Blind Transmitter Authentication for Spectrum Security and Enforcement

Vireshwar Kumar
Electrical and Computer Engineering,
Virginia Tech,
Blacksburg, VA, USA
viresh@vt.edu

Jung-Min “Jerry" Park
Electrical and Computer Engineering,
Virginia Tech,
Blacksburg, VA, USA
jungmin@vt.edu

Kaigui Bian
Electronics Engineering and Computer Science,
Peking University,
Beijing, China
bkg@pku.edu.cn

ABSTRACT

Recent advances in spectrum access technologies, such as cognitive radios, have made spectrum sharing a viable option for addressing the spectrum shortage problem. However, these advances have also contributed to the increased possibility of “hacked” or “rogue” radios causing harm to the spectrum sharing ecosystem by causing significant interference to other wireless devices. One approach for countering such threats is to employ a scheme that can be used by a regulatory entity (e.g., FCC) to uniquely identify a transmitter by authenticating its waveform. This enables the regulatory entity to collect solid evidence of rogue transmissions that can be used later during an adjudication process. We coin the term *Blind Transmitter Authentication* (BTA) to refer to this approach. Unlike in the existing techniques for PHY-layer authentication, in BTA, the entity that is authenticating the waveform is *not* the intended receiver. Hence, it has to extract and decode the authentication signal “blindly” with little or no knowledge of the transmission parameters. In this paper, we propose a novel BTA scheme called *Frequency offset Embedding for Authenticating Transmitters* (FEAT). FEAT embeds the authentication information into the transmitted waveform by inserting an intentional frequency offset. Our results indicate that FEAT is a practically viable approach and is very robust to harsh channel conditions. Our evaluation of FEAT is based on theoretical bounds, simulations, and indoor experiments using an actual implementation.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*wireless communication*

Keywords

PHY-layer authentication; transmitter identification; cognitive radios; spectrum sharing and management

CCS'14, November 3–7, 2014, Scottsdale, Arizona, USA.
Copyright 2014 ACM 978-1-4503-2957-6/14/11 ...$15.00.
http://dx.doi.org/10.1145/2660267.2660318.

1. INTRODUCTION

In the shared spectrum access model, the secondary users (i.e., users with secondary access priority) employ cognitive radio and/or other advanced technologies to access the spectrum opportunistically [10]. Unlike legacy radios, these technologies enable a user to readily re-configure the transmission parameters, allowing for greater flexibility, but such a feature also increases the possibility of malicious or “rogue” transmitters that pose a serious threat to other transmitters. Here, a “rogue” transmitter is defined as a non-compliant transmitter that violates regulator-prescribed spectrum access rules. One approach for deterring rogue transmissions is for a regulator (e.g., FCC's Enforcement Bureau) to have the capability to uniquely identify or authenticate “rogue” transmitters [22]. However, the regulator that is attempting to identify the non-compliant transmitter is *not* the intended receiver. Hence, we refer to such a receiver as a “blind receiver”. As the name implies, the blind receiver has little, if any, knowledge about the communication parameters needed to demodulate and decode the detected signal. Hence, the blind receiver would need to carry out transmitter authentication at the PHY-layer, where the least amount of knowledge of the communication parameters is needed to authenticate the transmitter. We coin the term *Blind Transmitter Authentication* (BTA) to refer to the problem of authenticating a transmitter by extracting its unique, identifiable information from the received signal with *little* or *no* knowledge of the transmission parameters.

For BTA to be a viable approach for spectrum access enforcement, all transmitters should be mandated to employ a mechanism for embedding an authentication signal—which contains the identity of the transmitter and possibly a certificate of compliance (e.g., FCC *Declaration of Conformity*)—into the message signal (which contains the data that the transmitter wants to send). Also, tamper resistance techniques should be employed to prevent hackers from circumventing this embedding mechanism. In this paper, we assume that such mechanisms are incorporated into each radio used by a secondary user.

We want to emphasize that there are a few important differences between BTA and the conventional PHY-layer authentication problem [25, 32]. In the latter problem, it is assumed that the receiver (that is authenticating the signal) has complete knowledge of the transmission parameters, whereas in the former problem, the receiver is “blind”. Moreover, most, if not all, of the PHY-layer authentication schemes are designed to work when the received signal's signal to interference and noise ratio (SINR) is sufficiently high—e.g., high enough to demodulate and decode the message signal correctly. Because a blind receiver is not the "intended" receiver, it may need to carry out BTA at a location where the SINR is very low with significant multipath fading. Conventional PHY-layer authentication schemes would perform very poorly under such conditions. An *ideal* BTA scheme satisfies three requirements: (1) It incurs minimal overhead in terms of the message throughput and transmission power; (2) It enables a receiver to "blindly" extract the authentication information from the signal with little or no knowledge of the transmission parameters; and (3) Authentication can be performed under very harsh conditions (i.e., low SINR and significant multipath fading).

In this paper, we propose a BTA scheme called *Frequency offset Embedding for Authenticating Transmitters* (FEAT). To the best of our knowledge, FEAT is the first scheme that satisfies the three requirements of an ideal BTA scheme. FEAT modifies the frequency offset of each frame of the message signal to embed the authentication signal into the message signal. This is achieved in such a way that the authentication signal does not interfere with the decoding process of the message signal. Also, the authentication signal can be estimated at the blind receiver with only limited knowledge about the transmission parameters by estimating the frequency offset of each frame.

This paper's main contributions are summarized below.

- We have defined the BTA problem, and described how it differs from the conventional PHY-layer authentication problem.
- We propose a BTA scheme called FEAT. We have demonstrated that FEAT is the first scheme that satisfies all of the required criteria of an ideal BTA scheme. According to our results, FEAT outperformed the existing PHY-layer authentication approaches in all of the performance criteria that were considered.
- We have evaluated FEAT using simulation results and theoretical analysis. In addition, we have verified the validity of FEAT by carrying out experiments with an actual implementation.

The rest of the paper is organized as follows. We provide the related work in Section 2 and describe the technical background in Section 3. We discuss the proposed scheme in Section 4 and analyze it in Section 5. We evaluate the proposed scheme by comparing with the prior art in Section 6. We discuss a prototype implementation of the proposed scheme in Section 7. Section 8 concludes the paper by highlighting the main contributions.

2. RELATED WORK

PHY-layer authentication schemes can be broadly divided into two categories: intrinsic and extrinsic approaches. The schemes in the first category utilize the transmitter-unique "*intrinsic*" characteristics of the waveform as unique signatures to authenticate/identify transmitters. They include RF fingerprinting, and electromagnetic signature identification [5, 8, 14, 27]. Although these intrinsic approaches have been shown to work in controlled lab environments, their sensitivity to factors—such as temperature changes, channel conditions, and interference—limit their efficacy in real-world scenarios. The schemes in the second category enable a transmitter to "*extrinsically*" embed an authentication signal (e.g., digital signature) in the message signal and enable a receiver to extract it. Such schemes include PHY-layer watermarking [7, 11, 13, 16] and transmitter authentication [17, 20, 21, 25, 28, 29, 32]. On one hand, the intrinsic approaches require the blind receiver to have only a little knowledge about the transmission parameters to authenticate the transmitter, but they are limited by their low robustness against noise and security attacks [9]. On the other hand, the extrinsic approaches can be made highly robust against noise and security threats, but they require the blind receiver to have complete knowledge about the transmission parameters. Hence, the authors in [31] propose an authentication scheme in which the authentication signal is embedded into the message signal extrinsically to modify an intrinsic characteristic (cyclo-stationary signature) of the message signal. This enables the blind receiver to decode the authentication signal with high robustness with only a little knowledge about the transmission parameters. However, this scheme achieves authentication at the cost of loss in the message throughput.

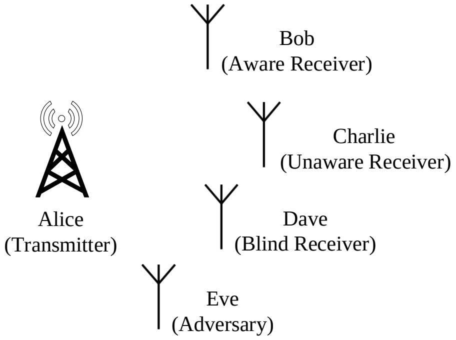


Figure 1: Authentication scenario.

3. TECHNICAL BACKGROUND

3.1 Models and Assumptions

Network Model: We assume that Alice, Bob, Charlie, Dave and Eve are five users which share the same wireless medium, as shown in Figure 1. Alice intends to transmit messages to Bob and Charlie via the wireless medium as per the rules established for dynamic spectrum sharing. Alice utilizes cyclic prefix based orthogonal frequency-division multiplexing (CP-OFDM) for its message signals, but can reconfigure its PHY-layer parameters as per the requirements for the wireless medium [26]. OFDM is an spectrum efficient modulation scheme used in high bit-rate wireless communications, e.g., IEEE 802.11a. Alice conveys the information about these parameters to Bob as well as Charlie so that they can demodulate and decode Alice's message signal. Dave (a.k.a. "blind receiver") represents a regulatory entity that needs to authenticate Alice. Suppose Alice and Dave have agreed on a keyed authentication scheme that enables Dave to blindly authenticate the waveforms that he receives from Alice. For this to work, we must require Alice's radio to embed an authentication signal into her message signal's waveform using the agreed authentication scheme, and Dave must have the capability to extract and decode the authentication signal from the received signal. We assume that tamper-resistance techniques are employed to deter malicious users from circumventing or altering the embedding process carried out by Alice's radio [19, 24, 30]. Bob (a.k.a. "aware receiver") has knowledge about the authentication scheme and can decode the message signal as well as the authentication signal from the received waveforms. Charlie (a.k.a. "unaware receiver") does not know the authentication scheme and cannot authenticate Alice's waveforms, but should be able to demodulate and decode Alice's message signal. Eve represents an adversary, and she is able to launch various types of attacks against Alice, e.g., extracting identity of Alice from the authentication signal, tampering with Alice's message signals, impersonation attacks, and replay attacks. We assume that Eve does not know the key used to generate Alice's authentication signal. More details on Eve are provided in Section 3.2.

Channel Model: Dave receives signals from Alice and Eve with low SINR and significant multipath. Also, there may be simultaneous transmissions from Alice and Eve on the same spectrum band. This means that Dave may receive signals from Alice and Eve at the same time. Hence, Dave should be able to authenticate even when the SINR is below 0 dB. Usually, it is very difficult for a receiver to decode the message signal under such harsh channel conditions [1].

Knowledge at Dave: It is assumed that Dave is aware of the fact that CP-OFDM is employed by Alice and Eve to modulate the message signals. Dave also knows the center frequency and the sampling frequency of their signals; these parameters are typically standardized as part of an air-interface standard [26].

3.2 Performance Criteria

We present a set of performance criteria which can be used to evaluate BTA schemes. We will use them to evaluate FEAT, and compare the performance of FEAT with the prior art.

Overhead: Embedding the authentication signal in the message signal requires applying changes to the message signal itself, and thus incurs some type of PHY-layer overhead when a signal with authentication is compared to a signal without authentication. Examples of such overhead include drop in message throughput, increase in bandwidth, increase in complexity of the transmitter (Alice) and aware receiver (Bob), and degradation of error performance, i.e., bit error rate (BER), of the message signal at the aware receiver.

Transparency: This criterion dictates that a BTA scheme should embed the authentication signal into the message signal such that it enables the blind receiver (Dave) to extract the authentication signal, while at the same time, enables the unaware receiver (Charlie) to recover the message signal *without* requiring the unaware receiver to change its demodulation or decoding procedure. This criterion also quantifies the possible impact of the authentication scheme on the error performance of the message signal at the unaware receiver.

Authentication Rate: The authentication rate is defined as the amount of authentication information (computed in bits) that can be transmitted per second. The authentication signal is embedded by altering the message signal in a certain manner so that the blind receiver can detect the alteration and use it to extract the authentication information. The rate at which the alteration can be made determines the authentication rate. Usually, the message rate (or message throughput) affects the authentication rate.

Robustness to Noise and Fading: This criterion determines the authentication signal's error performance at the aware receiver and the blind receiver. Note that the blind receiver should be able to extract the authentication signal from the received signal even in harsh channel conditions (i.e., very low SNR and significant multipath).

Authentication of Concurrent Transmissions: This criteria considers the feasibility of authentication of multiple transmitters which are transmitting concurrently. This means that if both, Alice and Eve, are transmitting on the same spectrum band at the same time, Dave should be able to uniquely extract the authentication signals corresponding to Alice and Eve from the received signal. The concurrent transmissions hamper the decoding of their authentication signals in two ways—sample-by-sample interference and authentication signature interference. Since an OFDM signal is Gaussian in nature, sample-by-sample interference from samples of one transmitter can be considered Gaussian noise to the other transmitter. The authentication signature interference depends on the BTA scheme utilized to embed the authentication signal into the message signal.

Blind Authentication: The blind receiver is not the intended recipient of the transmitted signal, and hence it does not know the transmission parameters, e.g., frame format, preamble samples, modulation scheme, and pilot samples. However, the blind receiver needs to be able to verify the authentication signal. This criterion takes into account the minimum amount of information needed by Dave to extract the authentication signal from the received signal.

Security: There are four facets of security that need to be considered: *privacy*, *integrity*, *impersonation*, and *replay*. To protect the privacy of Alice from Eve, the BTA scheme should not reveal the identity of Alice through the authentication signal. To ensure integrity, the BTA scheme should prevent Eve from modifying/corrupting Alice's messages without being detected by Dave. To thwart impersonation, the BTA scheme should prevent Eve from creating valid proofs of authenticity for her messages that can be used to impersonate Alice. To thwart replay attacks launched by Eve, Alice's authentication signal should incorporate countermeasures that deter the interception and replay of the authentication signal.

4. DESCRIPTION OF FEAT

We propose a BTA scheme that we refer to as *F*requency offset *E*mbedding for *A*uthenticating *T*ransmitters (FEAT). In the following text, we describe FEAT in the context of the authentication scenario depicted in Figure 1.

Alice embeds the authentication signal in the form of embedded frequency offset (EFO) in each frame of the message signal in the baseband. The embedded signal in the baseband is sent to the oscillator where it gets up-converted and transmitted along with the inherent carrier frequency offset (CFO) due to the inaccurate oscillator. This overall frequency offset does not affect the decoding procedure of the message signal by Bob and Charlie as being the intended receivers, they estimate and correct any frequency offset present in the received signal with the help of the preamble symbols, and the pilot samples. Dave estimates the authentication signal blindly. Further, we discuss in detail the generation of the message signal (MS_a) and authentication signal (AS_a), and embedding of AS_a into MS_a by Alice followed by extraction of the message signal (MS_b)

Table 1: Notations.

MS_a	message signal generated by Alice
AS_a	authentication signal generated by Alice
MS_b	message signal extracted by Bob
AS_b	authentication signal extracted by Bob
MS_c	message signal extracted by Charlie
AS_d	authentication signal extracted by Dave
N_f	size of IFFT used in each OFDM symbol of MS_a
N_c	size of cyclic prefix in each OFDM symbol of MS_a
N_s	number of OFDM symbols in each frame of MS_a
F_s	sampling frequency of MS_a
f_a	the maximum value of embedded frequency offset (EFO)

and authentication signal (AS_b) by Bob, extraction of the message signal (MS_c) by Charlie, extraction of the authentication signal (AS_d) by Dave, and verification of AS_b and AS_d. The notations for the important parameters used in the paper are provided in Table 1.

Generation of MS_a: The message data to be transmitted is assumed to be a sequence of quadrature amplitude modulated (QAM) samples which are statistically independent and identically distributed with zero mean and average power represented by σ_s^2. For each OFDM symbol, Alice generates N_f samples by taking the Inverse Fast Fourier Transform (IFFT) of N_u QAM samples corresponding to N_u non-zero sub-carriers loaded with data or pilot samples. The last N_c samples out of the N_f samples are repeated at the beginning of the N_f samples as the cyclic prefix (CP) to generate an OFDM symbol of $N_o = N_f + N_c$ samples. The message signal is transmitted in frames, and each frame contains $N_s = N_p + N_d$ OFDM symbols, where N_p represents the number of symbols carrying the preamble and N_d represents the symbols carrying data. The samples of a frame is represented by $\{s(n)\}$, where $n = 0, 1, \cdots N_s \cdot N_o - 1$. Figure 2 illustrates the symbol and frame structure of MS_a.

Generation of AS_a: The authentication signal contains three pieces of information: frequency, location and time (represented by F, L and T, respectively) at which the message signal is authorized to be transmitted. A timestamp, represented by TS, is also used to prevent replay of the authentication signal. This information, represented by $A_m = \{TS, F, L, T\}$, is digitally signed using a privacy preserving group signature scheme [3], and the signature of A_m is represented by $sign(A_m)$. Here, we assume that a unique membership certificate has been issued by a designated certificate authority (CA) to each member (including Alice) of the group of secondary users, and Dave has access to all the information available at the designated CA. Hence, one authentication sequence is given by $A_s = \{A_m, sign(A_m)\}$. Each A_s is channel-coded with an error-correcting code (e.g., convolution code), and synchronization and guard bits are appended to generate AS_a of K_a bits.

Embedding of AS_a into MS_a: For embedding the authentication signal into the message signal, we propose a novel scheme called *F*rame *F*requency *M*odulation (FFM) where the frequency offset of each frame of the message signal is modified (modulated) according to the authentication signal. FFM of order M (M-FFM) is represented by a set of M possible frequency offsets corresponding to $M = 2^b$ possible b-bit authentication symbols. Here, an authentication symbol is defined as a set of b authentication bits, and is obtained by using b-bit Gray code. The set of frequency offsets in M-FFM can be represented by $\{f_m\}$ such that

$$f_m = f_a \cdot \left(1 - 2 \cdot \frac{m-1}{M-1}\right), \tag{1}$$

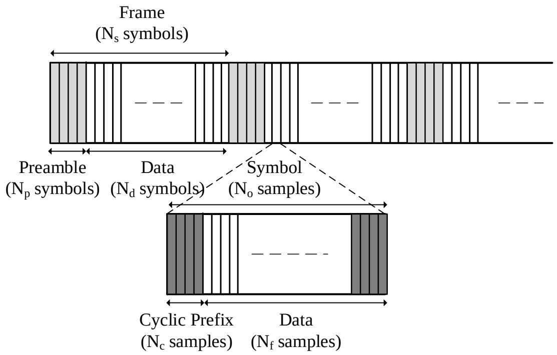
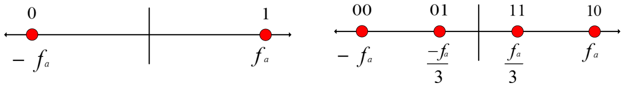


Figure 2: Structure of the OFDM message signal.



(a) M=2

(b) M=4

Figure 3: Mapping of authentication symbols to frequency offsets in M-FFM.

where $m = 1, 2, \cdots, M$, and f_a is the maximum positive frequency offset that can be used to embed the authentication signal into a frame of the message signal. Figures 3a and 3b represent the mapping schemes for 1-bit authentication symbols and 2-bit authentication symbols, respectively. Note that $f_{M-m+1} = -f_m$, for $m = 1, 2, \cdots, \frac{M}{2}$.

In k^{th} frame of the message signal, we embed the authentication symbol, represented by a_k, by embedding a frequency offset, f_k. Hence, for $n = 0, 1 \cdots N_s \cdot N_o - 1$, each sample of a frame of the embedded signal in the baseband is given by $x(n) = s(n) \cdot e^{j2\pi \frac{f_k}{F_s} n}$, where F_s is the sampling frequency. The embedded signal is up-converted to the carrier frequency (F_c) and transmitted. Assuming that CFO due to the inaccurate oscillator at Alice is f_t, the total frequency offset of the transmitted signal is $f_k + f_t$.

Extraction of MS_b, AS_b, and MS_c: After down-converting and sampling the received signal, Bob, with the knowledge of the preamble symbols and the pilot samples, can estimate and correct the frequency offset in each frame and extract the message signal, MS_b. Also, Bob maps the frequency offset in each of the frames to the closest one among $\{f_m\}$, for $m = 1, 2 \cdots M$, given by equation (1) and estimates the authentication signal, AS_b. Charlie, also equipped with the knowledge of the preamble symbols and the pilot samples, can correct the frequency offset in each frame and extract the message signal, MS_c. Since Charlie is not interested in the frequency offsets of the frames of the message signal, the information contained in these frequency offsets is simply discarded by Charlie.

Extraction of AS_d: Dave, the blind receiver, does not have the knowledge about the preamble symbols or the pilots samples inserted in the message signal. Hence, to blindly estimate the transmitted authentication signal, Dave needs to carry out four tasks—signal detection and sampling, symbol synchronization, frame synchronization, and frame frequency estimation.

Signal Detection and Sampling: Since Dave has the knowledge of the center frequency and sampling frequency of the transmitted signal, it down-converts and samples the received signal in the considered frequency band. Assuming a Gaussian channel, Dave observes the received signal with N_r discreet samples which can be represented by $r(n) = e^{j2\pi \frac{f_r}{F_s} n} \cdot x(n) + w(n)$ for $n = 0, 1, \cdots N_r - 1$, where f_r is the frequency offset due to the oscillator at Dave. The additive noise $w(n)$ is assumed to be independent of $x(n)$, and circularly complex Gaussian with zero mean, and σ_w^2 variance. It can be observed that the frequency offset in each frame of the received signal has one constant part, $f_c = f_t + f_r$, and a variable part, f_k, carrying authentication signal.

Symbol Synchronization: Estimation of symbol boundaries includes estimation of the IFFT size ($\widehat{N}_f$), the CP size ($\widehat{N}_c$) and the sample offset ($\widehat{\alpha}$). Dave estimates these three parameters using the sub-optimal maximum likelihood (ML) scheme described in [33] which utilizes the correlation in the received signal induced due to CP. The likelihood function, $\Lambda(\mathbf{r}, \widetilde{N}_f, \widetilde{N}_c, \widetilde{\alpha})$, can be expressed by

$$\begin{aligned}\Lambda \;\; = \;\; & \frac{1}{\widetilde{N}_n \cdot \widetilde{N}_c} \sum_{i=0}^{\widetilde{N}_n - 1} \sum_{l=0}^{\widetilde{N}_c - 1} r^* \left(i \cdot (\widetilde{N}_f + \widetilde{N}_c) + \widetilde{\alpha} + l \right) \\ & \cdot \; r \left(i \cdot (\widetilde{N}_f + \widetilde{N}_c) + \widetilde{N}_f + \widetilde{\alpha} + l \right).\end{aligned}$$

where $r^*(n)$ is the complex conjugate of $r(n)$, and $\widetilde{N}_n = \lfloor (N_r - \widetilde{\alpha})/(\widetilde{N}_f + \widetilde{N}_c) \rfloor$. Here, $\lfloor v \rfloor$ denotes the largest integer less than or equal to v. $\widehat{N}_f$, $\widehat{N}_c$ and $\widehat{\alpha}$ can be estimated as

$$\widehat{N}_f, \widehat{N}_c, \widehat{\alpha} = \underset{\widetilde{N}_f, \widetilde{N}_c, \widetilde{\alpha}}{\operatorname{argmax}} \left| \Lambda \left(\mathbf{r}, \widetilde{N}_f, \widetilde{N}_c, \widetilde{\alpha} \right) \right|.$$

where $|v|$ denotes the absolute value of v. Dave obtains the estimate of the constant part of the frequency offset as

$$\widehat{f}_c = \frac{F_s}{2\pi \widehat{N}_f} \cdot \angle \lambda, \tag{2}$$

where $\lambda = \Lambda(\mathbf{r}, \widehat{N}_f, \widehat{N}_c, \widehat{\alpha})$, and $\angle c$ denotes the polar angle of the complex number c. After symbol synchronization, the received signal is represented by $r_s(n) = r(\widehat{\alpha} + n)$ for $n = 0, 1, \cdots N_r - \widehat{\alpha}$. Note that the perfect symbol synchronization is achieved when $\widehat{N}_f = N_f$, $\widehat{N}_c = N_c$, and $\widehat{\alpha} = \alpha$, where α is the actual sample offset. In this case, the theoretical value of λ can be obtained as in Appendix A.

Frame Synchronization: Estimation of frame boundaries includes estimation of the total number of symbols in a frame ($\widehat{N}_s$), and the symbol offset ($\widehat{\beta}$). Dave estimates these two parameters using the correlation among the preamble symbols of the consecutive frames of the received signal. The likelihood function, $\Psi(\boldsymbol{r_s}, \widetilde{N}_s, \widetilde{\beta})$, can be expressed by

$$\begin{aligned}\Psi \;\; = \;\; & \frac{1}{\widetilde{K}_r \cdot \widehat{N}_o} \sum_{k=0}^{\widetilde{K}_r - 1} \sum_{l=0}^{\widehat{N}_o - 1} r_s^* \left(k \cdot \widetilde{N}_s \cdot \widehat{N}_o + \widetilde{\beta} \cdot \widehat{N}_o + l \right) \\ & \cdot \; r_s \left((k+1) \cdot \widetilde{N}_s \cdot \widehat{N}_o + \widetilde{\beta} \cdot \widehat{N}_o + l \right).\end{aligned}$$

where $\widetilde{K}_r = \lfloor (N_r - \widehat{\alpha} - \widetilde{\beta} \cdot \widehat{N}_o)/(\widetilde{N}_s \cdot \widehat{N}_o) \rfloor$, and $\widehat{N}_o = \widehat{N}_f + \widehat{N}_c$. Hence, $\widehat{N}_s$, and $\widehat{\beta}$ can be estimated as

$$\widehat{N}_s, \widehat{\beta} = \underset{\widetilde{N}_s, \widetilde{\beta}}{\operatorname{argmax}} \left| \Psi \left(\boldsymbol{r_s}, \widetilde{N}_s, \widetilde{\beta} \right) \right|.$$

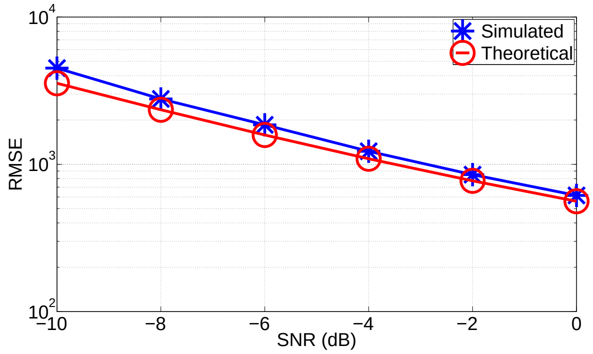


Figure 4: Theoretical CRLB and simulated RMSE in the estimate of $\widehat{f}_k$ at the blind receiver with $M = 2, f_a = 5$ kHz$, N_f = 64, N_c = 16, N_s = 50$.

The number of received frames is obtained as $\widehat{K}_r = \lfloor (N_r - \widehat{\alpha} - \widehat{\beta} \cdot \widehat{N}_o)/(\widehat{N}_s \cdot \widehat{N}_o) \rfloor$. After frame synchronization, the received signal is represented by $r_f(n) = r_s(\widehat{\beta} \cdot \widehat{N}_o + n)$ for $n = 0, 1, \cdots \widehat{K}_r \cdot \widehat{N}_s \cdot \widehat{N}_o - 1$. Note that the perfect frame synchronization is achieved when $\widehat{N}_s = N_s$, and $\widehat{\beta} = \beta$, where β is the actual symbol offset. In this case, the theoretical value of $\psi = \Psi(\boldsymbol{r_s}, \widehat{N}_b, \widehat{\beta})$ can be obtained as in Appendix B.

Frame Frequency Estimation: Having synchronized with the received signal, Dave estimates the correlation between the CP samples and the corresponding data samples in the symbols of each of the frames. For $k = 0, 1, \cdots \widehat{K}_r$, the correlation is given by

$$\begin{aligned}\Phi(k) \;\; = \;\; & \frac{1}{\widehat{N}_s \cdot \widehat{N}_c} \sum_{i=0}^{\widehat{N}_s - 1} \sum_{l=0}^{\widehat{N}_c - 1} r_f^* \left(k \cdot \widehat{N}_s \cdot \widehat{N}_o + i \cdot \widehat{N}_o + l \right) \\ & \cdot \, r_f \left(k \cdot \widehat{N}_s \cdot \widehat{N}_o + i \cdot \widehat{N}_o + \widehat{N}_f + l \right).\end{aligned}$$

Hence, the frequency offset for each frame is estimated as

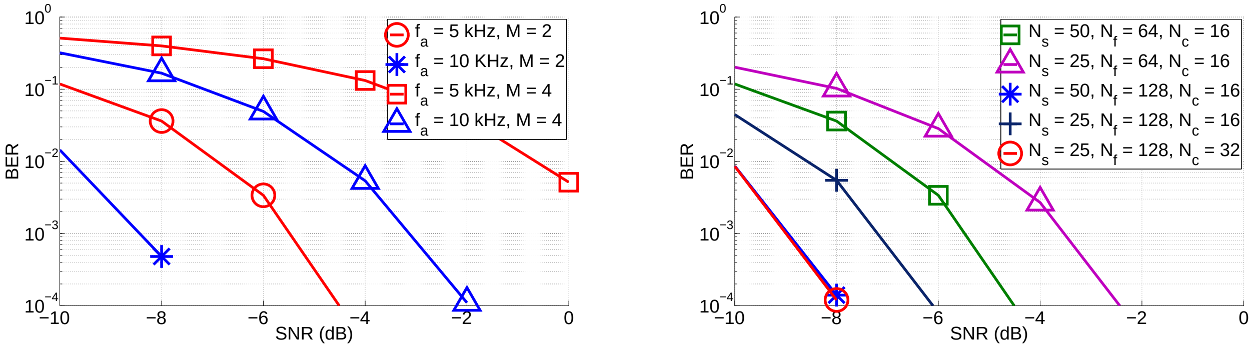
$$\widehat{f}_o(k) = \frac{F_s}{2\pi \widehat{N}_f} \angle \Phi(k), \tag{3}$$

The estimate of frequency offset embedded in the frame through M-FFM is obtained by $\widehat{f}_k = \widehat{f}_o(k) - \widehat{f}_c$, where $\widehat{f}_c$ is obtained from equation (2). Finally, Dave maps $\widehat{f}_k$ to the closest one among $\{f_m\}$, for $m = 1, 2 \cdots M$, given by equation (1), and estimates the authentication symbol of AS_d which is denoted as $\widehat{a}_k$.

Verification of $\boldsymbol{AS_b}$ and $\boldsymbol{AS_d}$: Having estimated the authentication signal, AS_b or AS_d, an estimate of the transmitted authentication sequence, $\widehat{A}_s$, is extracted by removing the synchronization and guard bits, and then carrying out error detection and correction. After extraction of various contents of the authentication signal, their authenticity is verified by utilizing the techniques for group signature verification [3].

5. ANALYSIS

In this section, we evaluate FEAT using Matlab-based simulation results. Specifically, we discuss the error performance of the authentication signal when Dave is the receiver. We also discuss security issues relevant to FEAT.



(a)

(b)

Figure 5: Error performance of AS_d with (a) $N_f = 64, N_c = 16, N_s = 50$, and (b) $M = 2, f_a = 5$ kHz.

5.1 Error Performance

To analyze the error performance of the authentication signal in FEAT, we assume that perfect symbol and frame synchronization have been achieved by Dave. An error in the authentication symbol means $\widehat{a}_k \neq a_k$ which occurs when the mapping of estimated EFO, $\widehat{f}_k$, to the closest one among $\{f_m\}$, for $m = 1, 2 \cdots M$, leads to a different EFO as compared to the transmitted EFO, f_k. This happens when the error in the estimate of the EFO exceeds the magnitude of half of the difference between two consecutive EFOs, i.e., $\left|\widehat{f}_k - f_k\right| > \frac{f_a}{M-1}$. Theoretically, the mean square error (MSE) of the estimate of $\widehat{f}_k$ is lower bounded by the Cramer-Rao Lower-Bound (CRLB) [4, 6]. We obtain the CRLB of the estimate of $\widehat{f}_k$ in FEAT as

$$CRLB = \frac{1}{8\pi^2 N_c} \cdot \left(\frac{1}{\rho^2} + \frac{2}{\rho}\right) \cdot \frac{F_s^2}{N_f^2 N_s}, \qquad (4)$$

where $\rho = \sigma_s^2/\sigma_w^2$, represents the SNR. In Figure 4, we present the root mean square error (RMSE) of the estimate of $\widehat{f}_k$ at different SNRs. Note that the simulated RMSE in FEAT is quite close to its theoretical bound given by square-root of the CRLB. The RMSE vs. SNR curve helps to estimate the error performance of AS_d at a particular SNR given the specific values of different parameters (presented in equation (4)). For instance, in Figure 4, RMSE of the estimate of $\widehat{f}_k$ at SNR of −6 dB is 2 kHz. Hence, in this example, we can estimate the error performance of AS_d when $f_a = 5$ kHz and $M = 2$. However, since the frequency estimate $\widehat{f}_k$ is non-Gaussian in nature, we analyze the effect of different parameters on the error performance of the authentication signal through simulation where the sampling frequency F_s is chosen to be 5 MHz [26].

Effect of ρ: In Figure 5a, when we observe the curve with $f_a = 5$ kHz and $M = 2$, we note that FEAT is quite robust against noise, and the error performance improves (i.e., BER decreases) significantly with increase in SNR, e.g., BER ≈ 0.03 at SNR $= -8$, and BER ≈ 0.003 at SNR $= -6$. This is because each frame of the message signal contains a large number of samples ($N_s \cdot N_o$) which are used to estimate one symbol of the authentication signal.

Effect of f_a: As the largest possible value of EFO, f_a, is increased, BER of AS_d decreases as observed in Figure 5a. This is because by increasing EFO, we effectively account for a larger margin of error in $\widehat{f}_k$. However, there are some limitations on the value of f_a as discussed in Appendix C).

Effect of M: While FEAT with $M = 2$ can carry only 1 authentication bit per frame of the message signal, but FEAT with $M = 4$ can carry 2 authentication bits per frame of the message signal. This means that the authentication rate (defined in Section 3.2) is increased by increasing M. However, as shown in Figure 5a, as M increase, the BER of AS_d increases significantly. This means that M leads to a trade-off between the error performance and the authentication rate of AS_d. This trade-off may play an important role in the cases where the size of data to be communicated between the transmitter and the intended receivers, is small.

In order to authenticate Eve, Dave should receive all the bits from at least one complete authentication sequence. Note that in order to verify the authentication signal, at least one complete authentication sequence should be received by Dave. This means that the estimated number of frames of received signal $\widehat{K}_r$ should be greater than the length of one complete authentication sequence, K_a, i.e., $\widehat{K}_r \geq K_a$. This means that for FEAT with $M = 2$, the number of frames transmitted by Eve should be more than the length of one authentication sequence which is K_a. However, when the size of data is small, the number of frames being transmitted can be significantly small. Hence, the authentication rate needs to be increased at the cost of the error performance to ensure embedding of the authentication bits of at least one authentication sequence. This will allow the transmitter to be authenticated for all its transmission including the burst mode.

Effect of N_f **and** N_c: In Figure 5b, we observe that the BER decreases by increasing N_f and N_c. Recall that N_c (CP size) is the number of samples in each OFDM symbol which are correlated with their corresponding data samples for frequency estimation. This implies that with the increase in N_c, the estimation error in frequency decreases leading to the decrease in BER of AS_d.

Effect of N_s: In Figure 5b, we observe that increasing N_s (frame size) leads to an improvement in error performance, i.e., we achieve lower BER of AS_d. However, larger frame size also leads to lower frame rate which results into lower authentication rate. Hence, we again observe a trade-off between the authentication rate and the error performance of AS_d in terms of N_s. We also observe that when the total number of CP samples in a frame given by $N_c \cdot N_s$ (used for correlation to estimate an authentication symbol) remains the same at a particular value of N_f, the BER of AS_d remains the same.

Moreover, the value of N_s leads to another trade-off between the authentication rate and the transparency, which is one of the main issues that we address through FEAT. We need to use the unit for transmitting one authentication symbol as a frame since we aim to embed the authentication in an absolute transparent manner. In other word, FEAT allows for the presence of unaware receivers (those who do not know about FEAT) in the network, e.g., Charlie. However, if the network environment does not require the condition of absolute transparency (i.e., the network does not have an unaware receiver), we could embed a frequency offset in any number (as low as 1) of OFDM symbols. However, as shown in Figure 5b, decreasing the number of symbols for frequency estimation significantly reduces the error performance. Hence, we can achieve an absolute transparency and high robustness to noise at low authentication rate for AS_d through FEAT, but the approach used in FEAT can also be utilized to achieve any feasible level of the error performance and the authentication rate of AS_d at cost of transparency.

5.2 Security and Robustness of FEAT

In addition to the strength of the cryptographic primitives used to create the authentication signal, the security of a BTA scheme also depends on the contents of the authentication signal and the embedding scheme (i.e., method for embedding the authentication signal into the message signal). We discuss these security issues in the context of FEAT in the following paragraphs.

Privacy: We ensure that Alice's privacy is protected by employing the privacy preserving group signature scheme proposed in [3]. When this scheme is used, Eve or Bob can verify the authenticity of Alice's authentication signal, but more importantly Eve cannot discover Alice's identity through the authentication process. However, the scheme does allow Dave (the regulator) to extract Alice's identity.

Hardware integrity: We assume that tamper resistance techniques are employed to prevent hackers from circumventing the authentication signal embedding mechanism. The tamper-resistant hardware detects any attempt to alter the embedding process [24]. Moreover, before embedding the authentication signal, it ensures that there is no frequency offset present in the message signal. This means that selective addition/removal of the authentication signal is not possible.

Integrity of the Authentication Signal: As mentioned previously, the authentication signal is made up of authentication sequences, and each authentication sequence includes a digital signature. The digital signature ensures the integrity of the authentication signal.

Robustness to Impersonation Attack: In a successful impersonation attack, Eve should be able to create proofs of authenticity for her messages to trick Bob and Dave into thinking that those messages have been created by Alice. Additionally, in the case of spectrum sharing, Eve may attempt to perform location, time, and frequency spoofing in order to gain unauthorized access to spectrum. Therefore, the authentication signal has to be designed to make such exploits infeasible. FEAT ensures that such an attack is readily detected because the authentication signal includes the information about authorized location L, time-frame T, and frequency F along with the certificate C containing the identity of the transmitter.

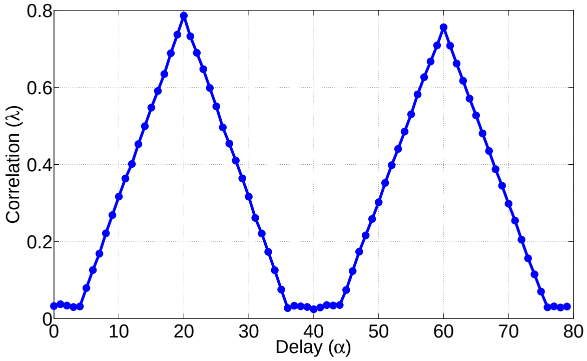


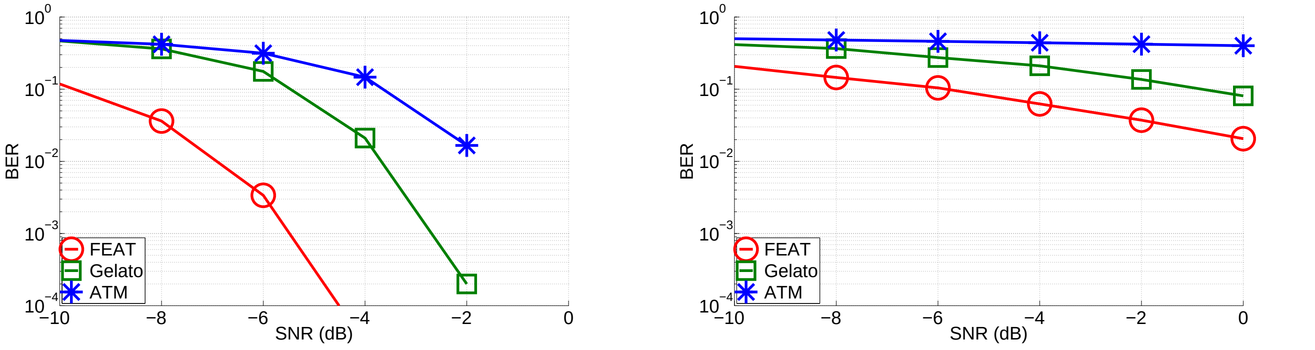
Figure 6: Correlation vs. Delay.

Robustness to Replay Attack: To launch replay attacks, Eve needs to store and re-transmit authentication signals previously transmitted by Alice. However, such replayed transmissions can be readily detected by Bob and Dave since the authentication signal contains a time-stamp TS that cannot be tampered without being detected.

Successful Transmission of the Authentication Signal: We consider the transmission to be successfully authenticated if the transmitted signal contains at least one authentication sequence. Due to the low authentication rate in FEAT, Dave may be unable to authenticate Alice's transmission if the transmitted message signal does not contain enough number of frames to embed a *complete* authentication sequence. Therefore, it is imperative to utilize a short digital signature so that the authentication sequence will be short. For this reason, FEAT utilizes a Elliptic Curve Cryptography (ECC) based signature scheme instead of a conventional digital signature scheme (such as RSA-based signatures) [18]. It is well known that ECC-based cryptosystems can provide an equivalent level of security with a much shorter key when compared with conventional cryptosystems. For instance, ECC with a key size of 163 bits provides an equivalent level of security to the signature when compared with RSA with a key size of 1024.

Robustness to Interference: Eve may also attempt to corrupt Alice's authentication signal through selectively jamming the authentication signal. This type of attack, called obstruction of authentication (OOA) jamming [17], may remain undetected if the transmission power required by Eve to corrupt the authentication signal is small as in the case of PHY-layer authentication schemes based on hierarchical modulation [25]. In these schemes, the message signal is embodied by a high-power constellation while the authentication signal is carried on a low-power constellation. An adversary can emit just enough interference to exploit the power difference between the two constellations to disable the decoding of the authentication signal without disabling the decoding of the message signal.

In FEAT, the frequency offset in an OFDM symbol is estimated using the correlation between CP samples and corresponding data samples of the symbol. Hence, only a subset of samples in an OFDM symbol is utilized for estimation of the frequency offset. This means that the change in the correlation among samples in a symbol other than the samples related to CP samples bear no effect on the ex-



(a) AWGN channel

(b) Rayleigh fading channel

Figure 7: Comparison of error performance of AS_d in FEAT with $f_a = 5$ kHz, Gelato with $N_a = 12$, and ATM with $\theta = \pi/8$, where $N_f = 64, N_c = 16$, and $N_s = 50$. .

traction of the authentication signal in terms of interference to the characteristics used to estimate AS_d, i.e., frequency offset. If the received signal contains *mutually exclusive* subsets of CP samples from multiple transmitters, these subsets can be extracted and utilized to estimate frequency offsets in the signals received from multiple transmitters concurrently. In FEAT, the probability that the set of CP samples of the two signals are mutually exclusive can be calculated to be $p_e = 1 - N_c/N_f$. This means that when we estimate $\lambda = \Lambda(\mathbf{r}, N_f, N_c, \alpha)$ to achieve the symbol synchronization discussed in Section 4, we can observe two independent peaks with probability p_e. To illustrate this property, we consider that Dave receives concurrent signals of equal power from Alice with sample offset $\alpha = 20$ and Eve with sample offset $\alpha = 60$. In this case, Figure 6 shows the amplitude of λ vs. α for known values of N_f and N_c. We can easily detect the start of the symbol of the signals from Alice at sample 20 and Eve at sample 60. When we synchronize with $\alpha = 20$, we can extract the authentication signal of Alice. On the other hand, when we synchronize with $\alpha = 60$, we extract the authentication signal of Eve. Hence, FEAT is extremely robust against interference from an adversary, and hence OOA jamming attack is not possible for Eve without detection. This means that FEAT enables Dave to detect the identity of Eve easily if Eve utilizes even a small power to jam the message or authentication signals from Alice.

6. PERFORMANCE EVALUATION

Based on the performance criteria established in Section 3.2, we evaluate FEAT through comparison with two schemes which represent the existing art of PHY-layer authentication: Authentication Tagging with Modulation (ATM)[25], and Gelato [31].

In FEAT, one bit of the authentication signal is embedded in each frame of the message signal by modifying its frequency offset, i.e., $M = 2$. In ATM, the authentication signal is embedded into the message signal by changing the phase of the QAM message samples. An authentication bit of 1 is embedded by shifting the phase of a QAM sample towards the Q-axis (representing quadrature-phase) by θ. An authentication bit of 0 is embedded by shifting the phase towards the I-axis (representing in-phase) by θ. For the sake of comparison, we embed one authentication bit per frame which means that the phase of all the QAM samples in a frame are shifted in only one direction corresponding to the authentication bit to be embedded. In Gelato, the authentication signal is embedded into the transmitted OFDM signal by repeating N_a QAM samples over the sub-carriers to generate a cyclo-stationary signature. For the sake of comparison, we embed one authentication bit per frame which means that all the OFDM symbols in a frame carry the same signature. An authentication bit of 1 is embedded by repeating the QAM samples from the first N_a sub-carriers to the next N_a sub-carriers. An authentication bit of 0 is embedded by repeating the QAM samples from the last N_a sub-carriers to the previous N_a sub-carriers.

Overhead: In FEAT, Alice embeds the frequency offset into the message signal through simple vector multiplication over each frame. This means that no significant computation overhead is incurred to include FEAT at Alice. Also, there are no power and message throughput overheads at Alice. In general, an intended receiver utilizes the preamble symbols added at the beginning of each frame, and the pilot samples in each symbol of the received signal to estimate and correct the frequency offset. In effect, no change is required in the message decoding procedure at Bob, and the embedding of the authentication signal has no effect on the error performance of the message signal at Bob. Moreover, no significant overhead is incurred at Bob to use those frequency estimates to estimate the authentication signal. In ATM, no significant computational overhead is needed to embed authentication at Alice along with no power and message throughput overheads. Bob using its pilot symbols can estimate and remove the phase offset and hence, there is no effect on the error performance of the message signal at Bob. In Gelato, the computation overhead to embed the authentication signal at Alice is non-significant. However, since N_a out of N_u useful sub-carriers are loaded with redundant data samples, the message data-rate is reduced by $\frac{N_a}{N_u} \cdot 100$ %. For instance, with $N_a = 6$ and $N_u = 48$, Alice loses 12.5% of its data-rate. Although Bob does not suffer in terms of the error performance of the message signal, the message decoding procedure needs to be modified to discard the data samples at the redundant sub-carriers.

Transparency: In the existing standards describing PHY-layer specifications, there is a significant margin allowed for the carrier frequency offset (CFO) in the message signals due to inaccurate oscillators at the transmitters and the receivers. For instance, as per IEEE 802.11g [2], the absolute value of CFO due to an inaccurate oscillator should be less

Table 2: Comparison of FEAT and prior art.

Scheme	Overhead	Transparency	Authentication Rate	Robustness to Noise & Fading	Authentication of Concurrent TX	Blind Authentication
[13]	Low	Good	Low	Medium	Good	Poor
[17]	Low	Poor	High	Medium	Poor	Poor
[21]	Low	Poor	Low	Good	Good	Poor
[25]	High	Good	High	Poor	Poor	Poor
[31]	High	Poor	Low	Good	Poor	Medium
[32]	High	Good	High	Poor	Poor	Poor
FEAT	Low	Good	Low	Good	Good	Good

than 25 ppm of the carrier frequency. This means that for transmitted signals at 2.4 GHz, a frequency offset of ±60 kHz is allowed. Also, the preamble structure (inserted in each frame) ensures that a frequency offset of $2 \cdot 60$ kHz = 120 kHz (considering the margin for the oscillator at receiver) can be tolerated by each frame of the message signal. In FEAT, Charlie utilizes the preamble symbols added at the beginning of each frame, and the pilot samples in each symbol of the message signal to estimate and remove the frequency offset. Hence, there is no effect on the error performance of the message signal at Charlie. In ATM, the phase offset can be estimated using the pilot symbols and hence there is no effect on the error performance of the message signal at Charlie. In Gelato, Charlie can demodulate the message signal, but the demodulated signal would not make sense for Charlie since it being the unaware of the presence of the authentication scheme does not know the presence of the repetition of QAM message samples on some of the sub-carriers. Hence, unlike FEAT and ATM, Gelato is not transparent with the unaware receiver.

Authentication Rate: By design, in FEAT, ATM as well as Gelato, one bit of authentication signal is embedded into each frame of the message signal. Hence, the authentication rate is equal to the frame rate of the message signal.

Robustness to Noise and Fading: We simulate FEAT, ATM and Gelato using Matlab to estimate their error performance at different SNR. With AWGN channel, FEAT performs significantly better than ATM and Gelato as shown in Figure 7a. For instance, at SNR of -6 dB, the BER in FEAT is 0.003 as compared to 0.2 in Gelato, and 0.3 in ATM. We also present the error performance of the authentication signal in a Rayleigh fading channel with 200 Hz doppler shift in Figure 7b. Recall that since Dave does not have the information of the pilot signals used by Alice, it is not possible for it to counter the channel effects generated due to multipath. Hence, in Figure 7b, we observe that the BER in ATM is close to 0.5. However, even in these channel conditions, FEAT achieves sufficient BER so that the authentication sequence can be recovered using the error correcting code.

Authentication of Concurrent Transmissions (TX): FEAT is robust to interference as discussed in Section 5.2. Hence, in presence of concurrent transmissions from Alice and Eve, each of the two can be authenticated at Dave. However, neither Gelato nor ATM can be used to extract the authentication signal from the received signal corrupted by interference from the similar type of signal. In ATM, the phase offsets in the received samples containing the authentication signals from Alice and Eve cannot be separated. In Gelato, in the absence of interference, each OFDM symbol contains one signature. But, when the received signal contains signals from multiple transmitters, multiple cyclostationary signatures can be observed in the received OFDM symbol, and there is no way to extract the authentication signature corresponding to a specific transmitter.

Blind Authentication: At a receiver, after down converting and sampling the received signal, time and frequency synchronization are the first steps to be performed to extract the message signal. A significant amount of work has been done in the field of blind (non-data-aided) parameter estimation, e.g., time and frequency offset estimation, for OFDM signals [12, 15, 23, 33]. Also, it has been shown in [14] that carrier frequency offset (CFO) is an intrinsic characteristic of a transmitter, and it can be used for authentication. Note that the actual CFO of an oscillator in a transmitter usually remains close to a constant value although some variations may be caused due to long life-span, temperature, and other environmental factors. Moreover, it has been shown in [21] that an authentication signal can be extrinsically embedded into the pilot symbols of the message signal in the form of frequency offsets. However, the blind receiver cannot utilize this scheme due to lack of knowledge of the pilot symbols. In FEAT, the authentication signal is embedded into each frame of the message signal using frequency offset such that it can be extracted using the techniques of blind parameter estimation. However, Dave (the blind receiver) needs to know the center frequency and the sampling frequency of the transmitted signal to authenticate the received signal. Gelato with the sample and symbol synchronization mechanism (proposed in this paper) can be used with the same knowledge as needed in FEAT. In ATM, other than the center frequency and the sampling frequency, the blind receiver also needs to know the modulation being used by the transmitter. In general, the center frequency and the sampling frequency depend on the standard to be utilized to set up the network [26] and hence, their knowledge can be considered to be available a priory. However, modulation schemes depend on the channel conditions between the transmitter and the intended receivers and hence, it is subject to change. This means that FEAT and Gelato enable blind authentication, but ATM does not.

Security: Considering that the contents and the length of the authentication signal in the three schemes are same, we compare the robustness of the scheme in the case where Eve may attempt to corrupt the authentication signal transmitted by Alice, i.e. OOA jamming attack. Since FEAT is the most robust scheme against interference, it is also the most robust scheme against OOA jamming attack. Moreover, since FEAT is the most robust scheme against noise as shown in Figure 7a, it is also the most secure scheme against incessant jamming.

Table 2 provides a qualitative comparison of FEAT and the state of the art in PHY-layer authentication, including Gelato and ATM, in terms of the performance criteria dis-

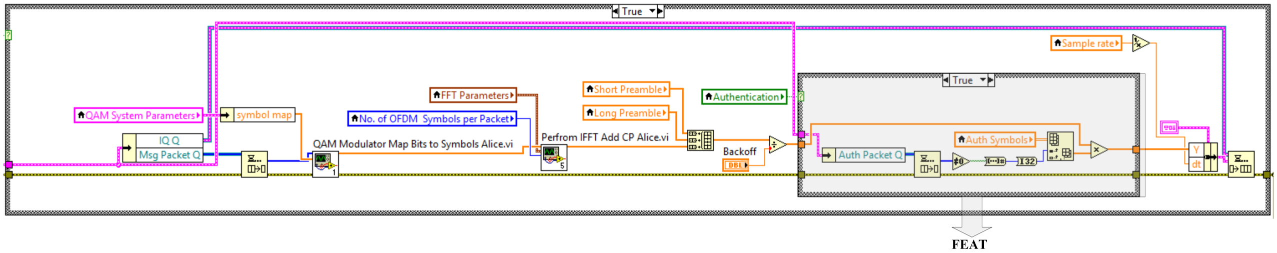


Figure 8: LabVIEW VI illustrating the implementation of FEAT.

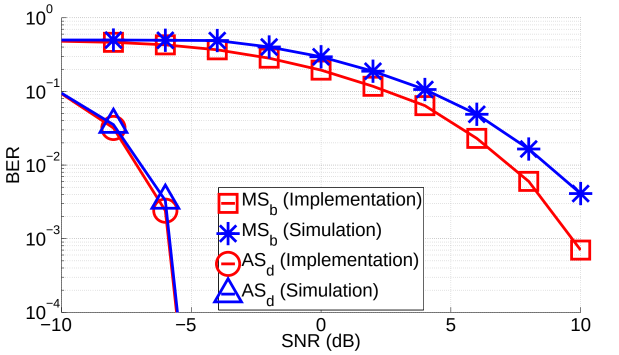


Figure 9: Comparison of the error performance of MS_b and AS_d in implementation and simulation.

cussed in Section 3.2. Note that FEAT outperforms the prior art in every respect except for authentication rate.

7. EXPERIMENTAL VALIDATION

We conducted a number of experiments using an implementation of FEAT. In the experiments, we used three Universal Software Radio Peripheral (USRP) radios, one each for Alice (transmitter), Bob (aware receiver), and Dave (blind receiver). National Instruments' LabVIEW is utilized as the system-design platform to configure the three USRPs. Alice and Bob use IEEE 802.11af [26] to communicate with each other. Alice also embeds an authentication signal using FEAT so that Dave is able to authenticate Alice.

Model and Assumptions: The three radios are placed in an indoor environment in such a way that the distance between any two radios is approximately 1 meter. The distances between the radios are limited by the fact that all the radios need to be connected to the computer running the LabVIEW application through network cables. Hence, to obtain a wide range of SNR values (from −10 dB to 10 dB), we add Gaussian noise at Bob and Dave in addition to the channel-induced noise added to the signal transmitted over-the-air. Here, we assume that adding Gaussian noise after receiving the signal is equivalent to increasing the distance between the transmitter and the receivers.

Design: We utilize the following PHY-layer parameters—the center frequency $F_c = 915$ MHz, the sampling frequency $F_s = 1$ MHz, IFFT size $N_f = 64$, the CP size $N_c = 16$, the number of useful sub-carriers $N_u = 52$ (48 for data samples and 4 for pilot samples), and the number of symbols in each frame $N_s = 50$. The preamble consists of four symbols (i.e., $N_p = 4$)—two symbols each for short and long preamble sequence. We utilize quadrature amplitude shift keying (QPSK) as the modulation scheme for the message signal. The data contained in the message signal consists of a time-stamp and a text, and is transmitted without any error correction coding. The authentication signal consists of a set of random bits for synchronization, a time-stamp and a text data without any error correction coding. It is embedded into the message signal using FEAT with $M = 2$ and $f_a = 1$ kHz. Since Bob is the receiver with the knowledge of all the PHY-layer parameters, he demodulates and decodes the received signal. The received message signal is synchronized using a time-stamp, and compared with the transmitted message signal to calculate the BER of the message signal.

Dave extracts the authentication signal by synchronizing with the received signal which is processed in blocks of 1 million samples (i.e., the number of samples received per second). Since the processing overhead needed to achieve synchronization is quite high, the parameters such as IFFT size ($\widehat{N}_f$), CP size ($\widehat{N}_c$), and frame size ($\widehat{N}_s$) are estimated only for the first block of the received samples. During the experiments, we noticed that the value of sample offset ($\widehat{\alpha}$) changes slowly because of the clock mismatch between the hardware platforms. Hence, the sample offset ($\widehat{\alpha}$) and symbol offset ($\widehat{\beta}$) are estimated for each block of received samples. The received authentication signal is synchronized using the synchronization bits, and compared with the transmitted authentication signal to calculate the BER of the authentication signal.

Figure 8 shows the LabVIEW VI of Alice illustrating the various steps needed to embed an authentication symbol into a frame of the message signal. The message signal is generated by creating conventional OFDM signals—mapping the message bits to QAM symbols, performing IFFT, adding CP, and adding preamble symbols. To embed the authentication signal, the message signal is multiplied sample-by-sample with a vector which embeds the frequency offset; this process is carried out by the blocks enclosed in the gray box shown in Figure 8.

Results: Figure 9 shows the error performance of the message signal at Bob (MS_b) and the authentication signal at Dave (AS_d). The error performance from Matlab simulations with the same PHY-layer parameters are also presented as a benchmark. We observe that the error performance of the USRP implementation is quite close to the error performance obtained from the simulations in the case of the authentication signal. However, the same is not true for the message signal. This result can be explained by recognizing the fact that the channel noise is Gaussian in the simulations, whereas the channel noise is not truly Gaussian in the over-the-air experiments when the message signal is decoded sample-by-sample. However, when an authentication symbol is estimated by correlating the CP samples of length $N_c \cdot N_s = 800$ with their corresponding data samples of equal length, then the channel noise added in the over-the-air experiments can be considered to be Gaussian for the authentication signal as a result of the central limit theorem.

8. CONCLUSION

In this paper, we have defined the BTA problem, and proposed a novel scheme called FEAT that satisfies all of the required criteria of the BTA problem. Through analytical analysis, simulations, and experiments with an USRP-based implementation, we have shown that FEAT is a viable approach for authenticating transmitters even in very harsh channel environments, where the SINR is low and the multipath fading is significant.

9. ACKNOWLEDGMENTS

This work was partially sponsored by NSF through grants CNS-1314598 and IIP-1265886; by the Beijing Natural Science Foundation under grant 4143062; and by the industry affiliates of the Broadband Wireless Access & Applications Center and the Wireless @ Virginia Tech group.

10. REFERENCES

[1] Design considerations for minimum SNR. `http://www.cisco.com/en/US/docs/wireless/technology/mesh/7.3/design/guide/Mesh_chapter_011.pdf`. Accessed: May 15, 2014.

[2] Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. *IEEE Standard 802.11-2012.*

[3] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A practical and provably secure coalition-resistant group signature scheme. In *Advances in Cryptology - CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 255–270. Springer Berlin Heidelberg, 2000.

[4] C. R. N. Athaudage and K. Sathananthan. Cramer-Rao lower bound on frequency offset estimation error in OFDM systems with timing error feedback compensation. In *Fifth International Conference on Information, Communications and Signal Processing*, pages 1231–1235, 2005.

[5] V. Brik, S. Banerjee, M. Gruteser, and S. Oh. Wireless device identification with radiometric signatures. In *Proc. ACM MobiCom*, pages 116–127, 2008.

[6] M.-H. Cheng and C.-C. Chou. Maximum-likelihood estimation of frequency and time offsets in OFDM systems with multiple sets of identical data. *Signal Processing, IEEE Transactions on*, 54(7):2848–2852, July 2006.

[7] I. Cox, M. Miller, and A. McKellips. Watermarking as communication with side information. *Proc. IEEE*, 87(7):1127–1141, July 1999.

[8] B. Danev and S. Capkun. Transient-based identification of wireless sensor nodes. In *Int. Conf. Inform. Process. Sensor Netw.*, pages 25–36, Apr. 2009.

[9] B. Danev, H. Luecken, S. Čapkun, and K. Defrawy. Attacks on physical-layer identification. In *ACM WiSec*, pages 89–98, 2010.

[10] S. Dudley, W. Headley, M. Lichtman, E. Imana, X. Ma, M. Abdelbar, A. Padaki, A. Ullah, M. Sohul, T. Yang, and J. Reed. Practical issues for spectrum management with cognitive radios. *Proceedings of the IEEE*, 102(3):242–264, March 2014.

[11] C. Fei, D. Kundur, and R. Kwong. Analysis and design of secure watermark-based authentication systems. *IEEE Trans. Inform. Forensics Security*, 1(1):43–55, Mar. 2006.

[12] T. Fusco and M. Tanda. Blind synchronization for OFDM systems in multipath channels. *IEEE Trans. Wireless Commun.*, 8(3):1340–1348, 2009.

[13] N. Goergen, T. Clancy, and T. Newman. Physical layer authentication watermarks through synthetic channel emulation. In *IEEE Symp. New Frontiers Dynamic Spectrum*, pages 1–7, Apr. 2010.

[14] W. Hou, X. Wang, and J.-Y. Chouinard. Physical layer authentication in OFDM systems based on hypothesis testing of CFO estimates. In *IEEE ICC*, 2012.

[15] H. Ishii and G. W. Wornell. OFDM blind parameter identification in cognitive radios. In *IEEE 16th Int. Symp. Personal, Indoor and Mobile Radio Commun.*, volume 1, pages 700–705, Sept 2005.

[16] J. Kleider, S. Gifford, S. Chuprun, and B. Fette. Radio frequency watermarking for OFDM wireless networks. In *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Process.*, volume 5, pages 397–400, May 2004.

[17] V. Kumar, J.-M. Park, T. Clancy, and K. Bian. PHY-layer authentication by introducing controlled inter symbol interference. In *IEEE CNS*, pages 10–18, 2013.

[18] K. Lauter. The advantages of elliptic curve cryptography for wireless security. *IEEE Wireless Communications*, page 63, 2004.

[19] C. Li, A. Raghunathan, and N. Jha. An architecture for secure software defined radio. In *Design, Automation and Test in Europe (DATE)*, pages 448–453, 2009.

[20] Y. Liu, P. Ning, and H. Dai. Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures. In *IEEE Symp. Security and Privacy*, pages 286–301, May 2010.

[21] R. Miller and W. Trappe. Short paper: ACE: authenticating the channel estimation process in wireless communication systems. In *Proc. ACM WiSec*, pages 91–96, 2011.

[22] J.-M. Park, J. Reed, A. Beex, T. Clancy, V. Kumar, and B. Bahrak. Security and enforcement in spectrum sharing. *Proc. IEEE*, 102(3):270–281, March 2014.

[23] A. Punchihewa, V. Bhargava, and C. Despins. Blind estimation of OFDM parameters in cognitive radio networks. *IEEE Trans. Wireless Commun.*, 10(3):733–738, March 2011.

[24] N. Smith, D. Johnston, G. Cox, and A. Shaliv. Device, method, and system for secure trust anchor provisioning and protection using tamper-resistant hardware, April 2014. US Patent App. 13/631,562.

[25] X. Tan, K. Borle, W. Du, and B. Chen. Cryptographic link signatures for spectrum usage authentication in cognitive radio. In *Proc. ACM WiSec*, pages 79–90, June 2011.

[26] J.-S. Um, S.-H. Hwang, and B.-J. Jeong. A comparison of PHY layer on the Ecma-392 and IEEE 802.11af standards. In *CROWNCOM, 7th Int. ICST Conf. on*, pages 313–319, 2012.

[27] O. Ureten and N. Serinken. Wireless security through RF fingerprinting. *Canadian J. Electr. Comput. Eng.*, 32(1):27–33, 2007.

[28] X. Wang, Y. Wu, and B. Caron. Transmitter identification using embedded pseudo random sequences. *IEEE Trans. Broadcast.*, 50:244–252, Sep. 2004.

[29] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe. Using the physical layer for wireless authentication in time-variant channels. *IEEE Trans. Wireless Commun.*, 7(7):2571–2579, July 2008.

[30] S. Xiao, J. Park, and Y. Ye. Tamper resistance for software defined radio software. In *COMPSAC*, pages 383–391, 2009.

[31] L. Yang, Z. Zhang, B. Y. Zhao, C. Kruegel, and H. Zheng. Enforcing dynamic spectrum access with spectrum permits. In *Proc. ACM MobiHoc*, pages 195–204, 2012.

[32] P. Yu, J. Baras, and B. Sadler. Physical-layer authentication. *IEEE Trans. Inf. Forensics Security*, 3(1):38–51, Mar. 2008.

[33] T. Yucek and H. Arslan. OFDM signal identification and transmission parameter estimation for cognitive radio applications. In *IEEE GlobeCom*, pages 4056–4060, 2007.

APPENDIX

A. SYMBOL SYNCHRONIZATION (λ)

For very large N_r, when no authentication signal is embedded, $\lambda = \sigma_s^2 \cdot e^{j\epsilon f_c}$, where f_c is the constant frequency offset, and $\epsilon = 2\pi N_f/F_s$ [33]. When FEAT is utilized to embed the authentication signal, we could define M sets of frames with the frequency offsets $f_c + f_k$, where $f_c = f_t + f_r$, and $f_k = f_m$ for $m = 1, 2, \cdots, M$. Assuming that the authentication symbols are statistically independent and identically distributed, λ is given by

$$\begin{aligned}
\lambda &= \frac{\sigma_s^2}{M} \cdot \sum_{m=1}^{M} e^{j\epsilon(f_c+f_m)} \\
&= \frac{\sigma_s^2}{M} \cdot e^{j\epsilon f_c} \cdot \left(\sum_{m=1}^{M/2} e^{j\epsilon f_m} + \sum_{m=M/2+1}^{M} e^{j\epsilon f_m} \right) \\
&= \frac{\sigma_s^2}{M} \cdot e^{j\epsilon f_c} \cdot \left(\sum_{m=1}^{M/2} e^{j\epsilon f_m} + \sum_{m=1}^{M/2} e^{j\epsilon f_{M-m+1}} \right) \\
&= \frac{\sigma_s^2}{M} \cdot e^{j\epsilon f_c} \cdot \left(\sum_{m=1}^{M/2} e^{j\epsilon f_m} + \sum_{m=1}^{M/2} e^{-j\epsilon f_m} \right) \\
&= \frac{2\sigma_s^2}{M} \cdot e^{j\epsilon f_c} \cdot \sum_{m=1}^{M/2} \cos \epsilon f_m \\
&= \frac{2\sigma_s^2}{M} \cdot e^{j\epsilon f_c} \cdot \sum_{m=1}^{M/2} \cos \epsilon f_a \left(1 - 2 \cdot \frac{m-1}{M-1} \right). \qquad (5)
\end{aligned}$$

B. FRAME SYNCHRONIZATION (ψ)

For very large N_r, when no authentication signal is embedded, each frame has the same frequency offset and hence the relative frequency offset between consecutive frames is zero which means $\psi = \sigma_s^2$. When FEAT is utilized to embed the authentication signal, we could define M^2 sets of relative frequency offsets between two consecutive frames—M sets of frequency offset 0, $M-1$ sets of frequency offset $+\frac{2f_a}{M-1}$, and so on. Hence, ψ is given by

$$\begin{aligned}
\psi &= \frac{\sigma_s^2}{M^2} \cdot M + \frac{\sigma_s^2}{M^2} \sum_{m=1}^{M-1} \frac{M-m}{N_o} \sum_{l=0}^{N_o-1} e^{j2\pi \frac{2mf_a}{(M-1)F_s} l} \\
&\quad + \frac{\sigma_s^2}{M^2} \sum_{m=1}^{M-1} \frac{M-m}{N_o} \sum_{l=0}^{N_o-1} e^{j2\pi \frac{-2mf_a}{(M-1)F_s} l} \\
&= \frac{\sigma_s^2}{M^2} \cdot \left(M + \sum_{m=1}^{M-1} \frac{M-m}{N_o} \sum_{l=0}^{N_o-1} 2\cos 2\pi \frac{2mf_a}{(M-1)F_s} l \right) \\
&\approx \frac{\sigma_s^2}{M^2} \cdot \left(M + \sum_{m=1}^{M-1} \frac{(M-m) \cdot \sin 4\pi \frac{mf_a}{(M-1)F_s} N_o}{N_o \cdot \sin 2\pi \frac{f_a}{F_s}} \right). \qquad (6)
\end{aligned}$$

C. THEORETICAL LIMITS ON EFO (f_a)

In the presence of very large number of samples present for synchronization, the performance of the proposed synchronization algorithm depends mainly on f_a. From equation (5), we note that the absolute value of λ decreases by increasing f_a. This means that the probability of detection of the peak of Λ decreases by increasing f_a. Again, from equation (6), we observe that the absolute value of ψ decreases by increasing f_a. This means that the probability of detection of the peak of Ψ decreases by increasing f_a. On the other hand, by increasing f_a, we can enhance the error performance of FEAT as shown in Section 5. Therefore, we need to find theoretical bounds on f_a.

From equation (5), for $M = 2$, λ is given by

$$\lambda = \sigma_s^2 \cdot e^{j\epsilon f_c} \cdot \cos \epsilon f_a.$$

where $\epsilon = 2\pi N_f/F_s$. Hence, the maximum value of λ is achieved when $f_a = 0$. This means that the synchronization is achieved with highest accuracy when no authentication signal is embedded into the message signal. On the other hand, when $f_a = \pi/(2\epsilon) = F_s/(4\pi N_f)$, the absolute value of λ is 0. This means that it is difficult to achieve the synchronization if the EFO is close to $F_s/(4\pi N_f)$. Hence, to achieve sufficient level of robustness for synchronization of the received signal and for extraction of the authentication signal, f_a needs to be sufficiently larger than 0, but sufficiently smaller than $F_s/(4\pi N_f)$.

Moreover, in the existing standards describing PHY-layer specifications, there is a limited margin allowed for the carrier frequency offset (CFO) in the message signals due to inaccurate oscillators at the transmitters and the receivers. For instance, as per IEEE 802.11g [2], the absolute value of CFO due to an inaccurate oscillator should be less than 25 ppm of the carrier frequency. Hence, we need to ensure that $f_t + f_a \leq F_o$, where F_o is the allowed frequency offset as per the standard.