OFDM with application to 802.11n WLAN," in *Proc. IEEE Mil. Commun. Conf.*, Nov. 2008, pp. 1–8.

[19] K. Pietikainen, A. Silvennoinen, M. Hall, and S. G. Haggman, "IEEE 802.11g tolerance to narrowband jamming," in *Proc. IEEE Mil. Commun. Conf.*, Oct. 2005, vol. 3, pp. 1825–1830.

[20] L. Lightfoot, L. Zhang, and T. Li, "Performance of QO-STBC-OFDM in partial-band noise jamming," in *Proc. 44th Annu. Conf. Inf. Sci. Syst.*, Mar. 2010, pp. 1–6.

[21] A. Best and B. Natarajan, "The effect of jamming on the performance of carrier interferometry/OFDM," in *Proc. IEEE Int. Conf. Wireless Mobile Comput., Netw. Commun.*, Aug. 2005, pp. 66–70.

[22] D. W. Chi and P. Das, "Effects of nonlinear amplifier and partial band jammer in OFDM with application to 802.11n WLAN," in *Proc. IEEE Mil. Commun. Conf.*, Oct. 2007, pp. 1–8.

[23] J. Park, D. Kim, C. Kang, and D. Hong, "Effect of partial band jamming on OFDM-based WLAN in 802.11g," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, Apr. 2003, vol. 4, pp. 560–563.

[24] R. Jha, S. Limkar, and U. Dalal, "Performance analysis under the influence of jamming for WiMAX system," in *Proc. 2nd Int. Conf. Emerging Appl. Inf. Technol.*, Feb. 2011, pp. 292–297.

[25] T. Karhima, A. Silvennoinen, M. Hall, and S.-G. Haggman, "IEEE 802.11b/g WLAN tolerance to jamming," in *Proc. IEEE Mil. Commun. Conf.*, Oct. 2004, pp. 1364–1370.

[26] D. W. Chi and P. Das, "Effect of jammer on the performance of OFDM in the presence of nonlinearity in Rayleigh fading channel with application to 802.11n WLAN," in *Proc. IEEE Mil. Commun. Conf.*, Oct. 2006, pp. 1–7.

[27] J. Li and S.-G. Haggman, "Performance of IEEE802.16-2004 based system in jamming environment and its improvement with link adaptation," in *Proc. 17th IEEE Int. Symp. Pers., Indoor, Mobile Radio Commun.*, Sep. 2006, pp. 1–5.

[28] I. Harjula, J. Pinola, and J. Prokkola, "Performance of IEEE 802.11 based WLAN devices under various jamming signals," in *Proc. Mil. Commun. Conf.*, Nov. 2011, pp. 2129–2135.

[29] H. Minn, V. Bhargava, and K. Letaief, "A combined timing and frequency synchronization and channel estimation for OFDM," in *Proc. IEEE ICC*, Jun. 2004, pp. 872–876.

[30] M. Moretti and I. Cosovic, "OFDM synchronization in an uncoordinated spectrum sharing scenario," in *Proc. IEEE GLOBECOM*, Nov. 2007, pp. 3796–3801.

[31] S. Patil and R. Upadhyay, "A symbol timing synchronization algorithm for WiMAX OFDM," in *Proc. CICN*, Oct. 2011, pp. 78–82.

[32] J. Kleider, S. Gifford, G. Maalouli, S. Chuprun, and B. Sadler, "Synchronization for RF carrier frequency hopped OFDM: Analysis and simulation," in *Proc. IEEE Mil. Commun. Conf.*, Oct. 2003, pp. 1237–1242.

[33] L. Nasraoui, L. Atallah, and M. Siala, "An efficient reduced-complexity two-stage differential sliding correlation approach for OFDM synchronization in the AWGN channel," in *Proc. IEEE VTC*, Sep. 2011, pp. 1–5.

[34] T. Pollet, M. V. Bladel, and M. Moeneclaey, "BER sensitivity of OFDM systems to carrier frequency offset and wiener phase noise," *IEEE Trans. Commun.*, vol. 43, no. 2–4, pp. 191–193, Feb.–Apr. 1995.

[35] L. Sanguinetti, M. Morelli, and H. V. Poor, "Frame detection and timing acquisition for OFDM transmissions with unknown interference," *IEEE Trans. Wireless Commun.*, vol. 9, no. 3, pp. 1226–1236, Mar. 2010.

[36] K. Ramiah and M. Zivkovic, "OFDM synchronization in the presence of interference," in *Proc. ICCSPA*, 2013, pp. 1–5.

[37] L. Tao *et al.*, "Robust joint interference detection and decoding for OFDM-based cognitive radio systems with unknown interference," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 3, pp. 566–575, Apr. 2007.

[38] P. Sun and L. Zhang, "Narrowband interference effect on timing synchronization for OFDM-based spectrum sharing system," in *Proc. ICWMC*, 2010, pp. 274–278.

[39] M. Marey and H. Steendam, "Analysis of the narrowband interference effect on OFDM timing synchronization," *IEEE Trans. Signal Process.*, vol. 55, no. 9, pp. 4558–4566, Sep. 2007.

[40] R. Prasad, *OFDM for Wireless Communications Systems*. Norwood, MA, USa: Artech House, 2004.

[41] R. P. R. van Nee, *OFDM for Wireless Multimedia Communications*. Norwood, MA, USA: Artech House, 2000.

[42] T. C. Clancy and N. Georgen, "Security in cognitive radio networks: Threats and mitigations," in *Proc. 3rd Int. Conf. CrownCom*, 2008, pp. 1–8.

[43] S. Sodagari and T. C. Clancy, "Efficient jamming attack on MIMO channels," in *Proc. IEEE ICC*, Jun. 2012, pp. 852–856.

[44] C. Shahriar, S. Sodagari, and T. C. Clancy, "Performance of pilot jamming on MIMO channels with imperfect synchronization," in *Proc. IEEE ICC*, Jun. 2012, pp. 898–902.

[45] C. Mueller-Smith and W. Trappe, "Efficient OFDM denial in the absence of channel information," in *Proc. IEEE MILCOM Conf.*, Nov. 2013, pp. 89–94.

[46] M. Han *et al.*, "An efficient channel estimation algorithm under narrowband jamming for OFDM systems," in *Proc. IEEE Mil. Commun. Conf.*, Oct. 2006, pp. 1–6.

[47] M. Han *et al.*, "OFDM channel estimation with jammed pilot detector under narrow-band jamming," *IEEE Trans. Veh. Technol.*, vol. 57, no. 3, pp. 1934–1939, May 2008.

[48] C. Patel, G. Stuber, and T. Pratt, "Analysis of OFDM/MC-CDMA under channel estimation and jamming," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Mar. 2004, vol. 2, pp. 954–58.

[49] R. Jover, "Security attacks against the availability of LTE mobility networks: Overview and research directions," in *Proc. 16th Int. Symp. WPMC*, Jun. 2013, pp. 1–9.

[50] M. Barbeau, "WiMax/802.16 threat analysis," in *Proc. 1st ACM Int. Workshop Qual. Serv. Security Wireless Mobile Netw.*, 2005, pp. 8–15.

[51] S. Ohno and G. B. Giannakis, "Optimal training and redundant precoding for block transmissions with application to wireless OFDM," in *Proc. IEEE ICASSP*, 2001, vol. 4, pp. 2389–2392.

[52] R. Negi and J. Cioffi, "Pilot tone selection for channel estimation in a mobile OFDM system," *IEEE Trans. Consum. Electron.*, vol. 44, no. 3, pp. 1122–1128, Aug. 1998.

[53] J. Stoer and R. Bulirsch, *Introduction to Numerical Analysis*. Berlin, Germany: Springer-Verlag, 2002.

[54] P. Massopust, *Interpolation and Approximation with Spline and Fractals*. Oxford, U.K.: Oxford University Press, 2010.

[55] R. A. Poisel, *Modern Communications Jamming: Principle and Techniques*. Norwood, MA, USA: Artech House, 2011.

[56] D. J. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," in *Proc. IEEE MILCOM*, 2006, vol. 6, pp. 1075–1081.

[57] E. Bayraktaroglu *et al.*, "On the performance of IEEE 802.11 under jamming," in *Proc. 27th IEEE INFOCOM*, 2008, pp. 1939–1947.

[58] K. Fazel and S. Kaiser, *Multi-Carrier and Spread Spectrum Systems: From OFDM and MC-CDMA to LTE and WiMAX*. Hoboken, NJ, USA: Wiley, 2008.
[59] S. Chao, W. Ping, and S. Guozhong, "Performance of OFDM in the presence of multitene jamming," in *Proc. IEEE ISRA*, Jun. 2012, pp. 118–121.
[60] R. Jantti, J. Kerttula, K. Koufos, and K. Ruttik, "Aggregate interference with FCC and ECC white space usage rules: Case study in Finland," in *Proc. IEEE Symp. New Frontiers DySPAN*, 2011, pp. 599–602.
[61] L. Shi, K. W. Sung, and J. Zander, "Secondary spectrum access in tv-bands with combined co-channel and adjacent channel interference constraints," in *Proc. IEEE Int. Symp. DYSPAN*, 2012, pp. 452–460.
[62] J. H. Reed and N. Tripathi, "Analysis of the V-COMM report estimating the impact of channel 51 and E block interference on band 12 and band 17 user equipment receivers," FCC, Washington, DC, USA, WT Docket 12–69, 2012.
[63] J. H. Reed and N. Tripathi, "The 600 MHz spectrum auction: An analysis of the band plan framework," FCC, Washington, DC, USA, 2013.
[64] "FCC: Concerning the 600 MHZ band plan," Washington, DC, USA, GN Docket 12–268, May 2013.
[65] E. Millios *et al.*, "Impact of low-frequency radar interference on digital terrestrial television," *IEEE Trans. Broadcast.*, vol. 59, no. 1, pp. 84–95, Mar. 2013.
[66] J. E. Bryson and L. E. Strickling, "An assessment of the viability of accommodating wireless broadband in the 1755–1850 MHz band," U.S. Dept. Commerce, Washington, DC, USA, Mar. 2012.
[67] M. LaPan, C. Clancy, and R. W. McGwier, "Protecting physical layer synchronization: Mitigating attacks against OFDM acquisition," in *Proc. 16th Int. Symp. WPMC*, 2013, pp. 1–6.
[68] P. Klenner and K. Kammeyer, "Temporal autocorrelation estimation for OFDM with application to spatial interpolation," in *Proc. Asilomar Conf. Signals, Syst. Comput.*, Oct. 2008, pp. 995–999.
[69] J. A. Mahal and T. Clancy, "The closed-form BER expressions of PSK modulation for OFDM and SC-FDMA under jamming and imperfect channel estimation," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 2221–2226.
[70] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[71] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[72] Y. Cho, J. Kim, W. Yang, and C. Kang, *MIMO-OFDM Wireless Communications With MATLAB*. Hoboken, NJ, USA: Wiley, 2010.
[73] J. G. Andrews, A. Ghosh, and R. Muhamed, *Fundamentals of WiMAX: Understanding Broadband Wireless Networking*. Upper Saddle River, NJ, USA: Prentice-Hall, 2007.
[74] S. Sesia, I. Toufik, and M. Baker, *LTE—The UMTS Long Term Evolution: From Theory to Practice*, 2nd ed. Hoboken, NJ, USA: Wiley, 2011.
[75] R. Miller and W. Trappe, "On the vulnerabilities of CSI in MIMO wireless communication systems," *IEEE Trans. Mobile Comput.*, vol. 11, no. 8, pp. 1386–1398, Aug. 2011.
[76] R. Miller and W. Trappe, "Subverting MIMO wireless systems by jamming the channel estimation procedure," in *Proc. 3rd ACM Conf. Wireless Netw. Security*, Mar. 2010, pp. 19–24.
[77] S. Sodagari and T. Clancy, "On singularity attacks in MIMO channels," *Wiley Trans. Emerging Telecommun. Technol.* May 2013, doi:10.1002/ett.2657, to be published.
[78] B. Muquet, Z. Wang, G. Giannakis, M. de Courville, and P. Duhamel, "Cyclic prefixing or zero padding for wireless multicarrier transmissions?" *IEEE Trans. Commun.*, vol. 50, no. 12, pp. 2136–2148, Dec. 2002.
[79] M. Nisar, W. Utschick, H. Nottensteiner, and T. Hindelang, "On channel estimation and equalization of OFDM systems with insufficient cyclic prefix," in *Proc. IEEE 65th VTC–Spring*, Apr. 2007, pp. 1445–1449.
[80] A. L. Scott, "Effects of cyclic prefix jamming versus noise jamming in OFDM signals," M.S. thesis, Air Force Inst. Tech Wright-Patterson AFB OH Graduate School Eng. Manage., Dayton, OH, USA, 2011.
[81] G. Philippe *et al.*, "LTE resistance to jamming capability: To which extend a standard LTE system is able to resist to intentional jammers," in *Proc. MCC Inf. Syst.*, Oct. 2013, pp. 1–4.
[82] T. Clancy, M. Norton, and M. Lichtman, "Security challenges with LTE-advanced systems and military spectrum," in *Proc. IEEE MILCOM Conf.*, Nov. 2013, pp. 375–381.
[83] S. Hasan and M. Qadeer, "Security concerns in WiMAX," in *Proc. 1st AH-ICI*, Nov. 2009, pp. 1–5.
[84] K. C. Beh, A. Doufexi, and S. Armour, "Performance evaluation of hybrid ARQ schemes of 3GPP LTE OFDMA system," in *Proc. IEEE 18th PIMRC*, Sep. pp. 1–5.
[85] S. Palat and P. Godin, "Network architecture," in *LTE, The UMTS Long Term Evolution: From Theory to Practice*, 2nd ed, S. Sesia, I. Toufik, and M. Baker, Eds. Chichester, U.K.: Wiley, 2011, ch. 2.
[86] M. Valenti and J. Sun, "The UMTS turbo code and an efficient decoder implementation suitable for software-defined radios," *Int. J. Wireless Inf. Netw.*, vol. 8, no. 4, pp. 203–215, Oct. 2001.
[87] 3rd Generation Partnership Project (3GPP). (2011). Physical Layer Procedures, Sophia-Antipolis, France, 3GPP Tech. Rep. 36.213. [Online]. Available: www.3gpp.org
[88] 3rd Generation Partnership Project (3GPP). (2011). Physical Channels and Modulation, Sophia-Antipolis, France, 3GPP Tech. Rep. 36.211. [Online]. Available: www.3gpp.org
[89] P. Bertrand and J. Jiang, "Random Access," in *LTE, The UMTS Long Term Evolution: From Theory to Practice*, S. Sesia, I. Toufik, and M. Baker, Eds., 2nd ed. Chichester, U.K.: Wiley, 2011, ch. 17.

Chowdhury Shahriar (S'01) was born in Dhaka, Bangladesh. He received the B.S. degree in electrical engineering from the Virginia Polytechnic Institute and State University (Virginia Tech), Blacksburg, VA, USA, in 2002 and the M.S. degree in electrical engineering from the Virginia Tech in 2006.

In 2007, he was with the US Patent & Trademark Office (USPTO), Alexandria, VA, USA. In 2013, he was a summer intern in the MIT Lincoln Lab, Lexington, MA, USA, where he was engaged in research on secure and jamming resistant MIMO communications. In 2014, he was a policy intern in the Cybersecurity and Communications Reliability Division, Federal Communications Commission (FCC), Washington, D.C., USA. He is currently a Ph.D. candidate in the Bradley Department of Electrical and Computer Engineering at the Virginia Tech and a Graduate Research Assistant in the Hume Center for National Security and Technology. His research interests are in the areas of wireless communications, communications security, signal processing, and spectrum management and policy.

Mr. Shahriar is a recipient of the National Science Foundation (NSF) summer research fellowship for the undergraduates (RUE) in 1999.

Matt La Pan (S'13) received the B.S. degree in electrical engineering from the University of Miami, Coral Gables, FL, USA, in 2010 and the M.S. degree in electrical engineering from the Virginia Polytechnic Institute and State University (Virginia Tech), Blacksburg, VA, USA, in 2012.

He is currently a Ph.D. candidate at Virginia Tech in the Bradley Department of Electrical and Computer Engineering. Additionally he is a Graduate Research Assistant of the Hume Center for National Security and Technology. His research is in the field of wireless communication with a focus on electronic warfare and wireless security for modern systems.

Marc Lichtman (S'09) received the B.S. degree in electrical engineering from the Virginia Polytechnic Institute and State University (Virginia Tech), Blacksburg, VA, USA, in 2011 and the M.S. degree in electrical engineering from the Virginia Tech, in 2012.

He is currently working toward the Ph.D. degree in the Bradley Department of Electrical and Computer Engineering at Virginia Tech and a Graduate Research Assistant in the Wireless@Virginia Tech. His research is focused on designing anti-jam approaches against sophisticated jammers, using machine learning techniques. He is also interested in analyzing the vulnerability of LTE to jamming.

Mr. Lichtman is the winner of the LabVIEW invitational programming contest, and his research has been featured in an MIT Technology Review article.

T. Charles Clancy (S'02–M'06–SM'10) received the B.S. degree in computer engineering from the Rose-Hulman Institute of Technology, Terre Haute, IN, USA, in 2001, the M.S. degree in electrical engineering from the University of Illinois, Urbana-Champaign, IL, USA, in 2002, and the Ph.D. degree in computer science from the University of Maryland, College Park, MD, USA, in 2006.

He is an Associate Professor in the Bradley Department of Electrical and Computer Engineering at the Virginia Polytechnic Institute and State University (Virginia Tech), Blacksburg, VA, USA. Additionally he is Director of the Hume Center for National Security and Technology, the L-3 Communications Faculty Fellow in Cybersecurity of the College of Engineering, and Co-Director of the NSF Security and Software Engineering Research Center. His research interests are focused in wireless security, spectrum management, and electronic warfare.

Dr. Clancy currently serves as Associate Editor for *IEEE Transactions on Information Forensics and Security*. He is co-founder of a number of companies, including Optio Labs, Federated Wireless, and Stochastic Research. He is author to over 100 peer-reviewed publications.

Robert McGwier (SM'12) received the B.S. degree in mathematics and electrical engineering from the Auburn University, Auburn, AL, USA, in 1978, and the Ph.D. degree in applied mathematics from Brown University, Providence, RI, USA, in 1984.

He is the Director of Research of the Hume Center for National Security and Technology, and Research Professor in the Bradley Department of Electrical and Computer Engineering at Virginia Polytechnic Institute and State University (Virginia Tech). He leads the overall execution of the Center's research mission and lead's the university's program development efforts in national security applications of wireless and space systems. Before joining Virginia Tech, he spent 26 years as a member of the technical staff at the Institute for Defense Analyses' Center for Communications Research in Princeton, NJ, USA, where he worked on advanced research topics in mathematics and communications supporting the federal government. His area of expertise is in radio frequency communications and digital signal processing.

Dr. McGwier's work on behalf of the government has earned him many awards, including one of the intelligence community's highest honors in 2002.

Ravi Tandon (S'03–M'09) received the B.Tech. degree in electrical engineering from the Indian Institute of Technology, Kanpur (IIT Kanpur) in May 2004. He received the Ph.D. degree in electrical and computer engineering from the University of Maryland, College Park (UMCP) in June 2010. From July 2010 through July 2012, he was a post-doctoral Research Associate at Princeton University. Since July 2012, he has been a Research Assistant Professor in the Hume Center for National Security and Technology and the Bradley Department of Electrical and Computer Engineering at Virginia Polytechnic Institute and State University. His research interests are in the areas of information theory, communication theory for wireless networks, cloud storage systems and information theoretic security. Dr. Tandon is a recipient of the Best Paper Award at the Communication Theory symposium at the 2011 IEEE Global Communications Conference.

Shabnam Sodagari (SM'12) received the Ph.D. degree in electrical engineering from the Pennsylvania State University. Among her research interests are topics related to secure wireless communications and coexistence of radar and communication systems. She is with the University of Maryland, College Park, MD, USA.

Jeffrey H. Reed (F'05) received the B.S.E.E. degree in 1979, the M.S.E.E. degree in 1980, and the Ph.D. degree in 1987, all from the University of California, Davis, CA, USA.

Currently he is the Willis G. Worcester Professor in the Bradley Department of Electrical and Computer Engineering at Virginia Polytechnic Institute and State University, Blacksburg, VA, USA, and founding Director of the Wireless@VT, the umbrella wireless organization, which is one of the largest and most comprehensive university wireless research groups in the USA. He has authored, co-authored, or co-edited ten books and proceedings, contributed to six books, and authored or co-authored over two hundred journal and conference papers. His textbook, *Software Radios: A Modern Approach to Radio Design* is one of the first books devoted exclusively to software radios. He is co-founder of multiple companies, including Cognitive Radio Technologies, Power Fingerprinting, and Federated Wireless.

Dr. Reed became Fellow to the IEEE for contributions to software radio and communications signal processing and for leadership in engineering education, in 2005. He is also a Distinguished Lecturer for the IEEE Vehicular Technology Society. In 2013, he was awarded the International Achievement Award by the Wireless Innovations Forum. In 2012, he served on the Presidents Council of Advisors of Science and Technology Working Group that examines ways to transition federal spectrum to allow commercial use and improve economic activity.