WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
Wirel. Commun. Mob. Comput. 2016; **16**:177–191
Published online 18 August 2014 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/wcm.2500

RESEARCH ARTICLE

Physical layer orthogonal frequency-division multiplexing acquisition and timing synchronization security[†]

Matthew J. La Pan*, T. Charles Clancy and Robert W. McGwier

Hume Center, Virginia Tech, 900 N Glebe Road, Arlington, VA 22203, U.S.A.

ABSTRACT

Orthogonal frequency-division multiplexing (OFDM) has become the manifest modulation choice for 4G standards. Timing acquisition and carrier frequency offset synchronization are prerequisite to OFDM demodulation and must be performed often. Most of the OFDM methods for synchronization were not designed with security in mind. In particular, we analyze the performance of a maximum likelihood synchronization estimator against highly correlated jamming attacks. We present a series of attacks against OFDM timing acquisition: preamble whitening, the false preamble attack, preamble warping, and preamble nulling.The performance of OFDM synchronization turns out to be very poor against these attacks, and a number of mitigation strategies and security improvements are discussed. Copyright © 2014 John Wiley & Sons, Ltd.

KEYWORDS
OFDM; synchronization; security

***Correspondence**
Matthew J. La Pan, Hume Center, Virginia Tech, 900 N Glebe Road, Arlington, VA 22203, U.S.A.

E-mail: mlapan4@vt.edu

[†] Portions of this paper were published in the IEEE Military Communications Conference (MILCOM), October 2012 and others were published in the 16th international IEEE Wireless Personal Media Communications (WPMC) Conference, June 2013.

1. INTRODUCTION

Orthogonal frequency-division multiplexing (OFDM) has become prevalent in wireless communications, particularly fourth generation (4G) standards [1,2]. This choice of modulation has many advantages including spectral efficiency, flexibility, and low computational complexity. However, the 4G standards such as Long-Term Evolution (LTE) and Worldwide Interoperability for Microwave Access (WiMAX) that have been developed with OFDM as the modulation of choice have notable gaps in security in a tactical scenario, which has left the OFDM waveforms vulnerable to external jamming attacks [3]. These attacks are not typical of a commercial communication setting—which explains the lack of focus on these scenarios when designing standards—but the impact that they could have on a system using OFDM must be considered.

As in any coherent wireless system, there are clock errors between the transmitter and receiver that must be rectified through synchronization. For systems that use OFDM, it is not only important to perform synchronization but it is also prerequisite to demodulation. Without this process, OFDM systems are susceptible to intersymbol interference, intercarrier interference, and loss of orthogonality among OFDM subcarriers. There are a number of algorithms that have been developed for performing this task [4–10]. The work performed in this paper is based on the three part, maximum likelihood algorithm designed by Schmidl and Cox [11]. The three parts of this algorithm are as follows: timing acquisition, fine frequency error estimation and correction, and coarse frequency error estimation and correction. Because of its optimality, this synchronization is used in most OFDM systems and is actually part of the WiMAX standard. While we only focus on one algorithm for the sake of analysis, it is critical to note that almost all of the previously aforementioned synchronization methods require similar training data and use correlation-based estimators. The security risks highlighted in this work apply to a majority of the algorithms for OFDM synchronization used in practice.

1.1. Orthogonal frequency-division multiplexing interference and jamming in literature

There has been a significant amount of research performed in the area of OFDM interference and to a lesser extent OFDM security. As previously mentioned, [3]—along with [12,13]—all highlight security flaws inherent to OFDM systems. A good deal of work has been performed on analyzing and mitigating the impact that interference has on OFDM acquisition [14–18]. However, almost all of the work performed either assumes narrowband interference or does not consider the impact of specifically targeted waveforms that are correlated to the OFDM synchronization itself.

We aim to analyze the performance of OFDM synchronization in the presence of targeted jamming attacks that are highly correlated to the acquisition waveforms. Specifically, we would like to determine the impact of an external jammer on an OFDM receivers ability to recover a useful symbol timing estimate. This work is unique in that it considers an ill-intentioned attacker versus environmental and incidental interference from sources such as additive white Gaussian noise (AWGN), multipath interference, and co-channel interference. In addition, this work implies the impact that a malicious adversaries knowledge of an OFDM system can have. Finally, the work presented here underlines the critical need for advanced OFDM security measures in wireless systems that could be vulnerable to the targeted jamming attacks, such as cellular networks using modern standards such as LTE or WiMAX, along with both public and private wireless access networks using technologies such as Wi-Fi.

This paper is organized as follows. Section 2 discusses relevant research in this area and the importance of this work. Section 3 describes the synchronization model used to investigate this problem. Section 4 presents the model for a hypothesized attack on an OFDM system, while Section 5 presents the specific attacks studied in this work. Section 6 provides simulation results and some discussion on the impact of these attacks on synchronization performance. Section 7 outlines some proposed attack mitigation strategies of interest for future work, with conclusions and acknowledgements are made in the remaining sections.

2. SYNCHRONIZATION MODEL AND ANALYSIS

In order to analyze the synchronization performance of an OFDM system, we used a mathematical model with several assumptions about the system. First, we assume that the system is subject to AWGN because of thermal noise, radiation, and other sources. We also assume that the system of interest is subject to multipath fading because of obstructing objects that are often present in cellular communications systems. Because cellular standards are generally public knowledge, we assume that an attacker has access to the standard itself and subsequent algorithms and symbols used for synchronization, although we have included reference cases for jammers without this knowledge.

Notations. All time domain signals and impulse responses are denoted by lower case letters, while computed values, metrics, and parameters are denoted by upper case or Greek letters. Time indices for signals are denoted by subscripts. The $(\cdot)^*$ notation represents complex conjugation, while $|\cdot|$ represents magnitude of a complex number $a + jb$ defined as $\sqrt{a^2 + b^2}$. Let $R_{x(d)x(d)}(l)$ denote the autocorrelation function of a signal x_d at lag l.

2.1. Synchronization model

As previously noted, the WiMAX synchronization algorithm from [11] has three parts—symbol timing estimation, fine carrier frequency offset estimation and correction, and coarse carrier frequency offset estimation. This synchronization method, like many others, is based on the use of OFDM training symbols called *preamble* symbols. There are two preamble symbols, and they have a specific structure that is covered in detail in [11]. Figure 1 depicts the structure of the first preamble symbol, which is the only one used for timing acquisition. The symbol has a time repetitive structure that allows the receiver to use delay line correlation in order to perform timing synchronization.

The receiver starts by using the first preamble symbol to compute a timing metric after the receiver obtains the complex baseband samples via radio-frequency down conversion. The metric is computed with a sliding window of length L samples, where L is half the length of the OFDM symbol without the cyclic prefix. Two terms are computed from the window; the first according to the following:

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

and the second according to the following:

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

where d is the time index that corresponds to the first sample taken in the window and r is the length-L vector of received symbols. The timing metric $M(d)$ is computed according to the following:

$$M(d) = \frac{|P(d)|^2}{R(d)^2} \tag{3}$$

The metric generates a plateau, shown in Figure 2 where the maximum values begin at $d = \hat{d}$, with the point $\hat{d}$ being at the beginning of the preamble, and end when $d = \hat{d} + (T_{cp} - T_{ch})f_s$, where T_{cp} is the period of the cyclic prefix and T_{ch} is the length of the channel impulse response, corresponding to its delay spread. Any estimate taken along the plateau is a valid symbol timing point. This plateau will be the length of the cyclic prefix minus the

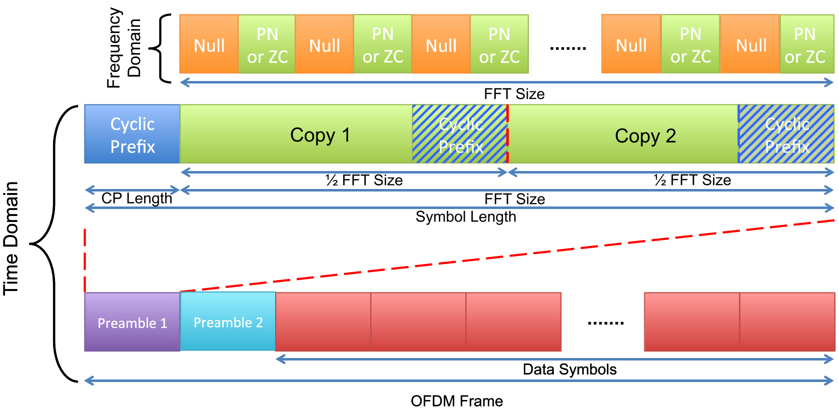


Figure 1. Structure of the timing preamble symbol within the orthogonal frequency-division multiplexing (OFDM) frame structure. The symbol occupies every other subcarrier of the fast Fourier transform (FFT) size in the frequency domain with a pseudo-noise (PN), Zadoff–Chu (ZC), or other known sequence. This leads to two identical half symbol copies being created in the time domain. The cyclic prefix is appended in the time domain at the beginning of the preamble and at the end of each half symbol copy.

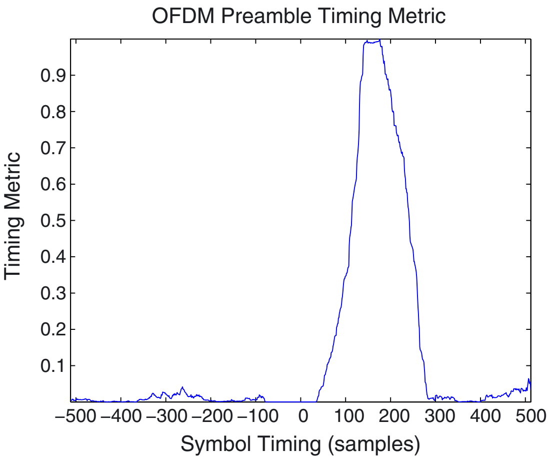


Figure 2. Plot showing the timing metric $M(d)$ computed from the first preamble symbol. In this case, the search range is a window that is three symbols long. Any point taken along the plateau of the metric will yield a correct timing estimate.

length of the channel impulse response. The receiver then uses the timing point as a reference for sampling all of the symbols within a frame and stripping the cyclic prefix. The receiver then moves on to fine and coarse frequency estimation, but the validity of both estimates depends on successful timing recovery (Figure 3).

2.2. Synchronization model analysis

After baseband conversion and resampling, the OFDM will have a series of complex samples that compose the search range for the preamble symbol. These samples will be randomly shifted in frequency subject to the clock error between the transmitter and receiver, limited to the allowable range of offset between these two devices. We make the assumption that the offset is approximately constant over the duration of the training sequence. The sequence at the receiver is represented by the following:

$$r_n = \left(\sum_{k=0}^{C-1} x_{n-k} h_k\right) e^{\left(2\pi j \frac{f}{f_s} n\right)} + n_n \qquad (4)$$

where x is the samples of the training symbol sent, h represents the impulse response of the channel with length C, f represents the frequency offset between the transmitter and receiver clocks, and the term n represents noise. Substituting this term into (1) yields the following:

$$P(d) = \sum_{m=0}^{L-1} \left(\sum_{k=0}^{C-1} x^*_{d+m-k} h^*_k e^{\left(-2\pi j \frac{f}{f_s}(d+m)\right)} + n^*_{(d+m)}\right) \left(\sum_{k=0}^{C-1} x_{d+m+L-k} h_k e^{\left(2\pi j \frac{f}{f_s}(d+m+L)\right)} + n_{d+m+L}\right) \qquad (5)$$

By expanding the terms in the numerator, we see the following:

$$\begin{aligned} P(d) = \sum_{m=0}^{L-1} \Bigg[& \left(\sum_{k=0}^{C-1} x^*_{d+m-k} h^*_k\right) \left(\sum_{k=0}^{C-1} x_{d+m+L-k} h_k\right) e^{\left(2\pi j \frac{f}{f_s} L\right)} \\ & + \sum_{k=0}^{C-1} x^*_{d+m-k} h^*_k e^{\left(-2\pi j \frac{f}{f_s}(d+m)\right)} n_{d+m+L} \\ & + \sum_{k=0}^{C-1} x_{d+m+L-k} h_k e^{\left(2\pi j \frac{f}{f_s}(d+m+L)\right)} n^*_{d+m} \\ & + n^*_{d+m} n_{d+m+L} \Bigg] \end{aligned} \qquad (6)$$

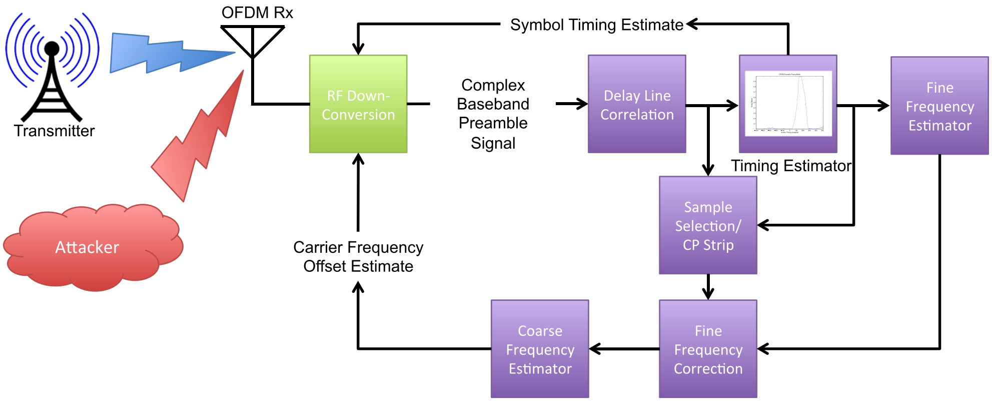

OFDM Rx
Transmitter
Attacker
RF Down-Conversion
Complex Baseband Preamble Signal
Symbol Timing Estimate
Delay Line Correlation
Timing Estimator
Fine Frequency Estimator
Sample Selection/ CP Strip
Fine Frequency Correction
Coarse Frequency Estimator
Carrier Frequency Offset Estimate

Figure 3. Block diagram depicting the system under consideration. An orthogonal frequency-division multiplexing (OFDM) receiver uses the synchronization algorithm (purple blocks) in order to correct timing and carrier frequency offsets between itself and the transmitter. The attacker shown in red attempts to destroy the timing acquisition of the receiver by inducing an error in the symbol timing estimate.

Looking at the timing plateau where $\hat{d} \leq d \leq \hat{d} + (T_{cp} - T_{ch})f_s$, we can simplify the first term in this expression on the basis of the fact that the first preamble symbol is repeated over two half symbol periods, excluding the prefix, as indicated in [11]. This means that values spaced L samples apart are identical, meaning that the first term in (6) can be simplified to the following:

$$\begin{aligned}&\sum_{m=0}^{L-1}\left(\sum_{k=0}^{C-1} x^*_{d+m-k}h^*_k\right)\left(\sum_{k=0}^{C-1} x_{d+m+L-k}h_k\right)e^{\left(2\pi j\frac{f}{f_s}L\right)}\\ &= \sum_{m=0}^{L-1}\left|\sum_{k=0}^{C-1} x_{d+m-k}h_k\right|^2 e^{\left(2\pi j\frac{f}{f_s}L\right)} \qquad (7)\end{aligned}$$

We define the term as follows:

$$\begin{aligned}\epsilon = \sum_{m=0}^{L-1}\Bigg[&\sum_{k=0}^{C-1} x^*_{d+m-k}h^*_k e^{\left(-2\pi j\frac{f}{f_s}(d+m)\right)} n_{d+m+L}\\ &+ \sum_{k=0}^{C-1} x_{d+m+L-k}h_k e^{\left(2\pi j\frac{f}{f_s}(d+m+L)\right)} n^*_{d+m}\\ &+ n^*_{d+m}n_{d+m+L}\Bigg] \qquad (8)\end{aligned}$$

We can also use (4) to determine the what the receiver will estimate for $R(d)$ on the basis of (2). Examining this result along the same plateau where $\hat{d} \leq d \leq \hat{d} + (T_{cp} - T_{ch})f_s$:

$$R(d) = \sum_{m=0}^{L-1}\left(\left|\sum_{k=0}^{C-1} x_{d+m-k}h_k + n_{d+m}\right|\right)^2 \qquad (9)$$

Applying the triangle inequality for complex numbers, this becomes the following:

$$R(d) \leq \sum_{m=0}^{L-1}\left(\left|\sum_{k=0}^{C-1} x_{d+m-k}h_k\right| + |n_{d+m}|\right)^2 \qquad (10)$$

Combining this result with (3), (7) and (8) gives us the following:

$$M(d) \geq \frac{\left|\sum_{m=0}^{L-1}\left|\sum_{k=0}^{C-1} x_{d+m-k}h_k\right|^2 + \epsilon\right|^2}{\left(\sum_{m=0}^{L-1}\left(\left|\sum_{k=0}^{C-1} x_{d+m-k}h_k\right| + |n_{d+m}|\right)^2\right)^2} \qquad (11)$$

We subsequently define the following:

$$\sigma^2_{xc} = \sum_{m=0}^{L-1}\left|\sum_{k=0}^{C-1} x_{d+m-k}h_k\right|^2 \qquad (12)$$

as the total power of the entire channel-affected OFDM symbol and

$$\sigma^2_n = \sum_{m=0}^{L-1} |n_{d+m}|^2 \qquad (13)$$

as the total noise power over one OFDM symbol period. We then utilize the following fact:

$$2\sum_{m=0}^{L-1}\left|\sum_{k=0}^{C-1}x_{d+m-k}h_k\right||n_{d+m}|\leq 2\sigma_{xc}\sigma_n \tag{14}$$

with the relationship in (11) to obtain the following:

$$M(d)\geq\frac{\left|\sigma_{xc}^2+\epsilon\right|^2}{\left(\sigma_{xc}^2+2\sigma_{xc}\sigma_n+\sigma_n^2\right)^2} \tag{15}$$

By taking the minimum possible value of ϵ, we obtain the following lower bound:

$$M(d)\geq\frac{\left(\sigma_{xc}^2-\epsilon\right)^2}{\left(\sigma_{xc}^2+2\sigma_{xc}\sigma_n+\sigma_n^2\right)^2} \tag{16}$$

Rearranging terms and defining

$$SNR=\frac{\sigma_{xc}^2}{\sigma_n^2} \tag{17}$$

produces the following result:

$$M(d)\geq\frac{\left(1-\frac{\epsilon}{\sigma_{xc}^2}\right)^2}{\left(1+\frac{1}{\sqrt{SNR}}\right)^4} \tag{18}$$

We can then use the central limit theorem to approximate the terms of ϵ as Gaussian random variables. Using the independence of the terms and the fact that they are all zero mean, we can say that

$$\epsilon\sim N\left(0,\frac{2\sigma_{xc}\sigma_n+\sigma_n^2}{L^2}\right) \tag{19}$$

The impact of this term will have a much smaller impact on the timing metric compared with the noise degradation in the denominator, as it has an expected value of zero and it's variance asymptotically approaches zero as L—half of the number of subcarriers used—increases. Additionally, this term can add to the timing metric plateau depending on the phase of ϵ. The lower bound of the timing metric, shown in Figure 4, gives an idea of the strength of the timing peak relative to the signal-to-noise ratio (SNR).

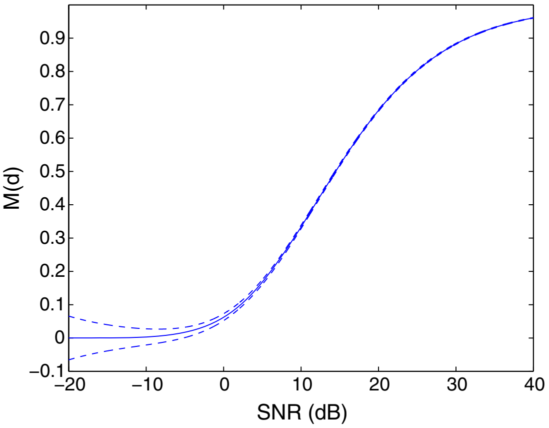


Figure 4. Lower bound on the peak value of the timing metric plateau relative to the signal-to-noise ratio (SNR). The solid line shows for when ϵ is at its expected value of zero, while the dotted lines show three standards deviations of ϵ in either direction for a system where $L = 500$. The plot shows that the ϵ term has a negligible impact on the lower bound above 0 dB SNR (the timing metric cannot be negative).

3. ADVERSARIAL INTERFERENCE

We have developed a model to describe the scenario of an OFDM system being attacked at the synchronization stage by an adversarial communications system. The model incorporates both the signal from the transmitter and the signal from the jammer into the signal at the receiver. The transmitter and the jammer broadcast signals x and j, which then pass through two unique multipath channels h and k, respectively. The multipath profiles h and k are approximated as finite impulse response (FIR) digital filters. An AWGN signal is also incurred at the receiver, denoted by n_n. The received signal is made up of the channel-affected transmitter and jammer signal plus noise. In this case, the received vector r is as follows:

$$r_n=\left(\sum_{k=0}^{C-1}x_{n-k}h_k\right)e^{\left(2\pi j\frac{f}{f_s}n\right)}+\alpha\left(\sum_{i=0}^{K-1}j_{n-i}k_i\right)e^{\left(2\pi j\frac{f_j}{f_s}n\right)}+n_n \tag{20}$$

where h_k and k_i are the impulse responses of the channel that the receiver and the jammer sees, respectively, of lengths C and K. The values f and f_j represent the relative frequency offsets of the receiver with the transmitter and the jammer, and n_n is a vector of WGN.

For the experiments and analysis in this work, we consider the transmitter power to be fixed, while varying the jammer power around it. This creates the following signal-to-jammer ration (SJR) power metric:

$$SJR = 10\log(\alpha^2) = 20\log(\alpha) \tag{21}$$

which is used to determine the power efficiency of the attacks presented in this paper.

It is important to classify some of the assumptions made in this work. As in a real system, it is assumed that there are clock differences between the transmitter, receiver, and the jammer. In order to implement and execute power-efficient jamming attacks, it is assumed that the jammer is aware of the synchronization algorithm and the corresponding preamble structure[†]. These assumptions are fundamental to all of the attacks presented in this work. The only exception is the continuous white noise jamming attack, which serves as a reference for power efficiency.

This work is focused on the impact that a hostile communication system can have on an OFDM timing metric, specifically the one used in WiMAX. We can use the estimators that make up the timing estimation to derive some analytical results for performance in the presence of attackers. Replacing the sum of the jammer and transmitter signals into (1) yields the following:

$$\begin{aligned} P(d) = \sum_{m=0}^{L-1} \Bigg[& \left(\sum_{k=0}^{C-1} x^*_{d+m-k} h^*_k\right) e^{-2\pi j \frac{f}{f_s}(d+m)} \\ & + \alpha \left(\sum_{i=0}^{K-1} j^*_{d+m-i} k^*_i\right) e^{-2\pi j \frac{f_j}{f_s}(d+m)} \Bigg] \\ \Bigg[& \left(\sum_{k=0}^{C-1} x_{d+m+L-k} h_k\right) e^{2\pi j \frac{f}{f_s}(d+m+L)} \\ & + \alpha \left(\sum_{i=0}^{K-1} j_{d+m+L-i} k_i\right) e^{-2\pi j \frac{f_j}{f_s}(d+m+L)} \Bigg] \end{aligned} \tag{22}$$

Expanding this result produces the equation that will be the starting point for deriving most of the attack-based performance metrics:

$$\begin{aligned} P(d) = \sum_{m=0}^{L-1} \Bigg[& \left(\sum_{k=0}^{C-1} x^*_{d+m-k} h^*_k\right) \left(\sum_{k=0}^{C-1} x_{d+m+L-k} h_k\right) e^{2\pi j \frac{f}{f_s} L} \\ & + \alpha \left(\sum_{k=0}^{C-1} x^*_{d+m-k} h^*_k\right) \left(\sum_{i=0}^{K-1} j_{d+m+L-i} k_i\right) e^{2\pi j \frac{f_j - f}{f_s}(d+m)} e^{2\pi j \frac{f_j}{f_s} L} \\ & + \alpha \left(\sum_{i=0}^{K-1} j^*_{d+m-i} k^*_i\right) \left(\sum_{k=0}^{C-1} x_{d+m+L-k} h_k\right) e^{2\pi j \frac{f - f_j}{f_s}(d+m)} e^{2\pi j \frac{f}{f_s} L} \\ & + \alpha^2 \left(\sum_{i=0}^{K-1} j^*_{d+m-i} k^*_i\right) \left(\sum_{i=0}^{K-1} j_{d+m+L-i} k_i\right) e^{2\pi j \frac{f_j}{f_s} L} \Bigg] \end{aligned} \tag{23}$$

The noise terms are neglected in these derivations in the interest of specifically analyzing the impact that the jammer has on the OFDM synchronization process at power levels well above the noise floor.

In addition, we define the scenarios in which the jammer has channel knowledge. In this case, the jamming signal $\hat{j}_n$ is defined as follows:

$$\hat{j}_n = \alpha \left(\sum_{l=0}^{K-1} p_{n-l} k_l^{-1}\right) e^{\left(2\pi j \frac{f_j}{f_s} n\right)} \tag{24}$$

where

$$p_n = \left(\sum_{i=0}^{C-1} j_{n-i} h_i\right) \tag{25}$$

where j_n is the jamming signal dependent on the attack, k^{-1} is the inverse jammer channel response such that $k^{-1} = \mathrm{FFT}^{-1}(1/\mathrm{FFT}(k))$, and $|\alpha| > 0$. In addition, f_j represents the frequency offset of the jamming signal at the receiver, which in most cases will be made to match the offset of the preamble at the receiver.

4. POWER-EFFICIENT JAMMING ATTACKS

The maximum likelihood synchronization algorithm provided by Schmidl and Cox is robust to environmental effects such as AWGN and multipath. However, it was not designed for the scenario where the synchronization stage for OFDM is sought out and attacked using power-efficient jamming signals. One of the main oversights in the design is the high level of visibility of the sync process itself. The control symbols used by this algorithm distinctly stand out among data bearing OFDM symbols, in particular the time repetitive first preamble symbol for this algorithm. In addition, these symbols are almost always at a fixed position within frame structure of OFDM transmission. The problems of synchronization visibility and symbol periodicity are inherent to various other algorithms [4–9], as well as various standards, including WiMAX and LTE. The two simplest attacks presented in this paper highlight the danger that these problems present.

4.1. Barrage jamming attacks

There are two types of basic jamming attacks that perform barrage attacks. Although they are not explicitly covered in this paper, they are important to mention as the most basic attacks against OFDM. The first is a continuous white noise jammer that aims to raise the noise floor at the receiver in order to degrade communication. This is the most inefficient and least intelligent jammer and can serve as a baseline for comparing the efficiencies of

[†] This information is public knowledge for any known signal standard.

other jammers. The second type of barrage attack, preamble whitening, is slightly more efficient and intelligent, although it still relies on uncorrelated noise in order to disrupt communications. This jammer raises the noise floor only during the synchronization phase, effectively trying to drown out the preamble symbols in order to jam the receiver.

4.1.1. Continuous white noise jamming.

The continuous white noise jamming attack is carried out when a jammer transmits AWGN across the bandwidth of an OFDM signal. It is important to consider this type of attack for a scenario where the jammer has no knowledge of the synchronization algorithm. This attack serves as the reference point for having the lowest power efficiency of any attacks in this paper. This jammer's impact is not best determined via (23) because the noise will impact demodulation before it begins to interfere with the synchronization process. The power requirement for this attack is based on the effective SNR of the OFDM symbol at the receiver and the baseband digital modulation used on the subcarriers. In order to deny service to an OFDM system, the jammer would have to induce the well-known *Shannon ultimate limit* for minimum possible energy per bit to noise power spectral density (PSD) ratio, or E_b/N_o, of -1.59 dB. This means that the required power can be derived from the following:

$$-1.59\,\mathrm{dB} \geq 10\log\left(\frac{E_b}{P_{cw}+N_o}\right) \tag{26}$$

where P_{cw} is the constant PSD of the continuous jammer, E_b is the energy per transmitted BPSK bit and N_o is the constant noise PSD. Rearranging terms in this equation, we see the following:

$$P_{cw} \geq \frac{E_b}{\ln(2)} - N_o \tag{27}$$

with the conditions that

$$P_{cw}, E_b, N_o \geq 0 \tag{28}$$

These results are the baseline for the brute force continuous white noise jammer.

4.1.2. Preamble whitening.

The preamble whitening attack is very similar to the continuous white noise jamming attack. The key difference is that preamble whitening is not a continuous attack. Instead the jammer identifies OFDM synchronization—which, as previously mentioned, is aided by the stationary and visible nature of training symbols within OFDM frame structure—and then only attacks the system during this process. The efficiency gain of this attack is based on the original SNR at the receiver and the number of symbols in each frame. The only sophistication that this attack requires is the ability to identify the time location and period of the synchronization process.

This attack does improve temporal efficiency, but the power requirement of the attack is still significant, as shown in Figure 5. The timing estimate is not adversely affected by AWGN until the SNR drops less than -10 dB. As an alternative, efficient jammers can offer superior performance degradation to OFDM signals at much lower jammer powers by exploiting the inherent features of OFDM.

These barrage attacks can still provide a useful baseline for jammer efficiency. In a scenario where an OFDM transmitter and receiver synchronize once every n symbols, preamble whitening will offer a savings of the following:

$$P_{sav}dB = 10\log\left(n\frac{P_{cw}}{P_{pw}}\right)\,\mathrm{dB} \tag{29}$$

in total transmit power compared with what a continuous white noise jammer would require. P_{cw} is defined as the average transmit power of the continuous white noise barrage jammer, and P_{pw} is the average transmit power of the preamble whitening jammer. Assuming that there is some required degradation to the preamble E_b/N_o, D_{req} in dB, we can say the following:

$$D_{req} \geq 10\log\left(\frac{E_b}{P_{pw}+N_o}\right) \tag{30}$$

or

$$P_{pw} \geq \frac{E_b}{10^{.1D_{req}}} - N_o \tag{31}$$

where

$$P_{pw} \geq 0. \tag{32}$$

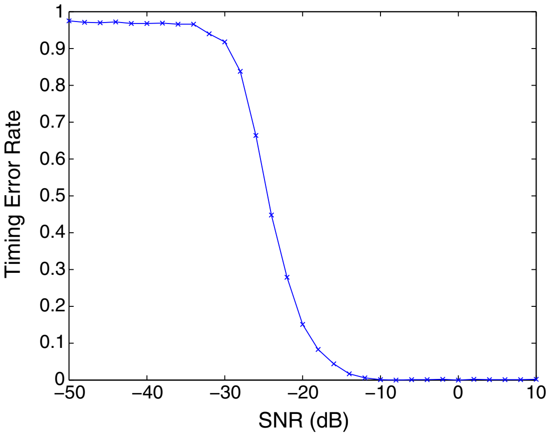


Figure 5. Timing estimate error as a function of the effective signal-to-noise ratio (SNR) at the receiver.

By substituting (27) and (31) into (29), we see the following:

$$P_{sav}dB = 10\log\left(n\frac{E_b/\ln(2) - N_o}{E_b/10^{.1D_{req}} - N_o}\right) \tag{33}$$

Because in most cases of interest $E_b >> N_o$ (or else jamming the signal would be much more trivial), we can make the following approximation:

$$P_{sav}dB \approx 10\log\left(\frac{n \cdot 10^{.1D_{req}}}{\ln(2)}\right) \tag{34}$$

Looking at Figure 5, for a required degradation of −30 dB, the value of n would have to be larger that 693 for the preamble whitening attack to have a power savings advantage. However, for a required degradation of −20 dB, the value of n only has to be larger than 69. So the overall power savings of the preamble whitening attack versus the continuous white noise attack is dependent on the frame structure of the system being attacked. However, it is also important to note the cost of the preamble whitener being able to sense and/or predict when the transmitter and receiver are attempting to perform synchronization.

4.2. False preamble timing attack

The idea behind corrupting OFDM timing acquisition is to either move the peak of the metric or to destroy it entirely. The false preamble timing attack attempts to move the peak of the timing metric by creating a new preamble. Depending on the system knowledge of the jammer, this can either be an exact copy of the original preamble or a different preamble symbol altogether.

This attack can be analyzed through (23). As previously mentioned, the false preamble attack signal can be either a time-delayed exact copy of the actual preamble or, more generally, a preamble constructed from a random sequence. The only requirement is that preamble generated by the attacker follows the format of the preambles used by the sync algorithm. For this general case, the resulting timing metric numerator that the receiver sees will take the following form:

$$\begin{aligned} P(d) = \sum_{m=0}^{L-1} \Bigg[& \left|\sum_{k=0}^{C-1} x_{d+m-k}h_k\right|^2 \\ & + \alpha\left(\sum_{k=0}^{C-1} x^*_{d+m-k}h^*_k\right)\left(\sum_{i=0}^{K-1} j_{d+m-i}k_i\right) \\ & + \alpha\left(\sum_{i=0}^{K-1} j^*_{d+m-i}k^*_i\right)\left(\sum_{k=0}^{C-1} x_{d+m-k}h_k\right) \\ & + \alpha^2\left|\sum_{i=0}^{K-1} j_{d+m-i}k_i\right|^2\Bigg]^2 \end{aligned} \tag{35}$$

From this point, there are two main cases: when the two preambles overlap and when they do not. We assume that the jamming symbol is sent so that there is significant separation between its timing metric plateau and the preamble's, specifically such that $\{N \in \mathbb{R} \mid |N| > T_{cp}f_s\}$ where N is the delay of the false preamble relative to the correct one. This is the optimal strategy for the jammer to make the receiver miss the timing point.

The first case is based around when $|N| > T_{sym}f_s$, and there is no overlap between the timing preamble symbols. This will simplify (35) to the following:

$$P(d) = \sum_{m=0}^{L-1}\left|\sum_{k=0}^{C-1} x_{d+m-k}h_k\right|^4 + \alpha^4\left|\sum_{i=0}^{K-1} j_{d+m-i}k_i\right|^4 \tag{36}$$

From here, we incorporate the lower bound from (18) and split the two plateaus to show the following:

$$M(d) > \begin{cases} \frac{1}{\left(1+\frac{1}{SNR}\right)^2} & : d \in \hat{D} \\ \frac{1}{\left(1+\frac{1}{\alpha^2 JNR}\right)^2} & : d \in \hat{D} - N \end{cases} \tag{37}$$

where $\hat{D}$ represents the range of the timing metric plateau for the preamble, $\hat{D} - N$ represents that range shifted by the delay N of the false preamble, and JNR represents the jammer-to-noise ratio determined by the symbol and jammer channel but independent of α.

The second case is when $T_{cp}f_s < |N| < T_{sym}f_s$ such that the two preambles overlap. In this case, the two cross terms are a factor. However, the terms represent single points in the cross-correlation between the two preambles. If the jammer has no channel information and the symbols are independent, then they approximate to zero either way. However, the case where the jammer has channel knowledge and sends the same symbol as the transmitter requires further analysis. In this case, the numerator of the timing metric becomes the following:

$$\begin{aligned} P(d) = \sum_{m=0}^{L-1} \Bigg[& \left|\sum_{k=0}^{C-1} x_{d+m-k}h_k\right|^2 \\ & + \alpha\left(\sum_{k=0}^{C-1} x^*_{d+m-k}h^*_k\right)\left(\sum_{k=0}^{C-1} x_{d-N+m-k}h_k\right) \\ & + \alpha\left(\sum_{k=0}^{C-1} x^*_{d-N+m-k}h^*_k\right)\left(\sum_{k=0}^{C-1} x_{d+m-k}h_k\right) \\ & + \alpha^2\left|\sum_{k=0}^{C-1} x_{d-N+m-k}h_k\right|^2\Bigg]^2 \end{aligned} \tag{38}$$

In order to analyze this equation, we define $R_{y(d)y(d)}(l)$ as the autocorrelation function:

$$R_{y(d)y(d)}(l) = \sum_{m=0}^{L-1} y_{d+m} y^*_{d+m-l} \tag{39}$$

where $y(d)$ represents the signal of interest and l is the lag between the two signals. If we define

$$y_{d+m} = \sum_{k=0}^{C-1} x_{d+m-k} h_k \tag{40}$$

then (38) becomes the following:

$$\begin{aligned} P(d) &= R_{y(d)y(d)}(0) + \alpha R_{y(d-N)y(d-N)}(-N) \\ &\quad + \alpha R_{y(d)y(d)}(N) + \alpha^2 R_{y(d-N)y(d-N)}(0) \end{aligned} \tag{41}$$

In order to accurately compute these terms, knowledge about the autocorrelation function of both the OFDM signal and the channel are necessary, as suggested in [19]. The autocorrelation of the OFDM symbol can be derived on the basis of the PSD via the Einstein–Wiener–Khinchin theorem. This is based on the fact that an OFDM signal is cyclostationary. The PSD of an OFDM symbol is a rectangular function over all subcarriers other than the guard band. The autocorrelation of an OFDM symbol is simply the inverse Fourier transform of its PSD. The resulting PSD of an OFDM symbol is therefore a relatively narrow sinc function, whose width is proportional to the size of the guard band in a particular implementation. This can be seen in Figure 6, where the computed autocorrelation of half of the timing preamble symbol is shown, after the stripping of the cyclic prefix. The autocorrelation function has a narrow main peak and does not show significant correlation anywhere other than zero lag. The channel autocorrelation can be estimated with a 0th order Bessel function using the Jakes' model. On the basis of this modeling, it can be shown that the cross-correlation terms have a relatively small impact on the peak of the timing metric, so the numerator can be represented as follows:

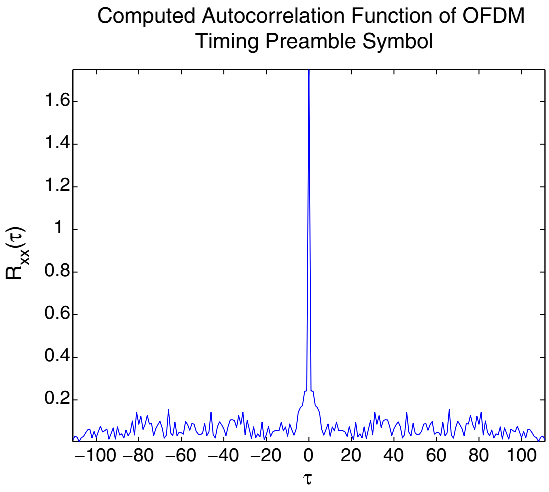


Figure 6. Computed autocorrelation of half of the first preamble symbol minus the cyclic prefix.

$$P(d) \approx R_{y(d)y(d)}(0) + \alpha^2 R_{y(d-N)y(d-N)}(0) \tag{42}$$

The most interesting case for the overlapping scenario is when $|N| = L$. In this case, the numerator will take the following form:

$$\begin{aligned} P(d) &= R_{y(d)y(d)}(0) + \alpha R_{y(d\pm L)y(d\pm L)}(\pm L) \\ &\quad + \alpha R_{y(d)y(d)}(\mp L) + \alpha^2 R_{y(d\pm L)y(d\pm L)}(0) \end{aligned} \tag{43}$$

which, on the basis of the preamble structure, becomes the following:

$$P(d) = (1+\alpha) R_{y(d)y(d)}(0) + \alpha(1+\alpha) R_{y(d\pm L)y(d\pm L)}(0) \tag{44}$$

This result will create two different scenarios for the timing metric plateau on the basis of the normalization term $R(d)$, dictated by $N = L, -L$:

$$M(d) > \begin{cases} \frac{1}{(1+\alpha)^2\left(1+\frac{1}{SNR}\right)^2} & : d \in \hat{D}, N = L \\ \frac{(1+\alpha)^2}{\alpha^2\left(1+\frac{1}{JNR}\right)^2} & : d \in \hat{D} - N, N = L \end{cases} \tag{45}$$

$$M(d) > \begin{cases} \frac{1+\alpha}{\left(1+\frac{1}{SNR}\right)^2} & : d \in \hat{D}, N = -L \\ \frac{\alpha^2}{(1+\alpha^2)\left(1+\frac{1}{JNR}\right)^2} & : d \in \hat{D} - N, N = -L \end{cases} \tag{46}$$

This result shows that the optimal strategy for the false preamble jammer is to transmit with a delay equal to L. This maximizes the power normalization term $R(d)$ without contributing to the timing metric peak in $P(d)$ caused by the transmitter's preamble. This lowers the bound on the timing metric peak $M(d)$. While all delay values $L \leq N \leq 2L$ will have this effect, the delay $N = L$ maximizes it. In addition, this effect will still make an impact even without channel or symbol knowledge.

4.3. Preamble nulling attack

The preamble nulling attack aims to destroy the timing symbol, specifically by inverting it in the time domain, thus destructively interfering with it at the receiver. Preamble nulling is predicated on the jammer having an extremely high level of knowledge of both the system it is attacking, as well as the radio-frequency environment. Without knowledge of these underlying conditions, this attack becomes much less effective.

The performance of the acquisition system in the presence of this attack can also be derived using the relationships in (23)–(25). The nulling jammer is sent by making

DOI: 10.1002/wcm

$j_n = -x_n$ and $f_j = f$. Substituting the jamming waveform into the (23) metric equations yields the following:

$$\begin{aligned} P(d) = \sum_{m=0}^{L-1} \Bigg[& \left| \sum_{k=0}^{C-1} x_{d+m-k} h_k \right|^2 e^{2\pi j \frac{f}{f_s} L} \\ & - \alpha \left| \sum_{k=0}^{C-1} x_{d+m-k} h_k \right|^2 e^{2\pi j \frac{f_j - f}{f_s}(d+m)} e^{2\pi j \frac{f_j}{f_s} L} \\ & - \alpha \left| \sum_{k=0}^{C-1} x_{d+m-k} h_k \right|^2 e^{2\pi j \frac{f - f_j}{f_s}(d+m)} e^{2\pi j \frac{f}{f_s} L} \\ & + \alpha^2 \left| \sum_{k=0}^{C-1} x_{d+m-k} h_k \right|^2 e^{2\pi j \frac{f_j}{f_s} L} \Bigg] \end{aligned} \tag{47}$$

This attack requires that the power of the preamble symbol detected at the receiver be very close to the noise floor. However, (47), along with 24 and (25), show that there are various opportunities for error between the preamble and the nulling attack. In an implementation, it is hard to guarantee that α be such that SJR = 0 dB (α = 1 in this case). In addition, there will be some slight errors in the channel estimation and inversion, plus some slight delay term on the basis of the arrival of each signal.

4.4. Preamble warping

Because 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. 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 inverse FFT and repeating it in the time domain or by taking a full-length inverse FFT in the frequency domain where every other subcarrier is populated with a pseudo-noise 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 in order to destroy time domain correlation.

Preamble warping essentially transforms the first symbol of the preamble into a generic preamble symbol, albeit that the pseudo-noise 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.

Analytically, the impact of the attack is actually better described starting from (23). In the case of the warping attack, the jamming signal will have the same form as the first preamble symbol. It is sent at the receiver frequency but shifted over one frequency bin, such that

$$\begin{aligned} r_n = & \left(\sum_{k=0}^{C-1} x_{n-k} h_k \right) e^{\left(2\pi j \frac{f}{f_s} n\right)} \\ & + \alpha \left(\sum_{i=0}^{K-1} j_{n-i} k_i \right) e^{\left(2\pi j \left(\frac{f}{f_s} + \frac{1}{2L}\right) n\right)} + n_n \end{aligned} \tag{48}$$

Applying this result to the numerator of the timing metric, while once again disregarding the noise term, yields the following:

$$\begin{aligned} P(d) = \sum_{m=0}^{L-1} \Bigg[& \left| \sum_{k=0}^{C-1} x_{d+m-k} h_k \right|^2 e^{2\pi j \frac{f}{f_s} L} \\ & + \alpha \left(\sum_{k=0}^{C-1} x^*_{d+m-k} h^*_k \right) \\ & \times \left(\sum_{i=0}^{K-1} j_{d+m+L-i} k_i \right) e^{2\pi j \frac{f}{f_s} L} e^{\pi j \frac{1}{L}(d+m+L)} \\ & + \alpha \left(\sum_{i=0}^{K-1} j^*_{d+m-i} k^*_i \right) \\ & \times \left(\sum_{k=0}^{C-1} x_{d+m+L-k} h_k \right) e^{2\pi j \frac{f}{f_s} L} e^{-\pi j \frac{1}{L}(d+m+L)} \\ & + \alpha^2 \left| \sum_{i=0}^{K-1} j_{d+m-i} k_i \right|^2 e^{2\pi j \frac{f}{f_s} L} e^{\pi j} \Bigg] \end{aligned} \tag{49}$$

factoring out the constant phase term, using the time repetition properties of both sequences, and noting that the middle terms are complex conjugates yields the following:

$$\begin{aligned} P(d) = \sum_{m=0}^{L-1} \Bigg[& \left| \sum_{k=0}^{C-1} x_{d+m-k} h_k \right|^2 \\ & + 2\alpha \operatorname{Re} \Bigg[\left(\sum_{k=0}^{C-1} x^*_{d+m-k} h^*_k \right) \\ & \qquad + \left(\sum_{i=0}^{K-1} j_{d+m-i} k_i \right) e^{\pi j \frac{1}{L}(d+m+L)} \Bigg] \\ & - \alpha^2 \left| \sum_{i=0}^{K-1} j_{d+m-i} k_i \right|^2 \Bigg] e^{2\pi j \frac{f}{f_s} L} \end{aligned} \tag{50}$$

The middle term represents a randomly phase-shifted correlation between the transmitter symbol and the jammer symbol, which has an expected value of zero. Combining this with the fact that the definition in (12) produces the following:

$$P(d) = \sigma_{xc}^2 - \alpha^2 \sigma_{jk}^2 \tag{51}$$

For cases where σ_{xc}^2 and σ_{jk}^2 are close in value, it is optimal for the jammer to set α = 1. This result shows that a jammer using this attack should adjust the value of α in order to match the power of the transmitted symbol at the receiver in order for this attack to be most effective. It also indicates that a scenario where the jammer has channel knowledge but does not use the exact same symbol as the transmitter is optimal. This way, the power terms for each of the symbols will be closest in value, and the cross terms will still have an expected value of zero.

5. SIMULATION

We developed simulations for both the synchronization system and each of the efficient attacks in order to test the performance of current synchronization algorithms in the face of symbol timing attacks. The tests were performed in multiple scenarios for each jammer in order to illustrate their individual capabilities. The minimum knowledge requirements for each of the jammers is displayed in Table I.

System performance versus the false preamble timing attack are in line with the analytical results. The results in Figure 7 indicate that the false preamble timing attack is extremely effective in destroying the symbol timing estimate, especially in the case where the delay, N, of the false preamble is equal to the timing window length L. This means that a hostile communication system could also fool the receiver into synchronizing with itself as opposed to the true transmitter, while still being power efficient.

The preamble warping results also reflect the analytical results as well. The attack is most effective when the two symbols are transmitted at identical power, which is the more likely when the jammer has channel knowledge. However, even in the case where the jammer has no channel knowledge, Figure 8 shows that there is a significant disruption to acquisition at the receiver, producing error rates of almost 0.5.

In addition, Figure 8 indicates that the error rate is higher at higher SJRs. This is because the signal power and the SNR were kept constant, while the jammer power was varied for comparison. This result signifies that increasing the jammer power too high will actually start to improve the timing acquisition at the receiver. This is because the warping attack is just a frequency shifted version of the timing preamble symbol, so sending a highly powered jamming signal will effectively increase the SNR seen at the receiver. However, the coarse frequency estimate would likely also be hampered, but as far as the timing estimation goes, this result is undesirable for a jammer. This is a useful result because it indicates that jammers using a warping attack are better off erring on the side of lower power than the transmitter signal, making this attack even more efficient.

Figure 9 illustrates the precision of the power level required for the preamble nulling attack. If the attack is not received at exactly equal power as the preamble, the system performance is then dictated by the effective SNR of the preamble at the receiver, shown in Figure 5.

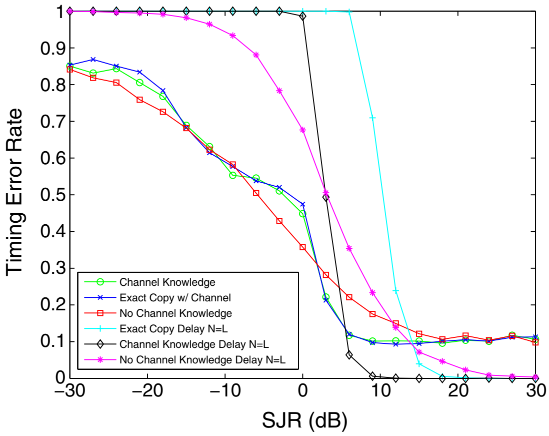


Figure 7. Symbol timing error rate as a function of the signal-to-jammer ration (SJR) of the false preamble timing attack.

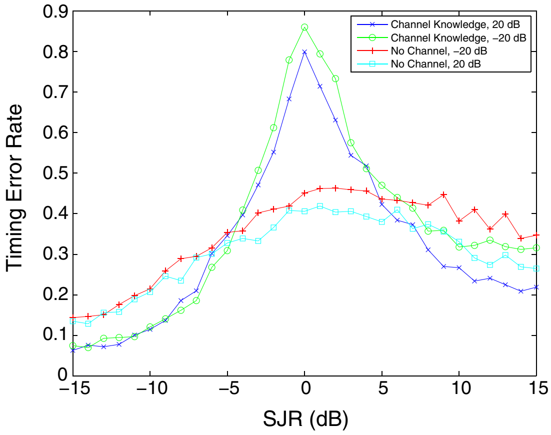


Figure 8. Symbol timing error rate as a function of the signal-to-jammer ratio (SJR) at the receiver caused by the preamble warping attack at a signal-to-noise ratio of 20 dB.

Table I. Situational knowledge provided to each jammer for simulation.

Jamming attack	Structure	Symbol timing	Frequency offset	Channel
False preamble	Yes	Window	No	No
Preamble nulling	Yes	Exact	Yes	Yes
Preamble warping	Yes	Exact	Yes	No

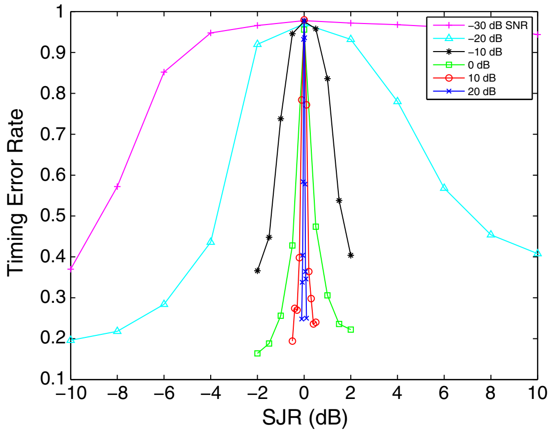


Figure 9. Timing estimate error rate as a function of the signal-to-jammer ration (SJR) for the preamble nulling attack at a signal-to-noise ratio (SNR) of 20 dB.

6. ATTACK MITIGATION

There are many security gaps in current OFDM acquisition schemes that leave room for future research. While many synchronization methods have been studied, there is a lack of work focused on scenarios involving jamming or other security threats. In this paper, we propose three solutions as the most viable and present some initial results regarding one of them.

6.1. 'Sync-amble' randomization

The first attack mitigation strategy proposed in this paper is called sync-amble randomization. This improved OFDM synchronization method allows for coordinated movement of the acquisition training symbol from frame to frame. The term sync-amble comes from the idea that the training symbol is no longer required to occur at the beginning of a block OFDM frame. In order to coordinate the start and end of each frame, as well as reduce computational complexity at the receiver, the sync-amble location within each frame after the first can be shared as secret knowledge between the transmitter and the receiver. Finally, the sync-amble location is chosen as a random variable of a uniform distribution with a support of discrete values covering the range of possible locations within a frame. Choosing from this maximum entropy distribution will ensure that the synchronization process is most protected from a cognitive jammer. Figure 10 illustrates the differences in frame structure between this method and existing synchronization strategy.

In terms of computational complexity, the receiver is now required two extra tasks. The first task is to buffer the entire OFDM frame until the preamble is located and synchronization is performed. The buffer length required would be $L_{buf} = \left(2L + T_{cp} * f_s\right) n$ samples. However, this would allow for demodulation of OFDM symbols to be performed in parallel.

There are two cases for the second task. The first case is for when there is no sharing of preamble location within the OFDM frame. This means that the preamble search extends along the entire buffered frame, resulting in an added complexity dependent on the synchronization method. For the method presented in [11], the timing metric computation can be implemented recursively, requiring around $\left(2L + T_{cp} * f_s\right) n$ computations. The second case is when the relative preamble location is shared between the transmitter and the receiver. If the location is shared in the preamble, for example, the symbol could be demodulated efficiently using an FFT, reducing the number of computations required to the order of around $\left(2L + T_{cp} * f_s\right) n_w$, where n_w represents the size of the preamble search window in terms of symbols ($n_w << n$), plus $\Theta(2L \log(2L))$ computations for the FFT (Figure 11).

6.2. Cross ambiguity function synchronization

The next strategy for improving OFDM acquisition security presented in this paper is cross ambiguity function (CAF) synchronization. This improvement is actually an entirely new synchronization algorithm aimed at making the structure of the preamble—or sync-amble—more generic relative to other OFDM symbols, in turn making it harder to detect by an outside threat. The CAF synchronization method does not require a time repetitive training symbol. Instead, CAF-based synchronization uses a training symbol that is known at the receiver in order to perform timing and frequency correction. In order to find the timing

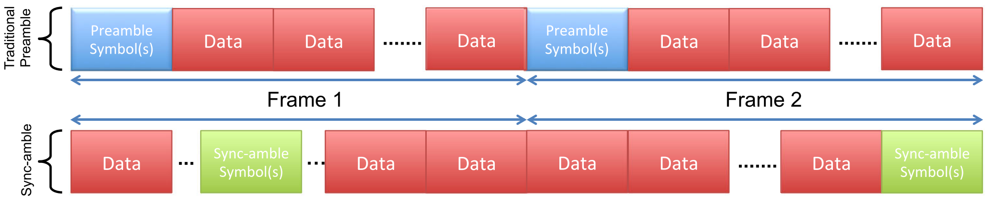


Figure 10. Orthogonal frequency-division multiplexing (OFDM) frame structure using a traditional preamble versus a sync-amble. The preamble occurs at the beginning of each frame, making its occurrence periodic. The sync-amble can be located anywhere within an OFDM frame—the trade off that it's location within the frame must be either conveyed to the receiver or the receiver must buffer and search the entire frame for the training symbol.

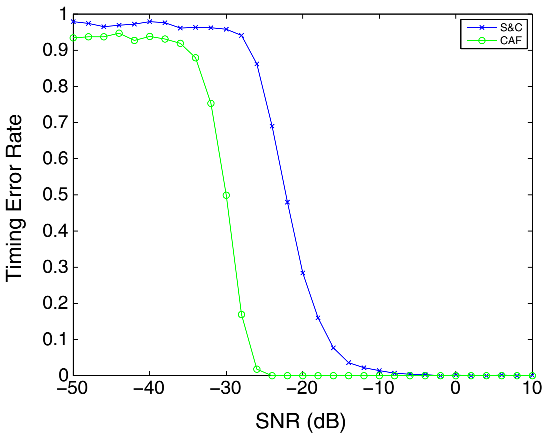


Figure 11. Timing estimate error rate as a function of the signal-to-noise ratio (SNR) for the cross ambiguity function (CAF) synchronization algorithm versus the Schmidl and Cox synchronization method. The increase in the CAF performance is attributed to the CAF using the entire OFDM training symbol—including cyclic prefix—to determine symbol timing. The Schmidl and Cox method utilizes only half of the symbol power without the cyclic prefix but has a much less computationally complex implementation.

and frequency offset with the CAF, the receiver must have a copy of the baseband equivalent of the preamble symbol x_n. The sampled signal at the receiver after baseband conversion is defined as follows:

$$r_n = \left(\sum_{k=0}^{C-1} x_{n-d-k} h_k \right) e^{2\pi j \frac{f}{f_s} n} + n_n \tag{52}$$

where the subscript n represents the sample index and spans the search area for the training symbol, d is the delay value and timing point of the symbol, C is the length of the channel approximation, f represents the carrier frequency offset, and n is the noise term. From this, the CAF is computed as follows:

$$A(u, v) = \left| \sum_{k=0}^{N-1} x_k r^*_{k+u} e^{-2\pi jkv/N} \right| \tag{53}$$

where u and v represent the timing and frequency offsets in terms of samples and frequency bins, respectively, such that $|u| \leq d_{max}$ and $|v| \leq Nf_{max}/f_s$. N represents the length of the signals used in the CAF computation, while t_{max} and f_{max} are the finite range over which the offsets for timing and frequency are computed. The peak of this function over both timing and frequency offsets provide the timing and frequency offsets for the receiver. Figure 12 demonstrates the performance of the CAF synchronization algorithm in an AWGN and multipath scenario, as well as against the preamble warping and false preamble attacks.

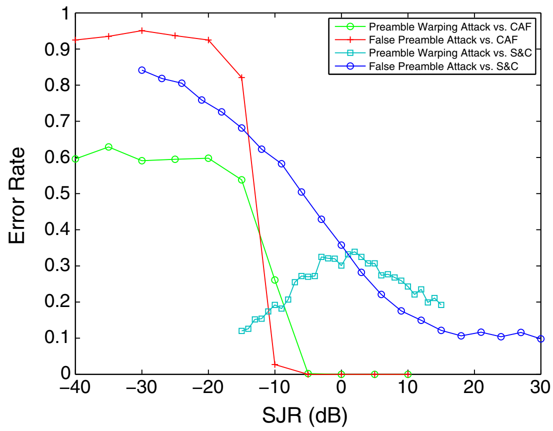


Figure 12. Timing estimate error rate as a function of signal-to-jammer ratio (SJR) for the cross ambiguity function (CAF) synchronization algorithm versus the Schmidl and Cox synchronization algorithm in the presence of various attacks. The CAF synchronization mitigates the power-efficient attacks at the expense of acquisition complexity.

In terms of system complexity, the CAF method requires a significantly higher computational burden than the method presented in [11]. While there are many known efficient methods for computing the CAF, there is no recursive implementation, and the correlation products must be computed either across $n \in u$ or $k \in v$. This means that the CAF synchronization method requires roughly $\left(2L + T_{cp} * f_s\right) \min(|u|, |v|)$ computations for each correlation plus $\Theta\left(\left(2L + T_{cp} * f_s\right) \min(|u|, |v|) \log\left(\left(2L + T_{cp} * f_s\right) \min(|u|, |v|)\right)\right)$ computations for FFTs because the cyclic prefix is not stripped for this method. The other important drawback to this method is that it requires a known training symbol at the receiver or a small set of known symbols—similar to LTE synchronization—which represents a new area of security vulnerability.

6.3. Spatial diversity synchronization security

The final security upgrade of OFDM synchronization proposed in this paper is through the use of multiple-input multiple-output. Work has already been performed in [20] to show that the advantages of multiple-input multiple-output can be harnessed for the purposes of synchronization. It is very possible that there is a synchronization solution that replaces the need for timing diversity in the training symbols—the repeated nature of the first symbol—with spatial diversity. The preamble symbol would still be detectable with correlation processing, and although it will need to be distinguishable from other OFDM symbols, this is achievable in a much more subtle way than time domain repetition.

7. CONCLUSION

There are various weak points in OFDM synchronization algorithms that are susceptible to intelligent jamming attacks. Attacks that specifically target the preamble can be highly effective and efficient in disrupting OFDM-based communication. By targeting symbol timing estimation, which is the first step in the synchronization process, a jammer can propagate massive errors to all sync estimates. While these attacks have been demonstrated on one algorithm in particular, almost all of the synchronization algorithms referenced in this paper use similar correlation-based approaches and have identifiable synchronization signals, leaving them susceptible to similar attacks. Many improvements can be made to this process in order to mitigate these attacks. We have proposed a CAF-based synchronization system to deal with some of these problems. Further research aimed at improving the robustness of these algorithms in adversarial scenarios will improve the overall performance of OFDM-based systems.

ACKNOWLEDGEMENTS

The authors would like to thank fred harris for his insightful discussions and correspondences on the topic.

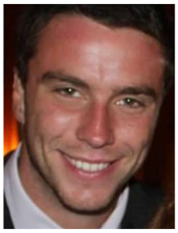
REFERENCES

1. The IEEE 802.16 Working Group on Broadband Wireless Access Standards. 802.16e-2009, 2009.
2. The 3rd Generation Partnership Project (3GPP). Long Term Evolution (LTE), 2009.
3. Clancy TC. Efficient OFDM denial: pilot jamming and pilot nulling. In *IEEE International Conference on Communications (ICC)*, Kyoto, Japan, 2011; 1–5.
4. Minn H, Bhargava V, Letaief K. A combined Timing and frequency synchronization and channel estimation for OFDM. In *IEEE International Conference on Communications (ICC)*, Paris, France, 2004; 872–876.
5. Moretti M, Cosovic I. OFDM synchronization in an uncoordinated spectrum sharing scenario. In *IEEE Global Telecommunications Conference (GLOBECOM)*, Washington, DC, USA, 2007; 3796–3801.
6. Patil S, Upadhyay R. A symbol timing synchronization algorithm for WiMAX OFDM. In *Conference on Computational Intelligence and Communication Networks (CICN)*, Gwalior, India, 2011; 78–82.
7. Kleider J, Gifford S, Maalouli G, Chuprun S, Sadler B. Synchronization for RF carrier frequency hopped OFDM: analysis and simulation. In *IEEE Military Communications Conference (MILCOM)*, vol. 2, Boston, MA, USA, 2003; 1237–1242.
8. Nasraoui L, Atallah L, Siala M. An efficient reduced-complexity two-stage differential sliding correlation approach for OFDM synchronization in the AWGN channel. In *IEEE Vehicular Technology Conference (VTC)*, San Francisco, CA, USA, 2011; 1–5.
9. Moose P. A technique for orthogonal frequency division multiplexing frequency offset correction. *IEEE Transactions on Communication* October 1994; **42**: 2908–2914.
10. van de Beek JJ. Low-complex frame synchronization in OFDM systems. In *International Conference on Universal Personal Communications (ICUPC)*, Tokyo, Japan, 1995; 982–986.
11. Schmidl T, Cox D. Robust frequency and timing synchronization for OFDM. *IEEE Transactions on Communications* December 1997; **45**(12): 1613–1621.
12. Shahriar C, Sodagari S, Clancy TC. Performance of pilot jamming on MIMO channels with imperfect synchronization. In *2012 IEEE International Conference on Communications (ICC)*, Ottawa, Canada, 2012; 898–902.
13. Shahriar C, Sodagari S, McGwier RW, Clancy TC. Performance impact of asynchronous off-tone jamming attacks against OFDM. In *2013 IEEE International Conference on Communications (ICC)*, Budapest, Hungary, 2013; 2177–2182.
14. Sanguinetti L, Morelli M, Poor HV. Frame detection and timing acquisition for OFDM transmissions with unknown interference. *IEEE Transactions on Wireless Communications* 2010; **9**: 1226–1236.
15. Ramiah KVS, Zivkovic M. OFDM synchronization in the presence of interference. In *International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, Sharjah, UAE, 2013; 1–5.
16. Tao L, Mow WH, Lau VKN, Siu M, Cheng RS, Murch RD. Robust joint interference detection and decoding for OFDM-based cognitive radio systems with unknown interference. *IEEE Journals on Selected Areas in Communications* 2007; **25**: 566–575.
17. Sun P, Zhang L. Narrowband interference effect on timing synchronization for OFDM-based spectrum sharing system. In *International Conference on Wireless and Mobile Communications (ICWMC)*, Valencia, Spain, 2010; 274–278.
18. Marey M, Steendam H. Analysis of the narrowband interference effect on OFDM timing synchronization. *IEEE Transactions on Signal Processing* 2007; **55**: 4558–4566.
19. Klenner P, Kammeyer K. Temporal autocorrelation estimation for OFDM with application to spatial interpolation. In *IEEE Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, 2008; 995–999.

DOI: 10.1002/wcm

20. Peng D, Peng L, Yin C, Yue G. The spatial diversity algorithms of carrier frequency offset synchronization for MIMO-OFDM systems. In *2006 IET International Conference on Wireless, Mobile and Multimedia Networks*, Hangzhou, China, 2006; 1–3.

AUTHORS' BIOGRAPHIES



Matthew J. La Pan is a PhD candidate at Virginia Tech in the Bradley Department of Electrical and Computer Engineering. Additionally, he is a 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. Matt received his BS in Electrical Engineering from the University of Miami in 2010 and his MS in Electrical Engineering from Virginia Tech in 2012.

T. Charles Clancy is an Associate Professor at Virginia Tech in the Bradley Department of Electrical and Computer Engineering. Additionally, he is director of the Hume Center for National Security and Technology. In his role, Dr. Clancy is responsible for leading Virginia Tech's collaboration with national security organizations within the US federal government and industry. His current research interests include wireless security, spectrum management, and electronic warfare. Dr. Clancy received his BS in Computer Engineering from the Rose-Hulman Institute of Technology, his MS in Electrical Engineering from the University of Illinois, Urbana-Champaign, and his PhD in Computer Science from the University of Maryland, College Park. He currently serves as an editor for *IEEE Transactions on Information Forensics and Security*. He is a Senior Member of the IEEE.

Robert McGwier is the Director of Research of the Ted and Karyn Hume Center for National Security and Technology and Research Professor in the Bradley Department of Electrical and Computer Engineering at Virginia Tech. He leads the overall execution of the center's research mission, Blacksburg operations, and lead's the university's program development efforts in national security applications of wireless and space systems. His area of expertise is in radio-frequency communications and digital signal processing. Before joining Virginia Tech, Dr. McGwier spent 26 years as a member of the technical staff at the Institute for Defense Analyses' Center for Communications Research in Princeton, NJ, where he worked on advanced research topics in mathematics and communications supporting the federal government. He received his PhD in applied mathematics from Brown University in 1988. His work on behalf of the federal government has earned him many awards, including one of the intelligence community's highest honor in 2002.