Phase Warping and Differential Scrambling Attacks Against OFDM Frequency Synchronization

Matthew J. La Pan *† T. Charles Clancy * Robert W. McGwier †
Bradley Department of Electrical and Computer Engineering
Virginia Tech
Email: {mlapan4, tcc, rwmcgwi}@vt.edu

***Abstract*—Orthogonal Frequency Division Multiplexing (OFDM) is used in many modern communications systems. Timing and frequency synchronization in an OFDM system are critical to performance and must be carried out early and often. Current synchronization methods, such as those developed by Schmidl and Cox [1], were not designed to be robust to adversarial signals. A series of attacks against the preamble synchronization stage have been developed and demonstrated to debilitate OFDM receivers. Multiple attacks against the frequency offset error estimation stage are discussed, and some possible improvements to OFDM synchronization algorithms are suggested.**

Keywords: OFDM, Synchronization, Jamming

I. Introduction

Orthogonal Frequency Division Multiplexing (OFDM) has become a leading modulation scheme in modern communications systems. This is because of its spectral efficiency, achievable data rates, and robustness in multipath fading environments. However, it has been shown that current implementations of OFDM are susceptible to a variety of signal jamming attacks [3]. Various efficient jamming attacks which target the pilot tones used by OFDM communications systems have been derived. While this is one aspect of communicating with OFDM which must be improved, it is not the only area of weakness to an intentional adversarial attack.

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 in order to avoid inter-symbol interference (ISI), as well as inter-carrier interference (ICI) and loss of orthogonality among OFDM subcarriers. A number of algorithms have been developed in order to efficiently and robustly perform the synchronization [6], [7], [8], [9], [10]. This paper is based on the symbol timing and carrier frequency offset estimation algorithm designed by Schmidl and Cox [1], which is the maximum likelihood detector for OFDM, and because of its optimality variations of this algorithm are widely used in commercial systems based on OFDM, such as WiMAX and Long Term Evolution (LTE).

While there has been some research conducted on analyzing and improving the robustness of OFDM synchronization algorithms, the majority of this work has been conducted under the assumption of uncorrelated interference. In this study, we look at specific adversarial signals which are highly correlated and designed with the intent of disrupting the communication of a transmitter and receiver using OFDM during the synchronization stage. In particular, this study has focused around preventing a receiver employing OFDM from ever acquiring the proper frequency offset error estimate. In order to fully explain this approach it is important to outline the synchronization approach and the physical model under which some of these scenarios were conducted.

II. Synchronization Model

The synchronization method proposed in [1] has three main stages–symbol timing estimation, fine carrier frequency offset estimation and correction, and coarse carrier frequency offset estimation. These stages are performed sequentially in the order listed. This algorithm is based on the use of specific *preamble* symbols, transmitted at the beginning of every frame. Because of the particular structure of this synchronization algorithm, the preamble symbols have a very specific structure as indicated in [1].

The first step in the synchronization process is the estimation of symbol timing. Only the first preamble symbol is used for the timing stage. Once the complex time domain samples are obtained after radio frequency (RF) down conversion then the timing estimation algorithm is carried out. A sliding window of L samples is used to search for 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

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

and the second according to

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

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

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

which determines the symbol timing.

This metric will generate a plateaued peak that is the length of the cyclic prefix less the length of the channel impulse response. The symbol timing estimate can be taken from anywhere on the plateau. This timing estimate will tell the receiver the starting point of the window of samples to grab in order to process an incoming frame. Once this stage 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. This stage corrects for the error introduced by the clocks at both the transmitter and the receiver. There are actually two sub-stages within frequency correction: fine frequency correction and coarse frequency correction. The fine frequency correction Δf is estimated using

$$\Delta f = \text{angle}(P(d))/\pi T \tag{4}$$

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. Once the fine frequency offset has been computed and corrected for, the frequency domain result will be the original symbol, with a possible frequency shift of an integer number of 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 in order to determine the number of bins that the symbols are shifted in either direction.

$$B(g) = \frac{|\sum_{k\in\mathcal{X}} R^*_{1,k+2g} v^*_k x_{2,k+2g}|^2}{2(\sum_{k\in X} |R_{2,k}|^2)^2} \tag{5}$$

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 differential sequence between the common subcarriers of the first and second preamble symbol is defined as

$$v_k = \sqrt{2}\frac{c_{2,k}}{c_{1,k}} \tag{6}$$

where $c_{2,k}$ and $c_{1,k}$ are the sequences of complex symbols on the common subcarriers of the first and second preamble symbols. The point g_{max} at which the function $B(\cdot)$ is maximized represents the coarse frequency offset. The overall frequency offset is:

$$\hat{\Delta f} = \text{angle}(P(d))/\pi T + 2g_{\text{max}}/T \tag{7}$$

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

III. Physical Model

In order to study some of the effects of adversarial signals on the OFDM synchronization process, a simple model was developed to imitate a realistic physical scenario. Within this basic model there are three main signals involved which represent the transmitter, receiver and the jammer. The transmitter and the jammer broadcast signals x and j, respectively, which then pass through two unique multipath channels h and k, respectively. These channels can be modeled as finite length digital filters with white Gaussian noise added to each signal at a fixed signal to noise ratio (SNR). The received signal is the aggregate of both the transmitter and jammer signal after the addition of channel effects and noise. In this case, the received signal r is

$$r_n = \left(\sum_{k=0}^{C-1} x_{n-k}h_k\right) e^{(2\pi j \frac{f}{f_s} n)} + \left(\sum_{i=0}^{K-1} j_{n-i}k_i\right) e^{(2\pi j \frac{f_j}{f_s} n)} + n_n \tag{8}$$

where C and K represent the lengths of the multipath channel of the transmitter and the jammer, respectively. The symbols x and j represent the samples of the signals transmitted by the transmitter and the jammer, while the terms f and f_j represent the relative frequency offsets of the transmitter and the jammer. Finally, the term n represents the additive white Gaussian noise.

The power of the transmitter is assumed to be fixed, while the power output of the jammer can vary based on the attack signal. This scenario gives rise to the signal-to-jammer ratio (SJR), that will be used as one metric of efficiency of an attack signal.

There are some underlying assumptions which help further describe the jamming scenario. It is, of course, assumed that there are clock errors between the transmitter and the receiver, but in a real environment there will also be clock error between the jammer and the other two parties. It is therefore assumed that the jammer has previous knowledge of the timing and frequency recovery algorithm. It is also assumed that the jammer has knowledge of the preamble structure used in OFDM synchronization[1]. These pieces of knowledge will be the baseline for all of the attacks presented. Some attacks will require additional knowledge of the jamming environment, while other attacks will be effective based on only these assumptions.

IV. Jamming Attacks

While the synchronization process described by Schmidl and Cox 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. It is interesting to note that, while OFDM is much more sensitive to errors in the estimation of carrier frequency offset than symbol timing,

[1]If the jammer is targeting a known signal standard, then this information would readily be available when constructing the jamming attack.

there are still various ways in which synchronization could be disrupted by creating error in either value, or possibly both.

A. Preamble Phase Warping

The first of the frequency based synchronization jamming attacks is preamble phase warping. This attack aims to disrupt the frequency offset estimate of the receiver by sending a frequency shifted preamble symbol which can be represented as

$$w_n = \left(\sum_{i=0}^{K-1} j_{n-i} k_i \right) e^{(2\pi j \frac{f_j}{f_s} n)} \tag{9}$$

at the receiver. The term f_j represents the phase warp term, which is just a random frequency shift of the preamble symbol. While it is important to note that this type of attack could be used to change the overall frequency error estimate at the receiver, its most likely use is to degrade the fine frequency estimate. This is because OFDM systems begin to suffer noticeable degradations in SNR for frequency offsets that are greater than 1% of the subcarrier spacing [11]. 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 type of attack can also have an effect on the timing estimate of the receiver, though that is beyond the scope of this paper.

B. Differential Scrambling Attack

The other frequency estimation smart attack proposed in this paper is the differential scrambling attack. 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 in order 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 equation 6. The differential scrambling attack targets this differential sequence and prevents subcarrier alignment by altering the sequence $c_{2,k}$ according to

$$w_k = \sqrt{2} \frac{c_{2,k}}{c_{1,k} + c_{ds,k}} \tag{10}$$

The attack is carried out by transmitting a constant stream of symbols across the subcarriers used in the first preamble symbol, in the case of these experiments a constant quadrature phase shift key symbol of $c_{ds} = 1 + 1j$. Although the differential sequence is the target of the attack, in sequence is unchanged since it is prerequisite knowledge at the receiver, rather the coarse frequency estimate becomes

$$B(g) = \frac{|\sum_{k \in \mathcal{X}} (H^*_{k-f+2g} X^*_{1,k-f+2g} + K^*_{k-f+2g} J^*_{1,k-f+2g} + N^*_{1,k}) \frac{X^*_{2,k}}{X^*_{1,k}} (X_{2,k-f+2g} H_{k-f+2g} + N_{2,k})|^2}{(\sum_{k \in \mathcal{X}} |X_{2,k-f} H_{k-f} + N_k|^2)^2} \tag{11}$$

This attack is similar in structure to the false preamble timing attack proposed in [2]. However, this attack will not disrupt the timing estimation at the receiver. Instead, 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.

V. Simulation

We developed some simulation scenarios in order to determine the impact of these frequency jamming attacks on OFDM synchronization. Each attack was tested under two different scenarios. The first scenario is assuming that the jammers have full channel knowledge of both their own channel and the transmitters. This means that the jammer can send a signal

$$\hat{j}_n = \alpha \left(\sum_{l=0}^{K-1} p_{n-l} k_l^{-1} \right) \tag{12}$$

where

$$p_n = \left(\sum_{i=0}^{C-1} j_{n-i} h_i \right) e^{(2\pi j \frac{f_j}{f_s} n)} \tag{13}$$

where α is determined by the SJR, and the frequency shift is a determined randomly and constrained to within a few subcarrier spacings. The term p_n is the jamming signal convolved with the channel response of the transmitter's channel at the given frequency offset. The term $\hat{j}_n$ represents the scaled convolution of signal p_n with k_i^{-1}, the inverse of the jammer's channel. This means that the received jamming signal will be p_n. The second scenario assumes no channel knowledge by the jammer, so that both the transmitter and jammer transmit across distinct multipath channels. Both of these scenarios were simulated a thousand times each over a range of SJRs. The frequency error threshold was conservatively chosen to be a tenth of a subcarrier, which is more than enough error to cause significant loss of orthogonality, leading to ICI and degredation[11]. It is also important to point out that these simulations required the receiver to detect the timing point correctly before frequency estimation. This means that a small portion of the errors–on the order of 10

The results for the phase warping attack from figure 1 show that it is highly disruptive to the frequency offset estimation at the receiver. While the phase warping attack is extremely effective in causing errors when it has channel knowledge and transmits at equal or higher power as the transmitter, the phase warper with no channel knowledge actually performs better at higher SJRs. Although this result is not intuitive and is somewhat surprising, it is most likely derived from the fact that the jammer without channel knowledge is more likely to

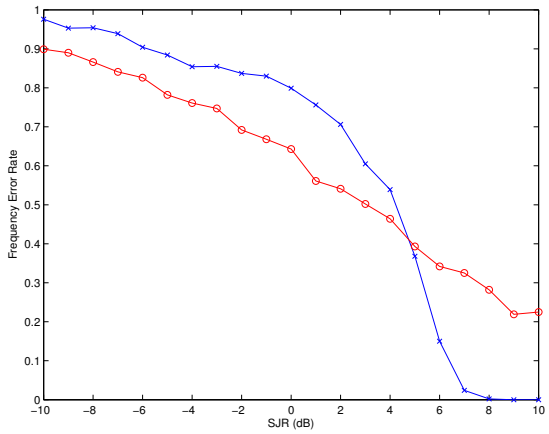

Fig. 1. Frequency offset estimation error rate as a function of the SJR for different varieties of the phase warping attack.

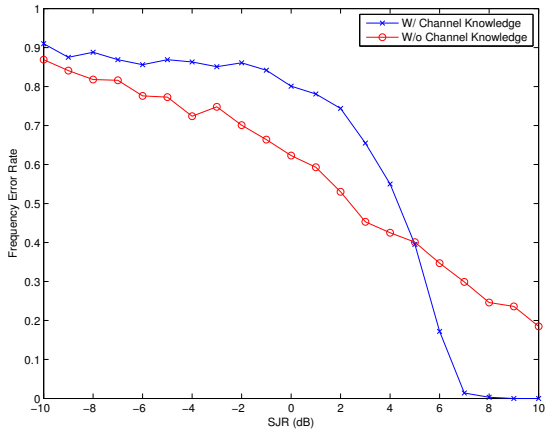

Fig. 2. Frequency offset estimation error rate as a function of the SJR of two varieties of the differential scrambling attack.

degrade the orthogonality of the received signal and cause ICI in the received symbol.

The differential scrambling attack shows a similar performance curve to the phase warping attack, although the error rate seems to approach a maximum of .9, as seen in figure 2. Again, the jammer without channel knowledge shows a higher performance at high SJRs. Although this result is not intuitive, it speaks to the sensivity of OFDM synchronization to slight errors in subcarrier alignment. It is important to note that this style of coarse jamming attack is the most basic– constant symbols are transmitted against all of the subcarriers. There For both cases the simulation results demonstrate just how devastating these synchronization attacks can be.

VI. Attack Mitigation

The deficiencies of existing OFDM signal acquisition algorithms against adversarial signals leaves plenty of room for future research and improvement. We propose that there are three solutions which are most pertinent to mitigating synchronization jamming in OFDM. The first of these mitigations is to randomize the preamble's location within a frame. Although this would require more processing at the receiver, it would prevent any jammer from being able to lock on to the synchronization process and launch timed attacks against the preamble.

The second solution proposed in this paper is to perform synchronization with the cross ambiguity function (CAF). This would be an entirely different method for synchronization that would better disguise the location of the preamble. The CAF provides a frequency difference of arrival (FDOA) and a time difference of arrival (TDOA) between two signals, which would represent the timing and frequency offsets at the receiver. This method would require a known copy of the preamble, or a table of preambles, at the receiver (much like the known differential sequence at the receiver for coarse estimation). This method has already been shown to be applicable for coarse frequency offset estimation [13]. However, this solution does not provide the matched filter features of the time delay line correlation and might require multipath channel estimation at the receiver before synchronization.

The last form of jamming mitigation proposed in this paper is an alternative form of synchronization using spatial diversity. As OFDM is becoming an integral part of modern communications, multiple-input multipl-output (MIMO) is becoming equally prevalent. Prior research has been conducted to show that carrier frequency offset estimation is possible using the spatial diversity advantages of MIMO [**?**]. This is another method which would make the synchronization process less obvious to a potential attacker.

VII. Conclusion

There are various weak points in OFDM synchronization algorithms which are susceptible to intelligent jamming attacks. Attacks which specifically target the preamble can be highly effective and efficient in disrupting OFDM based communication. Two such attacks are presented in this paper which specifically target the frequency error estimation step of the synchronization process. These attacks pose an especially high threat to OFDM systems because of the inherent sensitivity of OFDM to frequency offset errors. Both of the attacks presented in this paper are shown to significantly degrade the performance of an OFDM system. Many improvements can be made to the synchronization process in order to mitigate these attacks, and further research aimed at improving the robustness of these algorithms in adversarial scenarios will improve the overall performance of OFDM-based systems.

VIII. Acknowledgements

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

REFERENCES

[1] T. Schmidl, D. Cox, "Robust Frequency and Timing Synchronization for OFDM", *IEEE Transactions on Communications* Vol. 45, No.12, December 1997.

[2] M. La Pan, T. Clancy, R. McGwier, "Jamming Attacks Against OFDM Timing Synchronization and Signal Acquisition", *IEEE Military Communications Conference (MILCOM)*, October 2012.

[3] T. Clancy, "Efficient OFDM Denial: Pilot Jamming and Pilot Nulling", *IEEE International Conference on Communications (ICC)*, June 2011.

[4] T. Pollet, M. Van Bladel, M. Moeneclaey, "BER Sensitivity of OFDM Systems to Carrier Frequency Offset and Wiener Phase Noise", *IEEE Transactions on Communications (ICC) 1995*, Vol. 43, No. 2/3/4, Feb/Mar/Apr 1995.

[5] P. Klenner, K. Kammeyer, "Temporal Autocorrelation Estimation for OFDM with Application to Spatial Interpolation", *IEEE Asilomar Conference on Signals, Systems and Computers*, pp 995–999, October 2008.

[6] H. Minn, V. Bhargava, K. Letaief, "A Combined Timing and Frequency Synchronization and Channel Estimation for OFDM", *IEEE International Conference on Communications (ICC)*, June 2004.

[7] M. Moretti, I. Cosovic, "OFDM Synchronization in an Uncoordinated Spectrum Sharing Scenario", *IEEE Global Telecommunications Conference (GLOBECOM)*, November 2007.

[8] S. Patil, R. Upadhyay, "A Symbol Timing Synchronization Algorithm for WiMAX OFDM", *Conference on Computational Intelligence and Communication Networks (CICN)*, October 2011.

[9] J. Kleider, S. Gifford, G. Maalouli, S. Chuprun, B. Sadler, "Synchronization for RF Carrier Frequency Hopped OFDM: Analysis and Simulation", *IEEE Military Communications Conference (MILCOM)*, October 2003.

[10] L. Nasraoui, L. Atallah, M. Siala, "An Efficient Reduced-Complexity Two-Stage Differential Sliding Correlation Approach for OFDM Synchronization in the AWGN Channel", *IEEE Vehicular Technology Conference (VTC)*, September 2011.

[11] R. van Nee, R. Prasad, *OFDM for Wireless Multimedia Communications*, Boston, MA: Artech House, 2000.

[12] D. Peng, L. Peng, C. Yin, G Yue, "The Spatial Diversity Algorithms of Carrier Frequency Offset Synchronization for MIMO-OFDM Systems", *Wireless, Mobile and Multimedia Networks, 2006 IET International Conference on*, November 2006.

[13] D. Li, Y. Li, H. Zhang, L. Wang, "Cross Ambiguity Function Based Integer Frequency Offset Estimation for OFDM Systems", *IEEE Wireless Communications and Networking Conference: PHY and Fundamentals*, 2012.