Journal of Network and Computer Applications 91 (2017) 52–60

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Transmitter authentication using hierarchical modulation in dynamic spectrum sharing☆

Vireshwar Kumar[a,*], Jung-Min (Jerry) Park[a], Kaigui Bian[b]

[a] *Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA 24061, USA*
[b] *School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China*

ARTICLE INFO

Keywords:
Dynamic spectrum sharing
Transmitter authentication
PHY-layer authentication

ABSTRACT

One of the critical challenges in dynamic spectrum sharing (DSS) is identifying non-conforming transmitters that violate spectrum access rules prescribed by a spectrum regulatory authority. One approach for facilitating identification of the transmitters in DSS is to require every transmitter to embed an uniquely-identifiable authentication signal in its waveform at the PHY-layer. In most of the existing PHY-layer authentication schemes, the authentication signal is added to the message signal as noise, which leads to a tradeoff between the message signal's signal-to-noise ratio (SNR) and the authentication signal's SNR under the assumption of constant average transmitted power. This implies that one cannot improve the former without sacrificing the latter, and vice versa. In this paper, we propose a novel PHY-layer authentication scheme called *Hierarchical Modulation with Modified Duobinary Signaling for Authentication* (HMM-DSA), which relaxes the constraint on the aforementioned tradeoff. HMM-DSA utilizes a modified duobinary filter to introduce some controlled amount of inter-symbol interference into the message signal, and embeds the authentication signal in the form of filter coefficients. Our results show that the proposed scheme, HMM-DSA, improves the error performance of the message signal as compared to the prior art.

1. Introduction

It is widely believed that *dynamic spectrum sharing* (DSS) is one approach for significantly increasing spectrum utilization efficiency. In a DSS environment, secondary users (SUs) opportunistically access fallow radio spectrum that is not utilized by primary (a.k.a. incumbent) users (PUs). SUs are required to follow a set of spectrum access rules or regulations prescribed by a spectrum regulatory authority (e.g., the Federal Communications Commission (FCC) in the U.S.A.) to protect the PUs from interference, and to minimize inter-SU interference. Therefore, to ensure the viability of the spectrum sharing model, effective and low-cost spectrum (rule) enforcement measures must be adopted (Park et al., 2014; Dutta and Chiang, 2016). Spectrum rule enforcement is an especially critical issue when federal government (including military) systems share spectrum with non-government systems, such as the case in the 3.5 GHz band in which commercial small-cell networks are expected to coexist with incumbent military radar systems (Altamimi et al., 2013; FCC, 2015).

In spectrum enforcement and security, one of the critical challenges is identifying, and if possible authenticating, non-conforming ("rogue") or malfunctioning SU transmitters that have violated spectrum access rules. To authenticate transmitters, cryptographic mechanisms at the higher layers have been used. However, the ability to authenticate and/or uniquely identify SU transmitters at the PHY-layer is especially useful in heterogeneous coexistence environments, where incompatible systems (i.e., systems with different protocol stacks) cannot decode each others' higher-layer signaling—e.g., IEEE 802.22 and 802.11af systems coexisting in TV white space (Feng et al., 2013). In a PHY-layer authentication scheme for spectrum enforcement, all SUs are 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). Tamper resistance mechanisms are employed to prevent the circumvention of the authentication mechanism by hacking (Smith et al., 2012; Xiao et al., 2009).

In this paper, we define two types of intended receivers—*unaware* and *aware* receivers (Yu et al., 2008a). An unaware receiver is able to correctly demodulate and decode the message signal, but cannot authenticate the received signals, either because it has no knowledge of the authentication scheme or does not know the key required for

☆ Portions of this work were presented in Kumar et al. (2014).
* Corresponding author.
E-mail address: viresh@vt.edu (V. Kumar).

http://dx.doi.org/10.1016/j.jnca.2017.05.007
Received 12 June 2016; Received in revised form 7 March 2017; Accepted 10 May 2017
Available online 10 May 2017
1084-8045/ © 2017 Elsevier Ltd. All rights reserved.

authenticating the transmitter. Also, a receiver that does not intend to authenticate the received signals is classified as an unaware receiver. On the other hand, a receiver that needs to recover the message signal as well as the authentication signal (embedded into the message signal) in order to identify the transmitter and authenticate its signals is called an aware receiver.

A conventional PHY-layer authentication scheme should embed the authentication signal into the message signal such that it enables the aware receiver to extract the message and the authentication signals from its received signal, while at the same time, enables the unaware receiver to recover the message signal from its received signal *without* requiring the unaware receiver to change its demodulation or decoding procedure. One approach to achieve this is to add the authentication signal to the message signal as noise (Yu et al., 2008a). To limit the detrimental effects of the authentication signal on the message signal, the principle of hierarchical modulation (Yu et al., 2008b, Tan et al., 2011) is often applied—i.e., the authentication signal (low priority signal) is carried on the low-power, high-resolution constellation while the message signal (high priority signal) is embodied by the high-power, low-resolution constellation.

In such an approach, both the aware receiver and the unaware receiver decode the message signal in the presence of the authentication signal, thus resulting in decreased signal-to-noise ratio (SNR) for the message signal, assuming average transmission power has not been increased to embed the authentication signal. Hence, 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 embedded signal at the receiver (Jiang et al., 2012). This means that there is a fundamental *tradeoff* in the existing schemes between the SNRs (and the error performances) of the message signal and the authentication signal.

In this paper, we propose a novel PHY-layer authentication scheme, called *Hierarchical Modulation with Modified Duobinary Signaling for Authentication* (HMM-DSA), that can be used by the aware receivers to identify rogue SU transmitters without significantly affecting the error performance of the message signal at the aware and the unaware receivers. The proposed scheme is based on duobinary signaling, a waveform shaping technique that has been traditionally used to increase bandwidth efficiency (Pasupathy, 1977), and hierarchical modulation, a technique to enable multi-resolution signaling (Ramchandran et al., 1993). In HMM-DSA, a hierarchically modulated duobinary signal is generated by inducing controlled inter-symbol interference (ISI) into the message signal. The controlled ISI is introduced by utilizing a modified duobinary filter whose coefficients are generated by using the authentication signal. In this way, HMM-DSA embeds the authentication signal into the message signal as well as relaxes the constraint on the aforementioned tradeoff that plagues the existing schemes.

The main contributions of this paper are summarized below.

- We propose the PHY-layer authentication scheme, HMM-DSA, in which the intended receiver can be either an aware receiver (which extract both the message and authentication signals) or an unaware receiver (which only extracts the message signal).
- We show that our approach enables significant improvement in the error performance of the message signal at the aware receiver when compared to that at the unaware receiver. We also show that HMM-DSA outperforms the prior art in terms of the detection performance of the message signal at the aware receiver.
- We have implemented HMM-DSA on Universal Software Radio Peripheral (USRP) radio boards, and provided testbed experiment results that corroborate our simulation results.

The rest of the paper is organized as follows. We provide the related work in Section 2. We describe the problem statement for PHY-layer authentication in Section 3, and discuss HMM-DSA in Section 4. We analyze the error performance of HMM-DSA in Section 5, and compare HMM-DSA with the prior art in Section 6. We discuss the experimental validation of HMM-DSA in Section 7, and conclude the paper by highlighting the main contributions in Section 8.

2. Related work

Based on the definitions of the aware and unaware receivers, the PHY-layer authentication schemes in the existing literature can be broadly divided into two categories. The schemes in the first category do not enable the intended receivers to function as the unaware receivers (Goergen et al., 2010; Yang et al., 2012; Miller and Trappe, 2011; Kumar et al., 2016; Jin et al., 2015). This means that in these schemes, all the intended receivers need to know the employed authentication mechanisms to demodulate and decode the message signals. In other words, these schemes require every intended receiver to be an aware receiver.

The schemes in the second category enable the intended receivers to be unaware receivers (Yu et al., 2008a, 2008b; Tan et al., 2011; Jin et al., 2015; Kumar et al., 2014). This means that in these schemes, the intended receivers are able to decode and demodulate the message signals without the knowledge of the employed PHY-layer authentication mechanisms. In Yu et al. (2008a), the authentication signal is added to the message signal as noise. In Yu et al. (2008b), Tan et al. (2011), Jin et al. (2015), the technique of hierarchical modulation is employed, and the authentication signal is carried on the high-resolution constellation while the message signal is embodied by low-resolution constellation where the average power of the embedded signal remains the same as the original message signal (with unmodified constellation). In these schemes, this embedding procedure leads to a fundamental tradeoff between the SNRs of the message signal and the authentication signal. The scheme proposed in Kumar et al. (2014) avoids the aforementioned tradeoff, but has very low authentication rate (i.e., the rate at which the authentication bits are embedded into the message bits).

3. Problem description

3.1. Model

In this paper, we assume the following authentication scenario. Alice, Bob, and Charlie share the same wireless medium. Alice (a.k.a "transmitter") intends to transmit messages to Bob (a.k.a. "aware receiver") and Charlie (a.k.a. "unaware receiver") via the wireless medium as per the rules established for DSS. Alice and Bob have agreed on an authentication scheme that allows Bob to verify the messages he receives from Alice. Charlie does not know the authentication scheme, and cannot authenticate Alice's messages at the PHY-layer, but can demodulate and decode the message signal.

3.2. Challenges

In the above model, the operations performed by Alice can be decomposed into two parts—generation of the authentication signal, and embedding of the authentication signal into the message signal. Similarly, the operations performed by Bob can be decomposed into two parts—extraction of the authentication signals from the received signal, and verification of the authentication signal. Hence, there are two distinct technical problems in devising a PHY-layer authentication scheme: (1) generating the authentication signal that later needs to be verified by an aware receiver; and (2) embedding the authentication signal into the message signal that later needs to be extracted by an aware receiver. To solve the first problem successfully, various threats need to be considered and mitigated (Tan et al., 2011; Goergen et al., 2010; Yang et al., 2012; Kumar et al., 2016, 2014). In this paper, we do not consider the first problem, and only focus on the second problem.