PHY-Layer Authentication Using Duobinary Signaling for Spectrum Enforcement

Vireshwar Kumar, *Member, IEEE*, Jung-Min (Jerry) Park, *Senior Member, IEEE*, and Kaigui Bian, *Member, IEEE*

***Abstract*— Spectrum security and enforcement is one of the major challenges that need to be addressed before spectrum sharing technologies can be adopted widely. The problem of rogue transmitters is a major threat to the viability of spectrum sharing. One approach for deterring rogue transmissions is to enable receivers to authenticate or uniquely identify transmitters. Although cryptographic mechanisms at the higher layers have been widely used to authenticate transmitters, the ability to authenticate transmitters at the physical (PHY) layer has a number of key advantages over higher layer approaches. In existing schemes, the authentication signal is added to the message signal in such a way that the authentication signal appears as noise to the message signal and vice versa. Hence, existing schemes are constrained by a fundamental tradeoff between the message signal's signal-to-noise ratio (SNR) and the authentication signal's SNR. In this paper, we extend the precoded duobinary signaling (P-DS) technique to devise a new PHY-layer authentication scheme called P-DS for authentication (P-DSA). P-DSA exploits the redundancy introduced by P-DS to embed the authentication signal into the message signal. P-DSA is not constrained by the aforementioned tradeoff between the message and authentication signals. Our results show that P-DSA improves the detection performance compared with the prior art without sacrificing message throughput or increasing transmission power.**

***Index Terms*— PHY-layer authentication, spectrum sharing, spectrum enforcement, duobinary signaling.**

I. Introduction

IT IS widely believed that a transition from the legacy "command-and-control" spectrum regulatory model—where spectrum is parceled and allocated to specific stakeholders and applications—to a more flexible model of *dynamic spectrum sharing* is necessary to achieve more efficient spectrum usage. In dynamic spectrum sharing, secondary users (SUs) opportunistically utilize fallow spectrum that is not in use by primary (a.k.a incumbent) users (PUs), and they follow a set of prescribed rules or regulations to protect the PUs from interference. One of the critical challenges that needs to be addressed to realize the spectrum sharing model is the development of technologies for *spectrum enforcement and security* [2]. Spectrum enforcement and security is emerging as an especially critical issue because of the recent calls in the U.S. for sharing of federal government spectrum (including military spectrum) with non-government systems [3]–[5]. In such spectrum sharing scenarios, it is critical for a regulatory enforcement authority (such as the FCC) to be able to identify and authenticate rogue transmitters. Here, rogue transmitters denote SUs that violate prescribed spectrum access rules.

While cryptographic mechanisms at the higher layers have been widely used to authenticate transmitters, the ability to authenticate and/or uniquely identify transmitters at the PHY-layer has a number of key advantages over higher-layer approaches. A PHY-layer scheme enables a receiver to quickly distinguish between legitimate and rogue transmitters without having to complete higher-layer processing, which is unnecessary and wasteful since we do not need to authenticate the data contained in the messages, but instead authenticate the transmitter or its waveform. PHY-layer authentication is especially useful in heterogeneous coexistence environments, where incompatible systems (i.e., systems with different protocol stacks) may not be able to decode each others' higher-layer signaling—e.g., IEEE 802.22 and 802.11af systems coexisting in TV white space. Note that the objective of PHY-layer authentication is to uniquely identify the transmitter that has transmitted a given waveform by authenticating the waveform itself, which is different from authenticating the message carried by the waveform. The latter is handled at the application layer.

For a PHY-layer authentication scheme to be a viable approach for spectrum 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—into the message signal (which contains the data that the transmitter wants to send). In most of the existing schemes [6]–[8], the authentication signal is added to the message signal in such a way that the authentication signal appears as noise to the message signal and vice versa—we refer to this approach as the "*blind signal superposition*" method [9]. In such an approach, the authentication signal is fully present when the message signal is decoded, thus resulting in decreased

Manuscript received February 24, 2015; revised August 26, 2015 and October 23, 2015; accepted December 28, 2015. Date of publication January 12, 2016; date of current version February 24, 2016. This work was supported in part by the National Science Foundation under Grant 1265886, Grant 1314598, Grant 1431244, and Grant 1547241, in part by the National Natural Science Foundation of China under Grant 61572051, in part by Motorola Solutions, and in part by the Industrial Affiliates of the Broadband Wireless Access and Applications Center and the Wireless@Virginia Tech Group. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Negar Kiyavash.

V. Kumar and J.-M. Park are with the Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA 24061 USA (e-mail: viresh@vt.edu; jungmin@vt.edu).

K. Bian is with the School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China (e-mail: bkg@pku.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2016.2516904

signal-to-noise ratio (SNR) for the message signal, assuming that the transmission power has not been increased to embed the authentication signal. Hence, there is a fundamental tradeoff between the message signal's SNR and the authentication signal's SNR—it is impossible to improve the former without worsening the latter and vice versa. This means that the degradation in the message signal's SNR is significant when the authentication signal's SNR is increased to a level sufficient for authenticating the received signal at the receiver [10].

Precoded Duobinary Signaling (P-DS) is a waveform shaping technique that has been traditionally used to increase the bandwidth efficiency of the message signal [11], [12]. In P-DS, a controlled amount of inter symbol interference (ISI) is introduced in the transmitted message signal, and the detection procedure at the receiver cancels out the ISI. The proposed PHY-layer authentication scheme, called *P-DS for Authentication* (P-DSA), exploits the inherent redundancy introduced by P-DS to embed the authentication signal into the message signal without being constrained by the aforementioned tradeoff.

Further, the design of the authentication signals proposed in the existing PHY-layer authentication schemes [6], [9], [13] for spectrum enforcement, pose a potentially serious threat to the privacy of the transmitters. In these schemes, the authentication signal contains the unencrypted identity of the transmitter, and is transmitted over-the-air at the PHY-layer. This means that any RF receiver with the knowledge of the authentication embedding and extraction processes can demodulate the raw bits of the authentication signal. Hence, the authentication signal can be exploited by eavesdroppers to extract the identity of the transmitters, and monitor or track their transmission behavior, e.g., areas of operation, times of operation, etc. Similar privacy concerns arise in vehicular communication applications [14], [15]. In this paper, we propose the design of the authentication signal that preserves the privacy of the transmitters. The proposed design also enables an enforcement entity or an authorized receiver to extract the identity of the transmitters from the received authentication signals.

The main contributions of this paper are summarized below.

- We propose P-DSA, which is one of the first PHY-layer authentication schemes that do not suffer from the drawbacks of the blind signal superposition approach.
- We propose a comprehensive set of performance criteria that can be used to evaluate and compare existing PHY-layer authentication schemes, both qualitatively and quantitatively. Our results indicate that P-DSA outperforms the prior art in terms of these performance criteria.
- The proposed scheme, P-DSA, is complemented with a privacy preserving design of the authentication signal.
- We implement P-DSA on Universal Software Radio Peripheral (USRP) radio boards, and verify the validity of the simulation results through indoor experiments.

The rest of the paper is organized as follows. Section II provides the related work. We describe the problem in Section III, and review the background on P-DS in Section IV. We describe the proposed PHY-layer authentication scheme, P-DSA, and analyze it in Sections V. We establish the performance criteria of a PHY-layer authentication scheme and evaluate our scheme through comparison with the prior art in Section VI. We discuss privacy-preserving design of the authentication signal in Section VII, and evaluate its characteristics in Section VIII. We discuss a prototype implementation of the proposed scheme in Section IX. Section X concludes the paper.

II. Related Work

In essence, PHY-layer authentication [6]–[9], [13], [16]–[19] is closely related to or is equivalent to radio frequency (RF) fingerprinting [20], [21], electromagnetic signature identification [22], [23], PHY-layer watermarking [24], and transmitter identification [25]. These schemes can be broadly divided into the three categories.

Schemes in the first category utilize the idiosyncrasies of the communication system, such as RF signal characteristics [20]–[23] or intrinsic channel characteristics [17], [19], as unique signatures to authenticate/identify transmitters. Although this approach has been demonstrated to work in controlled lab environments, its sensitivity to environmental factors—such as temperature changes, channel conditions and interference—limits its efficacy in real-world scenarios.

Schemes in the second category embed an artificial authentication signal in the message signal and extract it at the receiver [6]–[8]. In this approach, the authentication signal is embedded in the message signal in such a way that the authentication signal acts as noise to the message signal and vice versa. The schemes of this category can be collectively referred to as *blind signal superposition*. As mentioned previously, this method is constrained by the unavoidable tradeoff between the message signal's SNR and the authentication signal's SNR.

The third category includes techniques that avoid the drawbacks of blind signal superposition [9], [13], [16], [18]. In [9], the message signal at the transmitter is processed with a synthesized channel-like filter that is generated using the authentication signal. However, since this approach requires estimation of the channel response at the receiver, it may not be a viable approach when the coherence time is short. In [13], the authentication signal is embedded into the transmitted OFDM signal by repeating some message symbols over the sub-carriers to generate a cyclo-stationary signature. However, this scheme achieves authentication at the cost of loss in the message throughput. In [16], the authentication signal is embedded into the message signal in the form frequency offset. Since the frequency offset can be embedded in each frame of the message signal, the rate of authentication information (computed in bits) that can be transmitted per second is very low. The PHY-layer authentication scheme in [18] embeds the authentication signal as a frequency shift in the pilots of the message signal. This scheme affects the performance of the channel estimation process at the receiver.

Note that all of the aforementioned schemes ignore the privacy of the transmitters—i.e., the authentication signal is designed in such a way that the identity of the transmitter is revealed to all the receivers within the transmission range of the transmitter. This is a serious problem in certain applications, such as in the broadcast of safety beacon messages

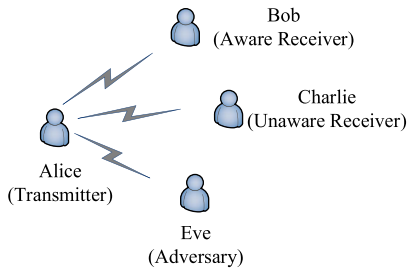

Fig. 1. Authentication scenario.

in vehicular networks [14], [15]. The notion of enabling the receivers to authenticate the received messages while protecting the true identity of the transmitters is referred to as privacy-preserving authentication.

The privacy preserving authentication schemes in the existing literature can be broadly categorized into two approaches: pseudonym-based signatures (PSs) [26] and group signatures (GSs) [27]. In a PS, the signer creates a signature based on a pseudonym, and replaces her pseudonym with a new one periodically to preserve anonymity. However, because each pseudonym needs to be used with its unique set of private and public keys as well as a certificate, key management and distribution become a very onerous burden in large networks [15]. In a GS, each signer is a member of a group, and she is provided with a private key tuple. Using this tuple, the signer generates signatures without revealing her true identity to the verifier. However, the computation time for the revocation check procedure performed by the verifier increases linearly with the number of revoked private keys. Hence, the computation time for signature verification becomes the major performance bottleneck of modern GS schemes [28].

III. Problem Description

In the spectrum sharing paradigm, a heterogeneous mix of cognitive radio devices/networks, with secondary access priority, opportunistically access the same band while avoiding interference to the PUs and minimizing interference to each other. In this scenario, malicious SUs that violate spectrum access rules pose a serious threat. Malicious users that effectively hijack spectrum resources or disturb peaceful coexistence need to be identified and thwarted. The first step in thwarting rogue transmitters is enabling regulators to uniquely identify or authenticate them. This can be achieved by requiring all secondary user radios to incorporate a mechanism for authenticating their waveforms and employ tamper resistance mechanisms to prevent the circumvention of the authentication mechanism by hacking [29]. In this approach, PHY-layer authentication is ideal because it enables a receiver to quickly distinguish between legitimate and rogue transmitters without having to complete higher-layer processing, which is unnecessary and wasteful.

Model: We assume an authentication scenario illustrated in Figure 1. In this scenario, Alice, Bob, Charlie and Eve are four SU systems which share the same wireless medium. Alice is a transmitter, and intends to transmit messages to Bob and Charlie via the wireless medium. Suppose Alice and Bob have agreed on a keyed authentication scheme (implemented at the PHY layer) that allows Bob (a.k.a. "aware receiver") to authenticate the waveforms he receives from Alice. To enable authentication, Alice embeds an authentication signal into the message signal. In this model, Bob represents a regular receiver that intends to authenticate Alice's message signal. Bob can also represent a regulatory authority (e.g., FCC) that needs to ensure that Alice complies with the established spectrum rules. Charlie (a.k.a. "unaware receiver") does not know the authentication scheme and cannot authenticate Alice's waveforms at the PHY-layer, but should be able to demodulate and decode the message signal that can be authenticated at upper layers. Eve, the adversary, has knowledge of the authentication scheme but does not know the key, and hence cannot forge Alice's authentication signal.

We use MS and AS to denote the message signal and the authentication signal generated by Alice in the baseband, respectively. We use $\widehat{MS}$ and $\widehat{AS}$ to denote the message signal and authentication signal estimated by Bob, respectively.

Challenges in PHY-Layer Authentication: The operations performed by Alice can be decomposed into two parts—generation of AS and embedding of AS into MS. Similarly, the operations performed by Bob can be decomposed into two parts—extraction of $\widehat{AS}$ and $\widehat{MS}$ from the received signal, and verification of $\widehat{AS}$. Alice needs to generate her transmission signal such that Bob can extract $\widehat{MS}$ and $\widehat{AS}$ from the received signal, and be able to verify the signal's validity by verifying $\widehat{AS}$. Hence, there are two primary technical challenges in devising PHY-layer authentication schemes: (1) how to embed the AS into the MS without negatively impacting receiver's performance; and (2) how to generate the AS such that the required security criteria are met.

IV. Background: Precoded Duobinary Signaling (P-DS)

In this section, we review the pulse shaping scheme, called *Precoded Duobinary Signaling* (P-DS). The core idea of P-DS is to introduce a controlled amount of ISI in the transmitted pulses, and change the detection procedure at the receiver to cancel out the ISI [30].

Assume that $\{d_n\}$, $n = 1, 2 \cdots N$, denotes a message sequence of bits representing the message signal that needs to be transmitted, where N represents the size of the block of the message signal. Using the non-return-to-zero (NRZ) encoding, a bipolar sequence, $\{w_n\}$, is generated from the message sequence, $\{d_n\}$. Further, a duobinary symbol, y_n, is generated by adding the delayed pulse of w_n to itself. Hence, the duobinary symbol is represented by

$$y_n = w_n + w_{n-1}. \tag{1}$$

This equation signifies that the duobinary symbol is generated by adding a given bipolar symbol to the immediately previous bipolar symbol. If $w_n = \pm 1$, this results in a three-level output—i.e., y_n has one of three possible values: $+2$, 0 or -2 (see Figure 2a).

Here, the duobinary symbol, y_n, can be 0 for two cases—when $w_{n-1} = +1$ is followed by $w_n = -1$, and when $w_{n-1} = -1$ is followed by $w_n = +1$. Therefore, if the

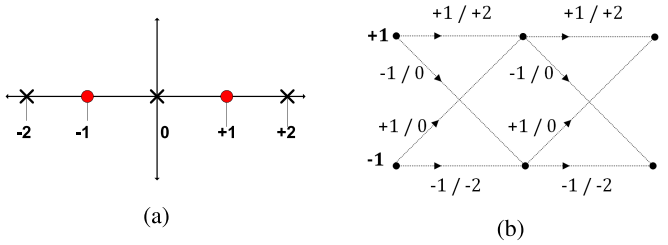

Fig. 2. (a) Constellation (red circles represent the bipolar signal, and black crosses represent the duobinary signal), and (b) Trellis used by MLSD.

receiver decodes w_{n-1} incorrectly, it affects the decoding of y_n and consequently, the detection of w_n is also likely to be in error. This error propagation can be avoided by *precoding* the message sequence at the transmitter, i.e., the message sequence is precoded to produce a new sequence called the precoded sequence. Therefore, we refer to this signaling technique as *Precoded Duobinary Signaling* (P-DS).

In P-DS, the precoded sequence, $\{p_n\}$, for the message sequence, $\{d_n\}$, is generated using the relation $p_n = d_n \oplus p_{n-1}$, where $\oplus$ represents modulo-2 addition. Further, the bipolar sequence, $\{w_n\}$, is generated from the precoded sequence, $\{p_n\}$, using NRZ encoding. Each symbol in the duobinary sequence, $\{y_n\}$, is generated using the equation (1), and transmitted after RF processing. We note that the first precoded bit is generated as $p_1 = d_1 \oplus p_0$. Also, we observe that the duobinary symbol, y_1, corresponding to the bipolar symbol, w_1, is given by $y_1 = w_1 + w_0$, where w_0 and w_1 are the bipolar symbols corresponding to the precoded bits, p_0 and p_1, respectively. Hence, in P-DS, we require an extra bipolar symbol, w_0 and a corresponding precoded bit, p_0, to start the encoding of the message sequence, $\{d_n\}$, $n = 1, 2 \cdots N$. The bit, p_0, is called an *initialization bit* which is usually given the value of 0. Correspondingly, the symbol, w_0, is called an *initialization state* which is usually given the value of -1.

At the receiver, after RF processing, the received signal is estimated as the duobinary sequence, $\{\hat{y}_n\}$ in the baseband. Henceforth, two decoding methods can be utilized—symbol-by-symbol detection (SSD) and maximum likelihood sequence detection (MLSD). Using SSD method, the estimated message sequence, $\{\hat{d}_n\}$, is obtained using the following decoding decision rule.

$$\hat{d}_n = \begin{cases} 0, & \text{if } \hat{y}_n = +2 \text{ or } -2; \\ 1, & \text{if } \hat{y}_n = 0. \end{cases} \tag{2}$$

The bit error rate (BER) of the message signal decoded using SSD [30] is given by

$$P_{SSD} = \frac{3}{4}\,\text{erfc}\left(\frac{\pi}{4}\sqrt{\frac{E_b}{N_0}}\right), \tag{3}$$

where erfc, E_b and N_0 represent the complementary error function, the average bit energy, and noise power spectral density, respectively.

Since the three-level duobinary signaling incurs an increase in the number of constellation points in Euclidean space compared to binary signaling, duobinary signaling's error performance against noise is inferior to that of binary signaling when SSD is utilized. However, the duobinary sequence in P-DS is generated from a bipolar sequence and has memory of length 1—i.e., the current state is related only to the previous state. Hence, we can use the MLSD (based on Viterbi trellis decoding) with two states (i.e., $+1$ and -1) to obtain an estimate of the transmitted bipolar sequence, $\{\hat{w}_n\}$. Figure 2b shows the trellis used by the MLSD, and it is generated by considering all possible transitions from each of the states. For example, an arrow from state $+1$ with the label $+1/+2$ represents a transition to the next state indicated by the left number, $+1$. The right number, $+2$, denotes the resultant signal level.

The received bipolar sequence, $\{\hat{w}_n\}$, is estimated from $\{\hat{y}_n\}$ using MLSD. Further, the estimated precoded sequence, $\{\hat{p}_n\}$, is generated from $\{\hat{w}_n\}$ using NRZ decoding. Finally, to obtain the estimated message sequence, $\{\hat{d}_n\}$, the decoding of the estimated precoded sequence is carried out as $\hat{d}_n = \hat{p}_n \oplus \hat{p}_{n-1}$, where $\oplus$ represents modulo-2 addition. The BER of the message signal using MLSD [31] is upper bounded by

$$P_{MLSD} = \text{erfc}\left(\sqrt{\frac{E_b}{N_0}}\right). \tag{4}$$

Table I provides an example illustrating the results of using P-DS encoding for the message sequence, $\{010110\}$ with the initialization bit, $p_0 = 0$. Table II illustrates the SSD of the message signal encoded in Table I.

TABLE I
AN EXAMPLE ILLUSTRATING P-DS ENCODING

d_n		0	1	0	1	1	0
p_n	0	0	1	1	0	1	1
w_n	-1	-1	$+1$	$+1$	-1	$+1$	$+1$
y_n		-2	0	$+2$	0	0	$+2$

TABLE II
AN EXAMPLE ILLUSTRATING SSD IN P-DS

$\hat{y}_n$	-2	0	$+2$	0	0	$+2$
$\hat{d}_n$	0	1	0	1	1	0

V. PRECODED DUOBINARY SIGNALING FOR AUTHENTICATION (P-DSA)

In this section, we provide a detailed description of P-DS for Authentication (P-DSA). P-DSA exploits the inherent redundancy introduced by P-DS to authenticate waveforms. In P-DS, a known initialization bit is needed to start the encoding of the message signal. However, we note that this initialization bit can be varied while encoding, with minimal effect on the performance of the message signal's decoding procedure. The core idea of P-DSA is to generate the embedded signal for each block of the message signal (MS) in such a way that the initialization bit is varied based on the authentication signal (AS), i.e., P-DSA uses this initialization bit as an authentication bit.

TABLE III

AN EXAMPLE ILLUSTRATING P-DSA ENCODING (THE UNDERLINED BITS ARE THE AUTHENTICATION BITS TO BE EMBEDDED)

d_n		0	1	0		0	1	0
p_n	$\underline{0}$	0	1	1	$\underline{1}$	1	0	0
w_n	-1	-1	$+1$	$+1$	$+1$	$+1$	-1	-1
y_n		-2	0	$+2$		$+2$	0	-2

A. Embedding of AS Into MS

We assume that MS contains K blocks of binary message sequences of length N represented by $\{d_n\}$, $n = 1, 2 \cdots N$. We also assume that AS is a binary sequence of length K generated using the scheme described in Section VII, and represented by $\{a_k\}$, $k = 1, 2 \cdots K$. The encoding procedure of P-DSA is the same as the one for P-DS except that the precoding of each block of the message sequence is initiated using an authentication bit to be embedded. For each block of message sequence of MS, $\{d_n\}$, we generate the precoded sequence, $\{p_n\}$. Next, we generate the bipolar sequence $\{w_n\}$ from $\{p_n\}$ using NRZ encoding. Finally, the duobinary sequence, $\{y_n\}$, is generated from $\{w_n\}$ using equation (1).

As noted earlier, an initialization bit, p_0, is required to initiate the precoding of $\{d_n\}$ in each block. In P-DS, it is achieved by choosing a standard value for p_0. For different blocks, the same p_0 and hence the same w_0 is repeatedly used to initiate the encoding. The core idea of P-DSA is to replace the bit, p_0, in each block of MS with a bit from AS, a_k. Hence, the bipolar symbol, w_0, for the k^{th} block is generated from the authentication bit, a_k, using NRZ encoding. In the k^{th} block of the embedded signal, the first precoded bit, p_1, is generated by using the first message bit, d_1 and an authentication bit, a_k. As a result, for $a_k = 0$, the resultant precoded bit, p_1, is 0 and 1 for $d_1 = 0$ and $d_1 = 1$, respectively. Similarly, for $a_k = 1$, the resultant precoded bit, p_1, is 1 and 0 for $d_1 = 0$ and $d_1 = 1$, respectively. Table III illustrates an example of P-DSA encoding.

B. Extraction of $\widehat{MS}$ and $\widehat{AS}$

In P-DSA, we generate the embedded signal by changing the encoding procedure and accordingly change decoding procedure to extract the message signal ($\widehat{MS}$) and the authentication signal ($\widehat{AS}$) from the received signal. Note that P-DSA modifies neither the symbol mapping nor the correlation among the symbols being transmitted. Hence, the SSD is not affected by this change in encoding, while MLSD needs only a slight modification as described below.

In P-DS, at the transmitter, the precoding of each block of N bits of the message signal is started with the pre-decided initialization bit. At the receiver, MLSD starts with the initialization state which is generated from the same initialization bit. The MLSD decides on the sequence of states that is closest to the received signal in terms of Euclidean distance over the whole trellis. The complexity of this problem is significantly reduced by using the Viterbi algorithm which makes a decision on the possible paths reaching each possible state independent of other states [32]. In this case, the MLSD starts with the two paths from the initialization state to the *possible first states* corresponding to the first received duobinary symbol as shown in Figure 3a. Recall that trellis decoding makes a decision on the path reaching a particular state only if there are two or more paths reaching it. Hence, in P-DS, no decision is needed to select the path on each of the possible first states from the initialization state.

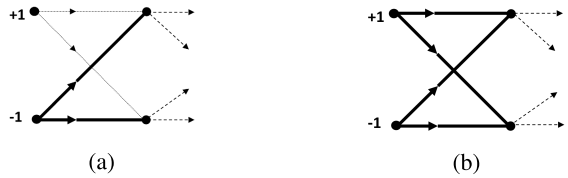

Fig. 3. (a) MLSD for P-DS, and (b) Modified MLSD for P-DSA (the bold lines represent the possible paths emanating from the initialization state).

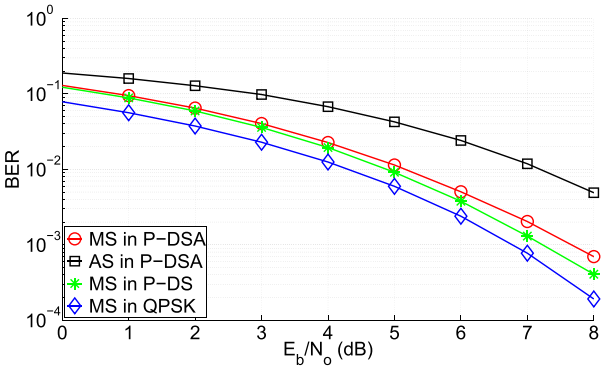

Fig. 4. BER performance of message signal (MS) modulated using QPSK, P-DS and P-DSA, and authentication signal (AS) embedded into MS using P-DSA.

In P-DSA, the initialization bit is an authentication bit, and hence it also has to be estimated by the MLSD in order to decode the sequence. Hence, we need to account for the paths emanating from both the possible initialization states as shown in Figure 3b. Out of the two possible paths reaching each of the possible first states, we find the one that pertains to the closest first received duobinary symbol. In effect, the receiver performs SSD to determine the first symbol—i.e., it selects the closest signal level among $+2$, 0 and -2, and uses this knowledge to estimate the path from the initialization state to the state corresponding to the first symbol. Note that the signal level of $+2$ (-2) can be detected for the first zero-valued message bit if the authentication bit's state is $+1$ (-1). With the first received signal level as 0, if the first message bit's state is $+1$, the authentication bit's state has to be -1 and vice versa.

C. Error Performance

Figure 4 shows BER vs. E_b/N_0 curves for MS and AS when P-DSA is applied to a quadrature phase-shift keying (QPSK) modulated signal, and one authentication bit is embedded into each block of message bits of length, $N = 16$. For comparison, we also show error performance of MS when P-DS is applied to a QPSK modulated signal, and no authentication signal is embedded. We observe that the performance of

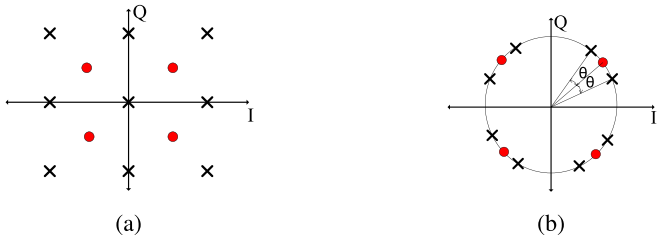

Fig. 5. Constellation (red circles represent the message signal and black crosses represent the embedded signal). (a) QPSK with P-DSA. (b) QPSK with ATM.

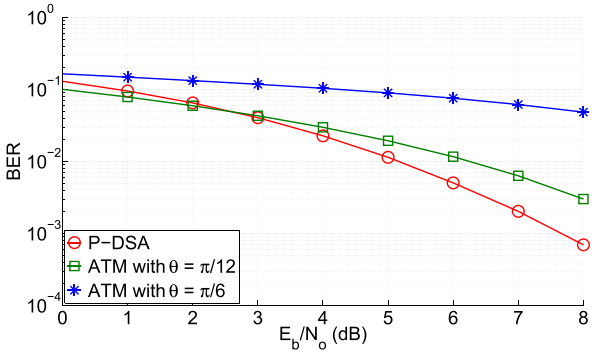

Fig. 6. BER performance of the message signal.

P-DS is very close to that of standard QPSK (without any ISI) which is used as the benchmark. This signifies that despite the addition of the ISI in the P-DS waveform, its message signal can be detected with nearly the same error performance as that of QPSK if MLSD, with sufficiently long block length, N, is used at the receiver.

We note that the error performance of MS in P-DSA is inferior to that of P-DS. There are two reasons for this degradation. Firstly, in P-DS, the receiver has perfect knowledge of the initialization bit's state; whereas in P-DSA, the initialization bit of each block are the authentication bits, and hence they need to be estimated. Secondly, in P-DSA, Bob employs SSD for detecting the state of the authentication bit and the first message bit of each block, but employs MLSD for rest of the message bits. Hence, the overall detection performance of MS in P-DSA is inferior to that of P-DS, which uses MLSD for *all* the bits in a block. As a result, the BER of the message signal in P-DSA can be upper bounded by

$$P_{MS} = \frac{1}{N} \cdot P_{SSD} + \left(1 - \frac{1}{N}\right) \cdot P_{MLSD}, \tag{5}$$

where P_{SSD} and P_{MLSD} are obtained using equations (3) and (4), respectively.

In P-DSA, the state of the authentication signal is determined by each block's first received signal level which, in turn, is estimated through comparison to the three signal levels: $+2$, 0, and -2. In essence, decoding the authentication signal depends on the performance of SSD, and does not benefit from MLSD as shown in Figure 4. Hence, the BER of AS, P_{AS}, is equal to P_{SSD} which is calculated using equation (3).

VI. Evaluation of P-DSA

In this section, we first define the fundamental criteria that characterize the performance of PHY-layer authentication schemes. Based on these criteria, we then compare P-DSA against a benchmark scheme that is representative of the prior art: *Authentication Tagging using Modulation* (ATM) [6]. We apply P-DSA and ATM, respectively, on a QPSK modulated message signal to obtain the embedded authenticated signal. In P-DSA, the controlled ISI added to the QPSK signal results in a constellation with nine possible symbol positions as shown in Figure 5a. On the other hand, ATM utilizes the phase based hierarchical modulation to embed the authentication signal which leads to a constellation of eight possible symbol positions as shown in Figure 5b. In ATM, an authentication bit of 1 is embedded by shifting the phase of a QPSK message constellation symbol 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.

A. Resource Overhead

Embedding the authentication signal in the message signal requires applying changes to the message signal itself, and thus incurs some PHY-layer resource overhead. For instance, the mechanism proposed in [13] results in drop in the message throughput. Other examples of resource overhead include increase in average transmission power, increase in bandwidth, and increase in computational complexity of the transmitter and/or receiver.

By design, P-DSA as well as ATM does not change the message throughput. Also, the overall average transmission power and bandwidth are unchanged from standard QPSK. In terms of the transmitter's and the aware receiver's computational complexity, ATM is advantageous compared to P-DSA. To implement ATM, the transmitter (Alice) and the receiver (Bob) only need to modify how the embedded signal is mapped to the constellation symbols. However, implementation of P-DSA is more complex—Alice needs to add controlled ISI, and Bob requires the use of MLSD to extract the message and the authentication signals. Specifically, at Bob, the computational complexity of decoding each modulated symbol is increased by $O(M^2)$ due to MLSD in P-DSA as compared to ATM, where M represents the order of the modulation scheme, e.g., $M = 4$ for QPSK.

B. Message Signal's Error Performance

This criterion refers to the achievable error performance (in terms of BER) when decoding the received message signal, $\widehat{MS}$. Figure 6 shows the error performance of MS in P-DSA with $N = 16$, ATM with phase shift of $\theta = \pi/12$ rad and ATM with phase shift of $\theta = \pi/6$ rad. In ATM, the message signal's constellation points are intentionally positioned in non-optimal positions so that the authentication signal's constellation can be superimposed on top of the message signal's constellation. Hence, as the presence of the authentication signal becomes more dominant (by increasing θ) in ATM,

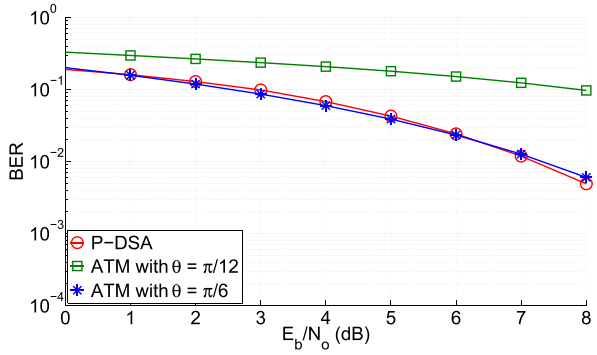

Fig. 7. BER performance of the authentication signal.

the BER performance of the message signal detection degrades as shown in Figure 6. Our scheme, P-DSA, is not constrained by such a tradeoff, and this attribute provides an important advantage in terms of error performance.

C. Authentication Signal's Error Performance

This criterion refers to the achievable error performance when decoding the received authentication signal, $\widehat{AS}$. Figure 7 shows the error performance of AS in P-DSA with $N = 16$, ATM with phase shift of $\theta = \pi/12$ rad and ATM with phase shift of $\theta = \pi/6$ rad. In ATM, the message and authentication signals are embodied in two different constellations (i.e., message signal is carried in the low-resolution constellation and authentication signal is carried in the high-resolution constellation). The effect of this multi-resolution modulation can be observed when we compare ATM's curves in Figure 6 and 7. Comparing the curve of ATM with phase shift of $\theta = \pi/12$ rad in Figure 6 with that of Figure 7, we see that the BER performance of message signal is noticeably better than that of authentication signal. Moreover, we also observe that the exact opposite is true for ATM with $\theta = \pi/6$ rad. When the phase shift is $\theta = \pi/12$ rad, the shift in the constellation points (from their conventional QPSK positions) is not significant enough to cause a significant drop in BER of message signal detection. However, this relatively small shift in phase makes decoding of the authentication signal difficult, because it is carried in a high-resolution constellation. When $\theta = \pi/6$ rad, the situation is reversed.

From Figure 7, we observe that with $\theta = \pi/6$ rad, ATM has comparable BER performance compared to P-DSA for the detection of the authentication signal. However, Figure 6 shows that P-DSA has a significant advantage in terms of BER performance of message signal detection. On the other hand, when ATM with $\theta = \pi/12$ is used, the BER performance of message signal detection is improved (compared to ATM with $\theta = \pi/6$). However, changing from $\theta = \pi/6$ to $\theta = \pi/12$ causes a significant increase in BER for the detection of the authentication signal as shown in Figure 7.

For a PHY-layer authentication scheme to be viable, Bob must be able to decode both the message and the authentication signals with sufficiently good BER. ATM makes a tradeoff between the message signal's SNR and the authentication signal's SNR under the assumption of constant average power. This implies that one cannot improve the former without sacrificing the latter, and vice versa. This attribute is a fundamental drawback of blind signal superposition. P-DSA does not make the aforementioned tradeoff, and instead embeds the authentication signal by exploiting the inherent redundancy in the waveform shaping process. The resulting nine-level signal does increase the number of constellation points (thereby decreasing the minimum Euclidean distance between constellation points), but nevertheless manages to outperform ATM in terms of BER performance. From Figures 6 and 7, and the above discussions, we can conclude that P-DSA offers a significant advantage over ATM.

D. Authentication Rate

In PHY-layer authentication, the authentication signal is embedded by altering the message signal in a certain manner so that the receiver can detect the alteration and use it to extract the authentication information. The rate at which the alteration can be made is called the authentication rate.

In P-DSA, one bit of AS is transmitted in each block (of length N bits) of MS, which leads to an authentication rate of $1/N$. Although the authentication rate in P-DSA can be varied by changing N, decreasing N leads to a lower trellis length for MLSD. This leads to lower error performance for MS, which is inferred using equation (5). However, changing N does not affect the error performance of AS in P-DSA as the detection of AS depends only on the detection of the first received signal level in each block. On the other hand, ATM achieves an authentication rate of $1/2$—one authentication bit can be inserted for every two message bits or one QPSK modulated symbol.

E. Security

This criterion determines the robustness of a PHY-layer authentication scheme against the attack carried out by Eve on the embedding and the extraction process of the authentication signal. In a PHY-layer authentication scheme, when the embedded signal with authentication signal embedded into the message signal is transmitted at the PHY-layer, Eve can launch a particular type of jamming attack specifically against the authentication signal. Hence, we propose the idea of *obstruction of authentication* (OOA) jamming attack. The OOA jamming is different from a conventional (or indiscriminate) jamming attack. The objective of conventional jamming is to prevent a targeted receiver from correctly decoding the transmitted message by generating interference of sufficient power. In contrast, the objective of OOA jamming is to generate just enough interference to prevent Bob from verifying the authenticity of the message, yet still enable him to correctly decode the message itself. OOA jamming is difficult to detect because it can readily be mistaken for naturally-occurring noise or non-malicious interference. In certain scenarios, this may encourage Bob to treat the received message as a legitimate message without actually authenticating it. Hence, this has obvious security implications. The effectiveness of OOA jamming is dictated by the PHY-layer scheme that is used to embed the authentication signal into the message

signal, and *not* the contents of the authentication signal. Hence, we discuss the security attributes of the contents of the authentication signal in Section VIII-C after proposing the design of the authentication signal in Section VII.

Because the two schemes—viz, P-DSA and ATM—dictate the methodology by which the authentication signal is embedded into the waveform, we focus our discussions on the two schemes' resilience against OOA jamming attack that may be launched by Eve. OOA jamming can be quite effective against blind signal superposition schemes [6]–[8], which allocate different amounts of transmission power to the message and authentication signals respectively, including ATM. In these schemes, the message signal is embodied by a high-power constellation while the authentication signal is carried on a low-power constellation. In this case, Eve can emit just enough interference to exploit the power difference, and thus prevent decoding of the authentication signal but enable decoding of the message signal. However, in P-DSA, to obstruct Bob from decoding the authentication signal, Eve would need to generate interference that is sufficiently powerful to also make decoding of the message signal impossible. Hence, P-DSA is robust to OOA jamming.

F. Transparency

This criterion dictates that a PHY-layer authentication scheme should embed the authentication signal into the message signal such that it enables the aware receiver (Bob) to extract the authentication signal, while at the same time, enables the unaware receiver (Charlie) to recover the message signal *without* requiring to change its demodulation or decoding procedure. In P-DSA, to avoid error propagation, we use precoding at the transmitter and remove the precoding to estimate the message signal at the aware receiver. Also, the embedded signal transmitted by Alice contains zero-valued signal levels as shown in Figure 5a. Therefore, the unaware receiver must have the knowledge of P-DSA for extracting the message signal. In contrast, in ATM, the unaware receiver does not need to change the demodulation/decoding procedure to recover the message signal—i.e., he simply treats the embedded signal as a regular QPSK modulated signal and the embedded authentication signal as noise. Therefore, ATM has the advantage over P-DSA in terms of transparency. However, in ATM, Bob, the aware receiver, with knowledge of the embedding scheme, does no better than the unaware receiver in terms of error performance of the message signal.

VII. Authentication Signal's Generation and Verification

In this section, we discuss the procedures for generation of keys for Alice by a regulatory entity (REG), generation of AS by Alice, and verification of $\widehat{AS}$ by Bob.

A. Generation of Keys

In the spectrum sharing paradigm, the first step for Alice is to contact REG, and request access to the available spectrum by providing its identity (represented by I) and its location (represented by L). As per spectrum availability, REG allows Alice to transmit at a particular frequency (represented by F) for a particular time-period (represented by T). Further, REG generates the keys which are used by Alice for generating AS, using the following steps.

1) REG stores Alice's identity I in its database which is indexed using F and L.
2) REG provides Alice with a master key k_a to generate "pseudo keys". We assume that the master key k_a is securely established between Alice and REG using a well-known key exchange protocol, such as the authenticated Diffie-Hellman key exchange protocol. The use of such a key exchange protocol prevents Eve from learning k_a. As a result, Eve cannot relate the pseudo keys to Alice.
3) REG divides the time-period of Alice's transmission, T, into n time-windows of length, T/T_r, where the i^{th} time-window is represented by $[(i-1)T_r, iT_r]$. It is assumed that all SU transmitters use the same value of T_r.
4) To generate a pseudo key for each time-window, REG utilizes a cryptographic hashing algorithm (e.g., SHA-3). That is, the REG generates $h_i = HASH\{k_a, i\}$, where h_i, for $i = 1, \cdots n$, is considered a valid pseudo key only in i^{th} time-window.
5) REG stores the pseudo keys in its database which is indexed using Alice's identity I and the time-window i. This means that a valid pseudo key is mapped to a set of frequency, location, and time values.

B. Generation of AS

Having received master key k_a from REG, Alice performs the following steps to generate the authentication signal, AS.

1) Alice generates the pseudo key for each time-window, $i = 1, \cdots n$, using the same method as REG. Hence, rather than communicating all pseudo keys, h_i for $i = 1, \cdots n$, REG has to communicate only the master key k_a to Alice. Alice uses the pseudo keys to renew her key after each time interval, T_r, to ensure her privacy.
2) Assume that Alice wants to transmit the authentication signal at time TS. Hence, Alice computes the value i such that $TS \in [(i-1)T_r, iT_r]$.
3) Assume that the data to be included in the authentication signal in the i^{th} time-window is represented by AS_d. In AS_d, Alice includes the frequency at which it is authorized to transmit (F), and her location (L). Alice also includes the current time-stamp (TS). Hence, $AS_d = \{F, L, TS\}$ represents the data of the authentication signal.
4) Alice computes the keyed hash of AS_d to generate a parameter c such that $c = HASH\{h_i, AS_d\}$.
5) The bit sequence represented by $\{AS_d, c\}$ is channel-coded into K_e bits with an error-correcting code (e.g., convolution code). Further, K_s synchronization bits and K_g guard bits are appended to the K_e bits to produce a bit sequence of $K = K_e + K_s + K_g$ bits, which is then encoded to a modulating signal to form the authentication signal, AS.

C. Verification of $\widehat{AS}$

After demodulating the received signal, Bob extracts $\widehat{AS}$ from the received signal, and performs the following steps to verify the authenticity of $\widehat{AS}$.

1) Bob extracts $\{\widehat{AS}_d, \hat{c}\}$ from the estimated authentication signal by removing the synchronization and guard bits, and then carrying out channel decoding for error detection and correction. Note that $\widehat{AS}_d = \{\widehat{F}, \widehat{L}, \widehat{TS}\}$ and $\hat{c}$ are the estimates of AS_d and c.
2) Bob validates that the value of $\widehat{F}$ corresponds to the frequency at it which he is receiving the message signal, the value of $\widehat{L}$ is within his range of communication, and the value of $\widehat{TS}$ is fresh. If the three values are valid, $\widehat{AS}_d$ is considered to be valid; otherwise, $\widehat{AS}_d$ is declared invalid.
3) If $\widehat{AS}_d$ is determined to be valid, Bob contacts REG to verify the authenticity of $\widehat{AS}_d$, and communicates $\{\widehat{AS}_d, \hat{c}\}$ to REG.
4) REG with the information of $\widehat{F}$ and $\widehat{L}$, searches its database to find the user $\tilde{I}$ who is authorized to transmit at $\widehat{F}$ and $\widehat{L}$. Further, with the information of $\widehat{TS}$, it computes the value $\tilde{i}$ such that $\widehat{TS} \in \left[(\tilde{i}-1)T_r, \tilde{i}T_r\right]$. Using $\tilde{I}$ and $\tilde{i}$, REG searches its database to find the pseudo key $\tilde{h}_i$. REG computes $\tilde{c} = HASH\{\tilde{h}_i, \widehat{AS}_d\}$, and compares the result with $\hat{c}$. If the two values match, $\widehat{AS}_d$ is considered to be an authentic authentication signal; otherwise, $\widehat{AS}_d$ is declared to be fraudulent. Finally, REG communicates its result to Bob.

VIII. Evaluation Criteria for the Authentication Signal

In this section, we evaluate the proposed approach for generating the authentication signal in the context of performance and security criteria.

A. Communication Overhead

1) Communication Between Alice and REG: As per the established protocol in the spectrum sharing environment [2], the communication between REG and Alice happens only when Alice contacts REG to obtain access to a desired spectrum band. During this communication, Alice obtains the information about the frequency F, and the power at which it can transmit, and the time-period T during which it can transmit. In order to preserve privacy of Alice, the time-period T is divided into time-windows of length T_r, and a pseudo key h_i is generated for each time-window i. Each h_i acts as the valid pseudo key only within one time window, and is utilized to generate the authentication signal within the time window. Rather than communicating a large number of pseudo keys, in the proposed design of the authentication signal, pseudo keys are generated using the hash function and the shared master key k_a. This methodology lowers the communication overhead of the authentication scheme.

2) Communication Between Alice and Bob: When heterogeneous systems share spectrum, incompatible systems (i.e., systems with different protocol stacks) may not be able to decode each other's higher-layer signaling. Hence, the design of the authentication signal should not require mutual interaction between Alice and Bob. In the proposed design, Bob authenticates Alice's messages without any prior coordination or any mutual interaction between the two. REG acts as the trusted third party to enable the authentication.

3) Communication Between Bob and REG: In the proposed authentication scheme, to check the authenticity of every received packet of the authentication signal, Bob needs to communicate with REG. To mitigate this onerous requirement, we propose that the PHY-layer authentication is invoked only if Bob needs to verify the source of the received signal at the PHY-layer. For instance, such a need would arise in the following scenario. Suppose that Bob is a regulatory enforcement entity (e.g., FCC) that needs to identify rogue transmitters and enforce spectrum access rules. Further, suppose that a malicious secondary user, Eve, starts rogue transmissions in frequency F without obtaining prior approval from REG. This causes harmful interference to another secondary user, Alice, who has been authorized by REG to use the same frequency F. Bob can detect this interference event by processing relevant spectrum sensing data collected from other nodes—either data from dedicated spectrum sensors located in the vicinity of Alice [5], or crowdsourced data from users that operate in the frequency F, including Alice [33]. Working together with REG, Bob can utilize such data and P-DSA to uniquely identify the source of the rogue transmissions, viz., Eve.

B. Implementation Complexity

In the spectrum sharing paradigm, the authentication signal is utilized for adding an additional level of transmitter authentication at the PHY-layer. Also, the transmitter employs tamper resistance mechanisms to prevent the circumvention of the authentication mechanism by hacking [29]. As a result, the hardware/software resources at the transmitter for the authentication scheme are limited. Hence, we have employed a light-weight, keyed hash-based authentication scheme to minimize the computation cost associated with generating and verifying authentication signals.

C. Security

In the following discussions, we present the four facets of security that need to be considered in the design of the authentication signal: *privacy*, *integrity*, *impersonation*, and *replay*.

1) Privacy: To protect the privacy of Alice from Eve, the authentication signal should not reveal the true identity of Alice. In the proposed scheme, the only information that is accessible by Eve is AS_d which contains the frequency F, the location L, and the current time stamp TS. Eve cannot uniquely identify Alice with this information.

2) Integrity: To ensure integrity, the authentication signal should not allow Eve to modify Alice's messages without being detected by REG. The hash function used in the authentication signal generation procedure provides integrity.

3) Impersonation: In a successful impersonation attack, Eve is able to create proofs of authenticity for her messages that can convince REG into thinking that those messages have been

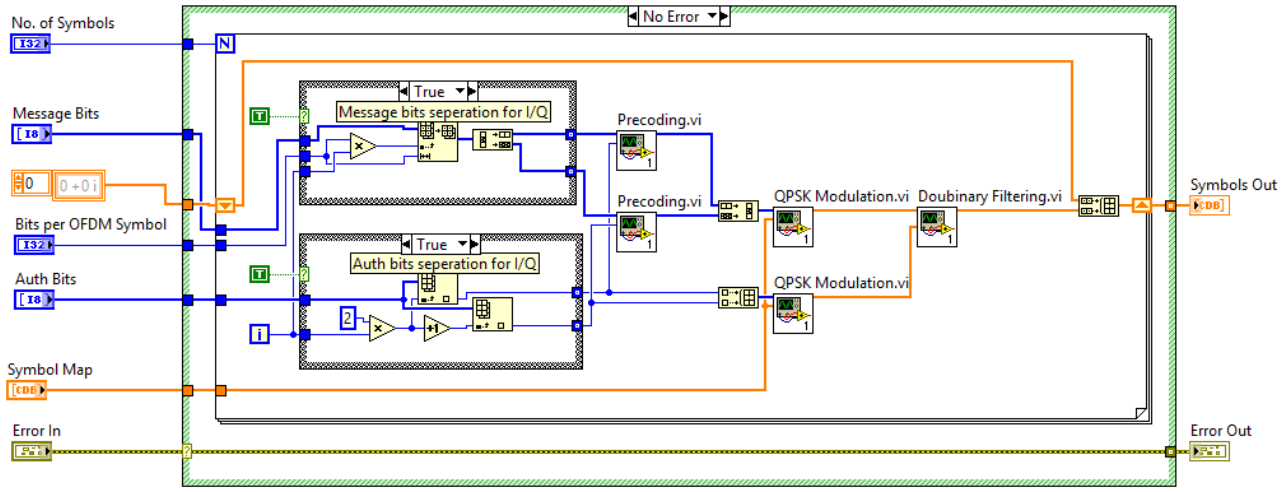

Fig. 8. LabVIEW VI illustrating the implementation of P-DSA.

created by Alice. To thwart impersonation, the process for generating the authentication signal should not enable Eve to create valid proofs of authenticity for her messages. In the proposed design, Alice and REG share a secret master key k_a which is used to generate the pseudo key, h_i in the i^{th} time-window. Therefore, only Alice can generate the authentication signal with pseudo key, h_i, and impersonation attacks are thwarted.

4) Replay: To launch replay attacks, Eve needs to store and re-transmit authentication signals previously transmitted by Alice. To thwart replay attacks, Alice's authentication signal should incorporate countermeasures that deter the interception and replay of her message signal. In the proposed design, such replayed transmissions can be readily detected by Bob since the authentication signal contains a time-stamp TS which cannot be tampered with without being detected.

IX. Experimental Validation

We implemented P-DSA as a prototype using two Universal Software Radio Peripheral (USRP) radios, one each for Alice (transmitter) and Bob (aware receiver). We used National Instruments' LabVIEW as the system-design platform to configure the USRPs.

In the prototype implementation, Alice and Bob use the PHY-layer protocol discussed in IEEE 802.11af draft standard [34] to communicate with each other at 900 MHz. Alice generates the message signal using orthogonal frequency division multiplexing (OFDM). She utilizes QPSK as the modulation scheme for the message signal. Alice also embeds an authentication signal into its message signal using P-DSA so that Bob is able to authenticate Alice.

Model and Assumptions: The two radios are placed approximately 1 meter away from each other in an indoor environment. The distance between the radios is limited by the fact that both the radios need to be connected to the computer running the LabVIEW application through network cables. Hence, to obtain variable E_b/N_0 values (from 0 dB to 8 dB), we add Gaussian noise at Bob in addition to the channel-induced and thermal noise added to the signal transmitted over-the-air.

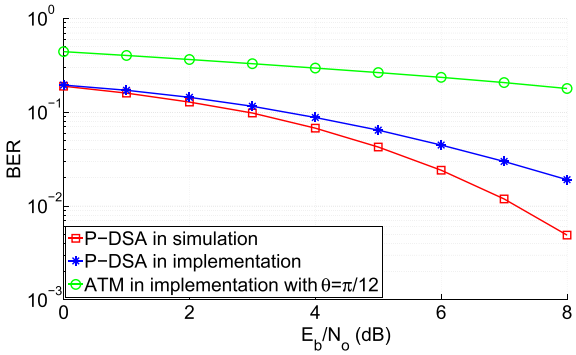

Fig. 9. BER performance of the authentication signal using the LabVIEW implementation.

Design: The data contained in the message signal consists of a time-stamp and message text, and it is transmitted without any error correction coding. The authentication signal also consists of a time-stamp and authentication text without any error correction coding. The authentication signal is embedded into the message signal using P-DSA with a block length of $N = 16$. Bob demodulates and decodes the received signal, and then separates the message and authentication signals. The received message and authentication signals are synchronized using the time-stamp, and compared with the transmitted message and authentication signals to calculate their BER, respectively.

Figure 8 shows the Virtual Instrument (VI) in LabVIEW illustrating the steps needed to embed an authentication symbol into the message signal using P-DSA. The message bits and the authentication bits are separated into in-phase and quadrature-phase streams. After precoding the message bits in each block with an authentication bit, the precoded sequence is mapped to QPSK symbols. Finally, duobinary signaling is carried out for each block. Further, conventional processes like performing inverse fast fourier transform (IFFT), adding cyclic prefix, and adding preamble symbols are performed to generate the OFDM signals to be transmitted over-the-air.

Results: Figure 9 shows the BER performance of the authentication signal (AS) for the LabVIEW implementation of P-DSA. As a benchmark, a BER performance curve generated from Matlab simulations using the same PHY-layer

parameters is also presented. We observe that the BER performance of the LabVIEW implementation is slightly inferior to that of the simulations. This phenomenon can be attributed to 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.

In Figure 9, we show the BER performance of the authentication signal when ATM is used for transmitter authentication. The ATM waveform was implemented in LabVIEW. We can observe that P-DSA outperforms ATM in terms of BER performance.

X. Conclusion

We propose a novel PHY-layer authentication scheme referred to as *Precoded Duobinary Signaling for Authentication* (P-DSA). P-DSA is fundamentally different from the prior art, and it is not constrained by the tradeoff that constrains the blind signal superposition schemes. Although P-DSA increases the number of points in the signal constellation (compared to conventional binary signaling), our simulation results show that it achieves improved error performance of message and authentication signals compared to the prior art without sacrificing message throughput or requiring an increase in transmission power. P-DSA inherits such desirable attributes at the cost of increased transmitter/receiver complexity.

References

[1] V. Kumar, J.-M. Park, T. C. Clancy, and K. Bian, "PHY-layer authentication by introducing controlled inter symbol interference," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2013, pp. 10–18.

[2] J.-M. Park, J. H. Reed, A. A. Beex, T. C. Clancy, V. Kumar, and B. Bahrak, "Security and enforcement in spectrum sharing," *Proc. IEEE*, vol. 102, no. 3, pp. 270–281, Mar. 2014.

[3] M. Altamimi, M. B. H. Weiss, and M. McHenry, "Enforcement and spectrum sharing: Case studies of federal-commercial sharing," in *Proc. SSRN*, Sep. 2013.

[4] *Enabling Innovative Small Cell Use in 3.5 GHZ Band NPRM & Order*, document FCC 12-148, FCC, Dec. 2012.

[5] FCC, "Shared commercial operations in the 3550-3650 MHz band," *Fed. Register*, vol. 80, no. 120, Jun. 2015.

[6] X. Tan, K. Borle, W. Du, and B. Chen, "Cryptographic link signatures for spectrum usage authentication in cognitive radio," in *Proc. 4th ACM Conf. Wireless Netw. Secur. (WiSec)*, Jun. 2011, pp. 79–90.

[7] P. L. Yu, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 38–51, Mar. 2008.

[8] P. L. Yu, J. S. Baras, and B. M. Sadler, "Multicarrier authentication at the physical layer," in *Proc. Int. Symp. World Wireless, Mobile Multimedia Netw.*, Jun. 2008, pp. 1–6.

[9] N. Goergen, T. C. Clancy, and T. R. Newman, "Physical layer authentication watermarks through synthetic channel emulation," in *Proc. IEEE Symp. New Frontiers Dyn. Spectr.*, Apr. 2010, pp. 1–7.

[10] T. Jiang, H. Zeng, Q. Yan, W. Lou, and Y. T. Hou, "On the limitation of embedding cryptographic signature for primary transmitter authentication," *IEEE Wireless Commun. Lett.*, vol. 1, no. 4, pp. 324–327, Aug. 2012.

[11] S. Pasupathy, "Correlative coding: A bandwidth-efficient signaling scheme," *IEEE Commun. Soc. Mag.*, vol. 15, no. 4, pp. 4–11, Jul. 1977.

[12] V. Vadde and S. Gray, "Partial response signaling for enhanced spectral efficiency and RF performance in OFDM systems," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, vol. 5. 2001, pp. 3120–3124.

[13] L. Yang, Z. Zhang, B. Y. Zhao, C. Kruegel, and H. Zheng, "Enforcing dynamic spectrum access with spectrum permits," in *Proc. 13th ACM Int. Symp. Mobile Ad Hoc Netw. Comput. (MobiHoc)*, 2012, pp. 195–204.

[14] J. Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing auditability and privacy in vehicular networks," in *Proc. 1st ACM Int. Workshop Quality Service Secur. Wireless Mobile Netw. (Q2SWinet)*, 2005, pp. 79–87.

[15] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[16] V. Kumar, J.-M. Park, and K. Bian, "Blind transmitter authentication for spectrum security and enforcement," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2014, pp. 787–798.

[17] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2010, pp. 286–301.

[18] R. Miller and W. Trappe, "Short paper: ACE: Authenticating the channel estimation process in wireless communication systems," in *Proc. 4th ACM Conf. Wireless Netw. Secur. (WiSec)*, 2011, pp. 91–96.

[19] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, Jul. 2008.

[20] W. Hou, X. Wang, and J.-Y. Chouinard, "Physical layer authentication in OFDM systems based on hypothesis testing of CFO estimates," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 3559–3563.

[21] O. Ureten and N. Serinken, "Wireless security through RF fingerprinting," *Can. J. Elect. Comput. Eng.*, vol. 32, no. 1, pp. 27–33, May 2007.

[22] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. 14th ACM Int. Conf. Mobile Comput. Netw. (MobiCom)*, 2008, pp. 116–127.

[23] B. Danev and S. Capkun, "Transient-based identification of wireless sensor nodes," in *Proc. IEEE Int. Conf. Inf. Process. Sensor Netw.*, Apr. 2009, pp. 25–36.

[24] I. J. Cox, M. L. Miller, and A. L. McKellips, "Watermarking as communications with side information," *Proc. IEEE*, vol. 87, no. 7, pp. 1127–1141, Jul. 1999.

[25] X. Wang, Y. Wu, and B. Caron, "Transmitter identification using embedded pseudo random sequences," *IEEE Trans. Broadcast.*, vol. 50, no. 3, pp. 244–252, Sep. 2004.

[26] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, 2007.

[27] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in *Proc. 11th ACM Conf. Comput. Commun. Secur. (CCS)*, 2004, pp. 168–177.

[28] V. Kumar, H. Li, J.-M. Park, K. Bian, and Y. Yang, "Group signatures with probabilistic revocation: A computationally-scalable approach for providing privacy-preserving authentication," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2015, pp. 1334–1345.

[29] N. M. Smith, D. Johnston, G. W. Cox, and A. Shaliv, "Device, method, and system for secure trust anchor provisioning and protection using tamper-resistant hardware," U.S. Patent 2014 0095 867, Apr. 3, 2012.

[30] J. G. Proakis and M. Salehi, *Digital Communications*, 5th ed. New York, NY, USA: McGraw-Hill, 2008.

[31] G. D. Forney, Jr., "Maximum-likelihood sequence estimation of digital sequences in the presence of intersymbol interference," *IEEE Trans. Inf. Theory*, vol. 18, no. 3, pp. 363–378, May 1972.

[32] G. D. Forney, Jr., "The Viterbi algorithm," *Proc. IEEE*, vol. 61, no. 3, pp. 268–278, Mar. 1973.

[33] A. Dutta and M. Chiang, "'See something, say something' crowdsourced enforcement of spectrum policies," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 67–80, Jan. 2016.

[34] J.-S. Um, S.-H. Hwang, and B. J. Jeong, "A comparison of PHY layer on the Ecma-392 and IEEE 802.1 laf standards," in *Proc. 7th Int. ICST Conf. Cognit. Radio Oriented Wireless Netw. Commun. (CROWNCOM)*, Jun. 2012, pp. 313–319.

Vireshwar Kumar received the bachelor's degree in electrical engineering from IIT Delhi, India, in 2009. He is currently pursuing the Ph.D. degree with Virginia Tech, USA. He was with Dar Consultants, Pune, India, as an Electrical Engineer, before moving to the Indian Institute of Science, Bangalore, India, in 2010, as a Project Assistant. He joined the Department of Electrical and Computer Engineering, Virginia Tech, in 2011. His research interests include security issues in wireless networks and dynamic spectrum access networks.

Jung-Min (Jerry) Park received the Ph.D. degree in electrical and computer engineering from Purdue University, West Lafayette, IN, USA, in 2003. He is currently a Professor with the Department of Electrical and Computer Engineering, Virginia Tech, and the Site Director of an NSF Industry–University Cooperative Research Center called Broadband Wireless Access and Applications Center (BWAC). As the Site Director of BWAC at Virginia Tech, he is leading several sponsored research projects on wireless networks and network security. He is widely recognized for his pioneering work on enforcement and security problems in cognitive radio networks and spectrum sharing. His research interests include cognitive radio networks, spectrum sharing, wireless security and privacy, applied cryptography, and wireless communications and networking. His current or recent research sponsors include the National Science Foundation, the National Institutes of Health, the Defense Advanced Research Projects Agency, the U.S. Army Research Office, the Office of Naval Research, and a number of industry sponsors. Recently, he has been elected to serve as an Executive Committee Member of the National Spectrum Consortium (NSC) starting in 2016. He was a recipient of a 2014 Virginia Tech College of Engineering Faculty Fellow Award, a 2008 NSF Faculty Early Career Development Award, a 2008 Hoeber Excellence in Research Award, and a 1998 AT&T Leadership Award. The primary mission of the NSC is to improve collaboration between the industry, government, and academia to advance research and development of technologies to enhance the utilization of the electromagnetic spectrum. The Executive Committee is the NSC leadership and governance body authorized to oversee the activities of the Consortium. He is currently serving on the Editorial Boards of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and the IEEE/KICS JOURNAL OF COMMUNICATIONS AND NETWORKS.

Kaigui Bian received the B.S. degree in computer science from Peking University, in 2001, and the Ph.D. degree in computer engineering from Virginia Tech, in 2011. He is currently an Associate Professor with the Institute of Network Computing and Information Systems, School of Electrical Engineering and Computer Sciences, Peking University. His research interests include cognitive radio networks, mobile computing, network security, and privacy.