Extrinsic Channel-Like Fingerprint Embedding for Authenticating MIMO Systems

Nate Goergen, W. Sabrina Lin, K. J. R. Liu, T. Charles Clancy

***Abstract*—A framework for introducing an extrinsic fingerprint signal to space-time coded transmissions at the physical layer is presented, where the fingerprint signal conveys a low capacity cryptographically secure authentication message of arbitrary length. The multi-bit digital fingerprint message conveyed by the fingerprint signal is available to all users within reception range and is used to authenticate the fingerprinted transmission. A novel approach is discussed where the fingerprint signaling mechanism mimics distortions similar to time-varying channel effects. Specifically, the fingerprint is detectable to receivers considering previous channel state information, but will be ignored by receivers equalizing according to current channel state information. Two example fingerprint signaling mechanisms and detection rules are presented based on pulse-amplitude keying and phase-shift keying approaches. The methods for obtaining the real (intrinsic) channel estimate, the extrinsic fingerprint message, and the primary transmission are analytically demonstrated using general pilot embedding schemes. The worst-case distortions caused by non-ideal equalization of a fingerprinted message are derived using the 2x2 Alamouti code. Simulation results including bit error rate (BER) and model mismatch error using a maximum-likelihood (ML) receiver are presented for both the primary and fingerprint signal, while authentication signal BERs *lower* than the primary signal are demonstrated.**

***Index Terms*—MIMO, spectrum sensing, dynamic spectrum access, authentication, physical-layer, primary user authentication.**

I. Introduction

With the widespread adoption of wireless communication, the security of wireless systems has become an extensively researched topic. While cryptographic methods at higher layers have been widely used to authenticate wireless users and prevent interception of transmissions by malicious or unintended users, the ability to authenticate and classify wireless transmissions at the physical (PHY) layer has a number of advantages over higher-layer approaches. Authentication at the PHY-layer, before demodulating and decoding the signal, can prevent wasteful processing of unintended transmissions and allows nodes to quickly authenticate legitimate users and implicate charlatans. Additionally, PHY-layer approaches provide a completely independent authentication mechanism decoupled from higher-layer authentication devices or protocols, allowing the authentication mechanism to be invariant of higher-level protocol changes or revisions. In general, robust authentication devices are crucial to securing wireless systems against message forgery and the malicious actions of impostors, thereby preventing a number of identity attacks to next-generation wireless systems [1], [2], [3], [4], [5].

Message fingerprinting, where a message conveying the credentials of a data source is appended to the data, has been successfully applied to multimedia systems allowing for secure transmission of multimedia content [6]. The fingerprint message is traditionally designed to be very small compared to the bandwidth required by the primary transmission, to minimize transmission overhead. Since very little capacity is required to transmit the authentication message when compared to the original transmission, and since the fingerprint processing mechanism can have completely independent synchronization requirements, robust physical layer fingerprint signals can be designed to allow for signal authentication even when the signal itself is unrecoverable due to low signal to noise ratio (SNR) or fading conditions. This key advantage helps address the needs of next-generation cooperative communication applications, such as Relaying and Dynamic Spectrum Access, where nodes are required to operate correctly (i.e. avoid occupied spectrum) even in scenarios when they cannot decode the transmissions they receive.

With this approach we are fingerprinting the modulated, PHY-layer signal and not the bits of the primary transmission's payload. A number of PHY-layer fingerprinting approaches for wireless digital communications have been investigated, using basic blind signal superposition methods. In [7] the superposition of low-power pseudo random sequences on digital television transmissions is discussed. In [8] and in [9] multi-resolution approaches are considered for narrowband signals, where a low-power fingerprint constellation is superimposed onto the main signal constellation. In [10] the innate characteristics of radio hardware are used for device identification, and in [11] general fingerprinting through superposition is discussed.

The main disadvantage of blind superposition is that the fingerprint signal appears as additional noise in the primary signal and is fully present when the signal is decoded, resulting in decreased SNR for the original signal. Instead, we investigate a fingerprinting approach that exploits how the primary signal will be distorted by the channel and perceived by the recipient, resulting in improved fingerprint designs. As a result, the undesirable effects of the fingerprint signal associated with blind superposition approaches [8] and [9] can be partially removed by the receiver through traditional channel equalization practices.

In [12] it was demonstrated that robust PHY-layer fingerprints can be obtained from intrinsic characteristics of

Manuscript received January 9, 2011; revised May 11, 2011 and August 31, 2011; accepted September 2, 2011. The associate editor coordinating the review of this paper and approving it for publication was I.-M. Kim.

The authors are with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD, 20742, USA (e-mail: goergen@umd.edu).

Digital Object Identifier 10.1109/TWC.2011.101211.110045

wireless channels, such as unique scattering environments and spatial variability, to authenticate the transmitter without additional signal superposition. This work demonstrated that transmitters can be validated when the multipath channel profiles for each transmitter are unique and sufficiently stationary. However, when channel conditions are not conducive to intrinsic fingerprint recognition, due to either highly correlated multipath profiles between transmitters or rapidly varying channel conditions, a more robust fingerprint is required to authenticate wireless nodes. We consider augmenting current intrinsic channel-based authentication mechanisms with an extrinsic synthetically-generated digital signal of an arbitrary length in bits, that is applied by the transmitter to convey a cryptographically secure digital signature along with the primary transmission. The authentication message is broadcast to all users allowing every user within range to authenticate the primary transmission. We aim to design 'channel-like' fingerprint signals that can be modeled as time-variant channel distortions which are subsequently corrected at the receiver through traditional channel equalization and synchronization methods. In other words, the channel-like fingerprint signal and intrinsic time-variant channel effects share the same signal space. In our previous work [13], the details of a cryptographically secure arbitrary-length digital signature by using an extrinsic channel-like fingerprint for narrowband single-input single-output (SISO) digital television signals was considered.

In this paper we extend our work in [14], which considers one fingerprinting function for Space-Time Coded (STC) transmissions.

This paper is organized as follows. Section II introduces the multiple-input multiple-output (MIMO) system model and presents a framework for embedding a channel-like fingerprint signal of an arbitrary length in bits. In Section III the extraction of the intrinsic channel state, the extrinsic fingerprint message, and the primary transmission are demonstrated. Section IV presents two fingerprint signaling functions and accompanying detection rules, and the performance of these functions are derived. In Section V we discuss the structure of a basic digital authentication message. In VI we present bit error rate simulations for the example fingerprinting functions, and in Section VII we present our conclusions.

II. System Model and Problem Formulation

We assume the transmitter and receiver are MIMO systems with L_t transmit antennas and L_r receive antennas, with a STC transmitted at index t described by matrix $\mathbf{U}[t]$ of size $L_t \times M$. The STC $\mathbf{U}[t]$ transmitted across all L_t transmit antennas in M time slots is a composite signal composed of both the original STC transmission data, which will be referred to as the primary signal, and pilot signals used for channel estimation. When the fingerprinting function $\mathbf{F}[t]$ is applied by the transmitter to the ST block $\mathbf{U}[t]$ before transmission, the block received at the receiver $\mathbf{Y}[t] \in \mathcal{C}^{L_r \times M}$ expressed in matrix form is

$$\mathbf{Y}[t] = \mathbf{H}[t]\mathbf{F}[t]\mathbf{U}[t] + \mathbf{N}[t], \tag{1}$$

where $\mathbf{H}[t] \in \mathcal{C}^{L_r \times L_t}$ is the channel coefficient matrix representing the intrinsic channel conditions experienced by the fingerprinted block at time t, and $\mathbf{F}[t] \in \mathcal{C}^{L_t \times L_t}$ is the fingerprinting function applied to the transmission. The channel noise $\mathbf{N}[t]$ is modeled as complex white Gaussian noise with zero mean and variance $(\sigma^2/2)\mathbf{I}_{(L_r \times M)}$. We assume the elements of $\mathbf{H}[t]$ to be independent Rayleigh fading and block-stationary, where $\mathbf{H}[t]$ remains constant over the block, or M symbols.

We now briefly describe the pilot-embedding framework presented in [15], which provides the edifice for the construction of $\mathbf{U}[t]$. We will demonstrate how our channel-like fingerprinting scheme conveys the fingerprint message through strategic manipulation of the pilot signals used for channel estimation, that are embedded in the transmission.

The transmission $\mathbf{U}[t]$ consists of a ST code data-bearer matrix $\mathbf{D}[t] \in \mathcal{C}^{L_t \times N}$ and data-projection matrix $\mathbf{A} \in \mathcal{R}^{N \times M}$. Here, N is the number of time slots reserved exclusively for data transmission, while time slots $M - N$, $N < M$ are reserved for data mixed with embedded pilot signals. The ST symbol $\mathbf{U}[t]$ with embedded pilots signals, becomes

$$\mathbf{U}[t] = \mathbf{D}[t]\mathbf{A} + \mathbf{P}, \tag{2}$$

where $\mathbf{P} \in \mathcal{R}^{L_t \times M}$ is the pilot matrix. The salient point of this data-bearing framework is that most pilot-embedding schemes can be generalized through the superposition of the data-bearing structure $\mathbf{D}[t]\mathbf{A}$ and the pilot matrix $\mathbf{P}[t]$. The data-projection and pilot matrix satisfy the following properties:

$$\begin{aligned} \mathbf{A}\mathbf{P}^H &= \mathbf{0} \in \mathcal{R}^{N \times L_t}, \quad \mathbf{A}\mathbf{A}^H = \mathbf{I} \in \mathcal{R}^{N \times N} \\ \mathbf{P}\mathbf{P}^H &= \mathbf{I} \in \mathcal{R}^{L_t \times L_t}. \end{aligned} \tag{3}$$

The properties (3) of the data-projection matrix $\mathbf{A}$ and $\mathbf{P}$ essentially allow $\mathbf{A}$ to project the data component $\mathbf{D}[t]$ onto the orthogonal subspace of the pilot matrix $\mathbf{P}$, allowing for signal demodulation by means of a Maximum Likelihood (ML) receiver. The expanded form of the signal at the receiver (1), with (2) becomes

$$\mathbf{Y}[t] = \mathbf{H}[t]\mathbf{X}[t]\mathbf{A} + \mathbf{H}[t]\mathbf{F}[t]\mathbf{P} + \mathbf{N}[t], \tag{4}$$

where $\mathbf{X}[t] = \mathbf{F}[t]\mathbf{D}[t]$ is the fingerprinted data transmission before projection by $\mathbf{A}$.

The heterogeneous wireless broadcast system we consider has two types of receivers:

- The *unaware receiver*: Regular, unmodified, MIMO receivers that will ignore the fingerprint signal and employ traditional channel equalization and data detection
- The *aware receiver*: Receivers designed to detect and decode the fingerprint in addition to the primary signal

To the *unaware* receiver the distortions introduced by the fingerprinting function $\mathbf{F}[t]$ can be combined with the channel distortions $\mathbf{H}[t]$ and will be subsequently removed through equalization. This is because we consider the case where the fingerprinting function $\mathbf{F}[t]$ is applied to both the pilot and data signals of the transmission, consistent with the distortions introduced by the intrinsic channel response. A MMSE equalizer operating on current CSI will reverse both the intrinsic and extrinsic channel-like distortions using the block's pilot signals as reference. This process will be explained analytically in a moment.

The *aware* receiver must detect the fingerprinting signal in the presence of time-variant channel distortions. We consider the case where the intrinsic channel estimate $\mathbf{H}[t]$ is delineated from the extrinsic fingerprinting component $\mathbf{F}[t]$ through periodic omission of the fingerprint signal $\mathbf{F}[t]$, which will serve as the channel sounding mechanism allowing for estimation of the intrinsic channel state only. Under this assumption, the coherence time of the channel will play an important role in the detection probability of $\mathbf{F}[t]$, since time-varying changes in $\mathbf{H}[t]$ will become noise when detecting $\mathbf{F}[t]$.

Since channel coherence over many blocks is a strong assumption for general time-variant channels [16], especially in high mobility scenarios when channel state is quickly changing, we consider here the most frequent channel sounding case where the fingerprint signal is omitted every even block and present on every odd block, yielding a fingerprint transmission with a 50 percent duty-cycle. With this design, channel coherence over only two blocks is sufficient for detecting our fingerprint message and a channel with less stationary behavior will result in degraded performance. Changing our time index to reflect this design, when $t = 2Mk$, the fingerprint is not present in the transmission and $\mathbf{F}[t]$ is replaced by the identity matrix, $\mathbf{I}$, for the channel sounding block. When $t = 2Mk - M$, $\mathbf{F}[t]$ is transmitted. Thus the received signal with the fingerprinting function applied to every other block transmission becomes

$$\mathbf{Y}[t] = \begin{cases} \mathbf{H}[t]\mathbf{U}[t] + \mathbf{N}[t], & t = 2Mk, \\ \mathbf{H}[t]\mathbf{F}[t]\mathbf{U}[t] + \mathbf{N}[t], & t = 2Mk - M. \end{cases} \tag{5}$$

While (5) considers a differential modulation where the perceived channel changes every block, in [13] *channel-tracking* equalizers were discussed. This work demonstrated that when equalizers that track channel state are employed, distortion to the primary-signal can be avoided by simply extending the symbol length of the fingerprinting function to be longer than the *forgetting period* of the equalizer. By increasing the length of the fingerprinting symbol, and thus decreasing the authentication symbol rate, (5) can be extend to any scenario where the equalizer ignores previous channel state beyond some finite duration.

When the coherence time of the channel is large the correlation between $\mathbf{H}[2Mk]$ and $\mathbf{H}[2Mk-M]$ is significant, and the fingerprint function can be decoded correctly with a higher probability. Conversely, as the coherence time of the channel decreases, there is less mutual information between the current and outdated CSI and the performance of fingerprint decoder degrades. The correlation between time-varying channel estimates are discussed in [17], [18] and [19].

To ensure fair analysis of the fingerprinting system, the fingerprinting function is designed according to transmission energy constraint

$$||\mathbf{X}[t]||_F = ||\mathbf{D}[t]||_F = P_o, \tag{6}$$

where $||\cdot||_F$ represents the Frobenius norm. Therefore, according to (5) the fingerprinting function $\mathbf{F}[t]$ must be designed such that $||\mathbf{F}[t]||_F = \sqrt{L_t}$, maintaining an equi-energy transmission for the period when the fingerprint is present, i.e. during $\mathbf{Y}[2Mk - M]$, and when it is omitted, i.e. during $\mathbf{Y}[2Mk]$.

Extending the time-varying channel model used in [12] to MIMO transmissions, we consider a generalized time-variant channel response matrix for the intrinsic component of the channel $\mathbf{H}[t]$, where each scalar complex gain element $H_{i,j}[t]$ for rows $i = 0, \ldots, L_r - 1$ and columns $j = 0, \ldots, L_t - 1$ is the summation of three model components:

- A fixed time-invariant channel gain denoted $\bar{H}_{i,j} = E\left[H_{i,j}[t]\right]$
- A zero-mean time-variant channel gain component denoted $\mu_{i,j}[t]$
- A zero-mean receiver noise component denoted $N_{i,j}[t]$,

where $\bar{H}_{i,j}$ is the mean of the random variable $H_{i,j}[t]$. Thus, $H_{i,j}[t]$ becomes

$$H_{i,j}[t] = \bar{H}_{i,j} + \mu_{i,j}[t] + N_{i,j}[t]. \tag{7}$$

While in general each mean of the channel gains, $\bar{H}_{i,j}$, will be changing in time, we will assume that this component will remain stationary over the duration of the channel sounding symbol and adjacent fingerprinted symbol in (5). We obtain the following matrix definition for the time-varying channel

$$\begin{aligned} \mathbf{H}[t] &= \left(\bar{\mathbf{H}} + \boldsymbol{\mu}[t]\right) + \mathbf{N}[t] = \\ &\begin{bmatrix} \bar{H}_{0,0} + \mu_{0,0}[t] & \cdots & \bar{H}_{0,L_t-1} + \mu_{0,L_t-1}[t] \\ \vdots & \ddots & \vdots \\ \bar{H}_{L_r-1,0} + \mu_{L_r-1,0}[t] & \bar{H}_{L_r-1,L_t-1} + \mu_{L_r-1,L_t-1}[t] \end{bmatrix} \\ &+ \begin{bmatrix} N_{0,0}[t] & \cdots & N_{0,L_t-1}[t] \\ \vdots & \ddots & \vdots \\ N_{L_r-1,0}[t] & \cdots & N_{L_r-1,L_t-1}[t] \end{bmatrix}, \end{aligned} \tag{8}$$

where each element $N_{i,j}[t]$ is zero-mean complex Gaussian noise with variance σ_N^2 representing the normalized receiver noise projected on the pilot signals, assuming the projected noise is uniformly distributed over $\mathbf{P}^H$ (i.e. the pilot signals are optimally embedded into the transmission). We model the time-variant portion of the channel response gain for each element of $\boldsymbol{\mu}[t]$ corresponding as an independent first-order autoregressive (AR-1) model. The AR-1 model has been used to describe time-variant channels in previous works [11], and [20], [12]. Assuming an average AR-1 noise power σ_T^2 over all time-variant gain elements $\mu_{i,j}[t]$, the AR-1 model is given as

$$\mu_{i,j}[t] = a\mu_{i,j}[t-1] + \sqrt{(1-a^2)}u_{i,j}[t]. \tag{9}$$

The AR model coefficient a in (9) represents the influence of the previous time-variant channel gain component $\mu_{i,j}[t-1]$ on the current estimate $\mu_{i,j}[t]$.The random component of the time-variant channel $\mu_{i,j}[t]$ is represented in (9) by $u_{i,j}[t] \sim \mathcal{CN}(0, \sigma_T^2)$, thus $E\left[\mu_{i,j}[t]\right] = 0, \forall i, j$. We consider the case where the AR model coefficient a, and the noise power σ_T^2 are the same for each independent channel i, j.

III. Fingerprint Analysis

Upon receiving the signal, the first step for both aware and unaware receivers is channel estimation. The channel estimation problem is to extract and estimate channel distortions in the received signal (5) for performing channel equalization and further recovering $\mathbf{D}[t]$. By post-multiplying both sides of (5) by $\mathbf{P}^H$ and using the properties in (3), the channel

response $\mathbf{H}[t]$ can be estimated from the received signal during the channel-sounding symbol at $t = \tau_0 = 2Mk$

$$\begin{aligned}\mathbf{Y}[\tau_0]\mathbf{P}^H &= (\mathbf{H}[\tau_0](\mathbf{D}[\tau_0]\mathbf{A}+\mathbf{P})+\mathbf{N}[\tau_0])\,\mathbf{P}^H \\ &= \mathbf{H}[\tau_0]+\mathbf{N}[\tau_0]\mathbf{P}^H,\end{aligned} \tag{10}$$

where $\mathbf{N}[t]\mathbf{P}^H$, the channel estimate noise in (8), is the projection of the noise vector onto pilot signals and represents noise in the channel estimate.

Similarly the joint intrinsic and extrinsic channel distortions, $\mathbf{H}[2Mk]$ and $\mathbf{F}[t]$, can be estimated from the received signal (5) during the fingerprinted symbol at $\tau_1 = 2Mk - M$

$$\begin{aligned}\mathbf{Y}[\tau_1]\mathbf{P}^H &= (\mathbf{H}[\tau_1]\mathbf{F}[\tau_1](\mathbf{D}[\tau_1]\mathbf{A}+\mathbf{P})+\mathbf{N}[\tau_1])\,\mathbf{P}^H \\ &= (\mathbf{H}[\tau_1]\mathbf{F}[\tau_1])+\mathbf{N}[\tau_1]\mathbf{P}^H,\end{aligned} \tag{11}$$

Combining results from (10) and (11), the channel estimate at the receiver, $\hat{\mathbf{H}}[t]$, becomes

$$\hat{\mathbf{H}}[t] = \begin{cases}\mathbf{H}[t]+\mathbf{N}[t]\mathbf{P}^H, & t=\tau_0=2Mk,\\ \mathbf{H}[t]\mathbf{F}[t]+\mathbf{N}[t]\mathbf{P}^H, & t=\tau_1=2Mk-M,\end{cases} \tag{12}$$

where $\mathbf{N}[t]\mathbf{P}^H$ is the normalized projected channel estimate noise. Since $\mathbf{N}[t]$ is uniformly distributed Gaussian noise, and since proper design of $\mathbf{P}$ should ensure that pilot symbols are placed such that channel conditions are uniformly estimated throughout the ST block, then $\mathbf{N}[t]\mathbf{P}^H$ should also have a uniform noise distribution.

A. Data Recovery

After the channel has been estimated via (10) and (11), the next step preformed by the receiver is the recovery of the transmitted data $\mathbf{D}[t]$. By post-multiplying both sides of (5) by $\mathbf{A}^H$ and using the properties (3), the data signal $\mathbf{D}[t]$ can be extracted from the received signal (5) during the channel-sounding symbol transmitted at $\tau_0 = 2Mk$, i.e.

$$\mathbf{Y}[\tau_0]\mathbf{A}^H = \mathbf{H}[\tau_0]\mathbf{D}[\tau_0]+\mathbf{N}[\tau_0]\mathbf{A}^H. \tag{13}$$

For the sake of exposition, we consider here the case where the number of transmit antenna and the number of receive antenna are equal, or $L_r = L_t$, and that $\hat{\mathbf{H}}[t]$ is invertible, which is the case considered later in simulation. Inversion for the case when $L_r \neq L_t$ is obtainable via a number of methods such as the pseudoinverse, however this topic is beyond the scope of this paper. An estimate for the intrinsic channel response $\hat{\mathbf{H}}[\tau_0]$ is produced via (10), and thus the data signal can be recovered by pre-multiplying (13) by the inverse of the normalized channel estimate produced by the MMSE estimator, or $\hat{\mathbf{H}}^{-1}[\tau_0]$. When the channel is perfectly estimated for either the τ_0 or τ_1 block, i.e.

$$\hat{\mathbf{H}}^{-1}[t] = \mathbf{H}^{-1}[t],\ t=\tau_0 \text{ or } \tau_1 \tag{14}$$

the extracted data signal at $t = \tau_0 = 2Mk$ is

$$\begin{aligned}\hat{\mathbf{D}}[\tau_0] =& \hat{\mathbf{H}}^{-1}[\tau_0]\mathbf{Y}[\tau_0]\mathbf{A}^H \\ =& \mathbf{D}[\tau_0]+\hat{\mathbf{H}}^{-1}[\tau_0]\mathbf{N}[\tau_0]\mathbf{A}^H.\end{aligned} \tag{15}$$

Similarly, when post-multiplying by $\mathbf{A}^H$ for $t = \tau_1 = 2Mk - M$

$$\mathbf{Y}[\tau_1]\mathbf{A}^H = \mathbf{H}[\tau_1]\mathbf{F}[\tau_1]\mathbf{D}[\tau_1]+\mathbf{N}[\tau_1]\mathbf{A}^H, \tag{16}$$

an estimate for the intrinsic channel response combined with the extrinsic response $\hat{\mathbf{H}}[\tau_0]\mathbf{F}[\tau_1]$ is produced via (11) and the data signal can be recovered by pre-multiplying (16) by $\left(\hat{\mathbf{H}}[\tau_1]\mathbf{F}[\tau_1]\right)^{-1}$. For the perfectly estimated channel (14) the extracted data signal at $t = \tau_1 = 2Mk - M$ becomes

$$\hat{\mathbf{D}}[\tau_1] = \mathbf{D}[\tau_1]+\left(\hat{\mathbf{H}}[\tau_1]\mathbf{F}[\tau_1]\right)^{-1}\mathbf{N}[\tau_1]\mathbf{A}^H. \tag{17}$$

We note that from (11) and (17) it has been shown that the data signal $\mathbf{D}[\tau_1]$ can be recovered from $\mathbf{Y}[\tau_1]$ in the presence of the fingerprinting distortion $\mathbf{F}[\tau_1]$ without explicitly extracting and detecting the fingerprinting function $\mathbf{F}[\tau_1]$. Thus the primary transmission in the proposed fingerprinting system can be recovered independently from the fingerprint detection by both the aware and unaware receivers.

A further advantage to the proposed system is that channel estimates obtained during (10) and (11), and subsequent channel equalization steps preformed in (15) and (17) are identical steps taken by an unmodified/unaware receiver. Thus, we have demonstrated that the fingerprinted signal is received by unaware receivers without modification to the receiver, channel estimation procedure, or equalization device when generalized pilot embedding and channel estimation are employed.

B. Fingerprint Detection

We now consider two methods for detecting the fingerprint signal given the sequence of channel state information in (12).

The first detection rule, also considered in [12], is the differential channel estimate denoted $\mathbf{Z}_{SUB}[\tau_1,\tau_0]$. This detection rule is useful for detecting amplitude differences between the even and odd block transmissions in (5), i.e. our differential fingerprint signaling method, and is obtained by subtracting the sounding symbol estimate from the fingerprinted symbol estimate. Under the assumption that the fingerprinting function is transmitted independently from the channel response, their difference becomes

$$\begin{aligned}&E\left[\mathbf{Z}_{SUB}[\tau_1,\tau_0]\right] = E\left[\mathbf{Y}[\tau_1]\mathbf{P}^H-\mathbf{Y}[\tau_0]\mathbf{P}^H\right] \\ =&E\left[\bar{\mathbf{H}}\mathbf{F}[\tau_1]\right]+E\left[\boldsymbol{\mu}[\tau_1]\mathbf{F}[\tau_1]\right]+E\left[\mathbf{N}[\tau_1]\right]- \\ &E\left[\bar{\mathbf{H}}\right]-E\left[\boldsymbol{\mu}[\tau_0]\right]-E\left[\mathbf{N}[\tau_0]\right] \\ =&\bar{\mathbf{H}}\mathbf{F}[\tau_1]-\bar{\mathbf{H}}.\end{aligned} \tag{18}$$

From (18) we note that this detector is unbiased, since only the means $\bar{\mathbf{H}}$ and $\mathbf{F}[t]$ are present.

We also consider the Hadamard product, or element-wise product between two matrices, for detecting fingerprinting functions perturbing signal phase. Denoted $\mathbf{Z}_{HAD}[\tau_1,\tau_0]$, this detection rule is the element-wise product between the channel sounding estimate and the conjugate of the fingerprinted channel estimate, and is given as

$$\begin{aligned}&E\left[\mathbf{Z}_{HAD}[\tau_1,\tau_0]\right] = E\left[\left(\mathbf{Y}[\tau_1]\mathbf{P}^H\right)\circ\left(\mathbf{Y}[\tau_0]\mathbf{P}^H\right)^*\right] \\ =&E\left[\left(\bar{\mathbf{H}}\mathbf{F}[\tau_1]\right)\circ\bar{\mathbf{H}}^*\right]+E\left[\left(\bar{\mathbf{H}}\mathbf{F}[\tau_1]\right)\circ\boldsymbol{\mu}^*[\tau_0]\right]+ \\ &E\left[\mathbf{N}[\tau_1]\circ\boldsymbol{\mu}^*[\tau_0]\right]+E\left[\left(\boldsymbol{\mu}[\tau_1]\mathbf{F}[\tau_1]\right)\circ\mathbf{N}^*[\tau_0]\right]+ \\ &E\left[\left(\boldsymbol{\mu}[\tau_1]\mathbf{F}[\tau_1]\right)\circ\bar{\mathbf{H}}^*\right]+E\left[\mathbf{N}[\tau_1]\circ\bar{\mathbf{H}}^*\right]+ \\ &E\left[\left(\boldsymbol{\mu}[\tau_1]\mathbf{F}[\tau_1]\right)\circ\boldsymbol{\mu}^*[\tau_0]\right]+E\left[\mathbf{N}[\tau_1]\circ\mathbf{N}^*[\tau_0]\right]+ \\ &E\left[\left(\bar{\mathbf{H}}\mathbf{F}[\tau_1]\right)\circ\mathbf{N}^*[\tau_0]\right] \\ =&||\bar{\mathbf{H}}||^2\mathbf{F}[\tau_1],\end{aligned} \tag{19}$$

where $(\circ)$ represents the Hadamard product and $(*)$ represents conjugation. Here the perturbation factor can be extracted from the argument of the product of the individual scalar estimates. We will use these two detectors in the following fingerprint examples and demonstrate their performance.

IV. Some Fingerprinting Scenarios

We now consider some simple fingerprinting functions as candidates for $\mathbf{F}[t]$. We will give examples for each fingerprinting function using the 2x2 Alamouti code [21] according to the polar representation of the complex valued intrinsic channel model (8), i.e.

$$\begin{aligned}\mathbf{H}[t] &= \begin{bmatrix}\bar{H}_{0,0}+\mu_{0,0}[t] & \bar{H}_{0,1}+\mu_{0,1}[t]\\ \bar{H}_{1,0}+\mu_{1,0}[t] & \bar{H}_{1,1}+\mu_{1,1}[t]\end{bmatrix}\\ &\quad+\begin{bmatrix}N_{0,0}[t] & N_{0,1}[t]\\ N_{1,0}[t] & N_{1,1}[t]\end{bmatrix}\\ &= \begin{bmatrix}\alpha_1 e^{j\theta_1} & \alpha_3 e^{j\theta_3}\\ \alpha_2 e^{j\theta_2} & \alpha_4 e^{j\theta_4}\end{bmatrix}+\begin{bmatrix}\mu_1[t] & \mu_3[t]\\ \mu_2[t] & \mu_4[t]\end{bmatrix}+\\ &\quad\begin{bmatrix}N_1[t] & N_3[t]\\ N_2[t] & N_4[t]\end{bmatrix},\end{aligned} \tag{20}$$

where the indices $\{i,j\}$ are serialized to $1,2,\ldots,L_tM$ first column-wise and then row-wise, for simplicity of notation. Here $\bar{H}_{i,j}$ is represented in polar form, with amplitude $\alpha_x,\ x=1,\ldots,ML_t$ and angle $\theta_x,\ x=1,\ldots,ML_t$. In the case of the 2x2 code, $N=L_t=2$.

A. Antenna Amplitude Modulation (AAM)

The first fingerprinting function we consider introduces a gain offset of ϵ between symbols to be transmitted by each antenna such that the overall transmission energy constraint is withheld. This function can also be thought of as a modulation of the gain of each antenna, and will be designated with the subscript AAM. The antenna gain fingerprinting function for the 2x2 code (i.e. $L_t=2,\ M=3,\ N=2$) can be represented as

$$\mathbf{F}_{AAM}[t]=\gamma\begin{bmatrix}1-\epsilon & 0\\ 0 & 1+\epsilon\end{bmatrix},\ |\epsilon|<1, \tag{21}$$

where γ is a normalization constant used to maintain the constant energy constraint as in (6). For the AAM fingerprinting function this normalization constant becomes

$$\gamma=\frac{1}{\sqrt{1+\epsilon^2}}. \tag{22}$$

Since the AAM fingerprinting function perturbs the amplitude of transmitted symbols, we apply the differential channel test statistic (18) to detect amplitude distortions between channel estimates. Using (18) and (20) applied to the AAM fingerprint function (21), test statistic for the 2x2 Alamouti code, denoted $\mathbf{Z}_{AAM}[\tau_1,\tau_0]$, becomes

$$\begin{aligned}&\mathbf{Z}_{AAM}[\tau_1,\tau_0]=E\left[\mathbf{Z}_{SUB}[\tau_1,\tau_0]\right]=\bar{\mathbf{H}}\mathbf{F}[\tau_1]-\bar{\mathbf{H}}\\ &=\begin{bmatrix}\alpha_1(1-\epsilon)e^{j\theta_1} & \alpha_3(1+\epsilon)e^{j\theta_3}\\ \alpha_2(1-\epsilon)e^{j\theta_2} & \alpha_4(1+\epsilon)e^{j\theta_4}\end{bmatrix}-\\ &\begin{bmatrix}\alpha_1 e^{j\theta_1} & \alpha_3 e^{j\theta_3}\\ \alpha_2 e^{j\theta_2} & \alpha_4 e^{j\theta_4}\end{bmatrix}=\begin{bmatrix}-\epsilon\alpha_1 e^{j\theta_1} & \epsilon\alpha_3 e^{j\theta_3}\\ -\epsilon\alpha_2 e^{j\theta_2} & \epsilon\alpha_4 e^{j\theta_4}\end{bmatrix}.\end{aligned} \tag{23}$$

The estimates received in each time slot $i=0,\ldots,N-1$ for each antenna $j=0,1$ in (23), $Z_{AAM_{i,j}}$, can be combined by subtracting the amplitude of the estimates corresponding to the signals received by each antenna, i.e. the columns of (23). The ensemble estimate for ϵ becomes,

$$\begin{aligned}\hat{\epsilon}&=\sum_{i=0}^{N-1}Re\{Z_{AAM_{i,1}}[\tau_1,\tau_0]\}-\sum_{i=0}^{N-1}Re\{Z_{AAM_{i,0}}[\tau_1,\tau_0]\}\\ &=(\epsilon\alpha_3+\epsilon\alpha_4)-(-\epsilon\alpha_1-\epsilon\alpha_2)=\epsilon\lambda,\qquad \lambda=\sum_{i=1}^{L_tN}\alpha_i,\end{aligned} \tag{24}$$

is the total channel gain measured during the sounding symbol transmitted at $t=\tau_0$.

From (24) we see that the performance of the test signal $\mathbf{Z}_{AAM}[\tau_1,\tau_0]$ depends on the aggregate signal gain of the channel λ and the value chosen for the perturbation amplitude ϵ. Therefore when using the AAM fingerprinting function we conclude that the symbol error rate (SER) for the authentication signal, and thus the detection performance of the fingerprint for the aware receiver, can be improved by increasing ϵ at the transmitter.

To analyze the performance of this fingerprinting function, we must also compute the variance of the test statistic. This computation, similar to the proof in [12], becomes

$$\begin{aligned}&Var\left[\mathbf{Z}_{SUB}[\tau_1,\tau_0]\right]\\ &=Var\left[\left(\mathbf{H}[\tau_1]\mathbf{F}[\tau_1]+\mathbf{N}[\tau_1]\mathbf{P}^H\right)-\left(\mathbf{H}[\tau_0]+\mathbf{N}[\tau_0]\mathbf{P}^H\right)\right]\\ &=Var\left[\boldsymbol{\mu}[\tau_1]\mathbf{F}[\tau_1]\right]+Var\left[\boldsymbol{\mu}[\tau_0]\right]+Var\left[\mathbf{N}[\tau_1]\mathbf{P}^H\right]\\ &-2Cov\left[\boldsymbol{\mu}[\tau_1]\mathbf{F}[\tau_1],\boldsymbol{\mu}[\tau_0]\right]+Var\left[\mathbf{N}[\tau_0]\mathbf{P}^H\right].\end{aligned} \tag{25}$$

Due to the design of the AAM fingerprinting function, the gain of the j^{th} column of (23) is either increased or decreased by the perturbation factor ϵ, thus (25) becomes

$$\begin{aligned}&Var\left[\mathbf{Z}_{SUB}[\tau_1,\tau_0]\right]=\\ &\begin{cases}\sigma_T^2(1+(1-2a)(1-\epsilon)^2)+\sigma_N^2, & j{=}0,i{=}0,\ldots,N{-}1\\ \sigma_T^2(1+(1-2a)(1+\epsilon)^2)+\sigma_N^2, & j{=}1,i{=}0,\ldots,N{-}1.\end{cases}\end{aligned} \tag{26}$$

Therefore, the total variance of the estimate (24) for the 2x2 code becomes

$$\sigma_\epsilon^2=Var\left[\hat{\epsilon}\right]=\frac{\sigma_T^2(2(1-a)+\epsilon^2(1-2a))+\sigma_N^2}{L_tN}. \tag{27}$$

If we select a typical antipodal binary signal constellation for the AAM fingerprint function $\mathbf{F}$ with parameter ϵ, i.e.

$$\mathbf{F}_{AAM}[t]\in\left\{\gamma\begin{bmatrix}1-\epsilon & 0\\ 0 & 1+\epsilon\end{bmatrix},\ \gamma\begin{bmatrix}1+\epsilon & 0\\ 0 & 1-\epsilon\end{bmatrix}\right\}, \tag{28}$$

it can be shown that the symbol error rate for the maximum-likelihood fingerprint detector detecting the transmitted fingerprint function $\mathbf{F}$ from the noisy estimate at the receiver $\hat{\mathbf{F}}$ is

$$P\left[\hat{\mathbf{F}}\neq\mathbf{F}\right]=Q\left(\sqrt{\frac{2\epsilon^2\lambda^2}{\sigma_\epsilon}}\right), \tag{29}$$

where $Q(\cdot)$ is the Gaussian tail function. We note that the variance (27) decreases linearly as the number of elements in

the code increases, i.e. as L_t or N increase, however we also note that the variance also increases quadratically in ϵ.

B. AAM Fingerprint Distortion

We now consider the distortions experienced by the Maximum Ratio Combining (MRC) decoder operating on the 2x2 Alamouti code when equalizing the AAM-fingerprinted signal $\mathbf{Y}[\tau_1]$ according to an incorrect channel estimate that considers only the intrinsic channel estimate, i.e. if $\mathbf{H}[\tau_0]$ were used as the channel estimate for a symbol transmitted at $t = \tau_1 = 2k$ instead of $\mathbf{H}[\tau_1]\mathbf{F}[\tau_1]$. This important result delineates the worst-case degradation in performance the MRC receiver would experience due to channel model estimate mismatch, which generally destroys the orthogonality of the signals in the transmitted space-time code $\mathbf{D}[t]$. These distortions might be applicable to unaware receivers with non-adaptive equalization, and demonstrates how the perturbation parameter ϵ must be carefully chosen to limit maximum signal degradation when considering a heterogeneous system of receivers. For the 2x2 Alamouti code,

$$\mathbf{D}[t] = \begin{bmatrix} d_1 & -d_2^* \\ d_2 & d_1^* \end{bmatrix}, \tag{30}$$

the transmitted symbol $\mathbf{X}[t]$ with fingerprinting function (21) becomes

$$\begin{aligned} \mathbf{X}_{AAM}[t] &= \begin{bmatrix} 1-\epsilon & 0 \\ 0 & 1+\epsilon \end{bmatrix} \begin{bmatrix} d_1 & -d_2^* \\ d_2 & d_1^* \end{bmatrix} \\ &= \begin{bmatrix} d_1(1-\epsilon) & -d_2^*(1-\epsilon) \\ d_2(1+\epsilon) & d_1^*(1+\epsilon) \end{bmatrix}. \end{aligned} \tag{31}$$

The data signal estimate using MRC on the extracted data (15), using (20) becomes

$$\mathbf{Y}_{AAM}[t] = \begin{bmatrix} r_1 & r_3 \\ r_2 & r_4 \end{bmatrix} + \mathbf{N}[t]\mathbf{P}^H, \tag{32}$$

where

$$\begin{aligned} r_1 = &\quad \alpha_1 d_1(1-\epsilon)e^{j\theta_1} + \alpha_3 d_2(1+\epsilon)e^{j\theta_3} \\ r_3 = &-\alpha_1 d_2^*(1-\epsilon)e^{j\theta_1} + \alpha_3 d_1^*(1+\epsilon)e^{j\theta_3} \\ r_2 = &\quad \alpha_2 d_1(1-\epsilon)e^{j\theta_2} + \alpha_4 d_2(1+\epsilon)e^{j\theta_4} \\ r_4 = &-\alpha_2 d_2^*(1-\epsilon)e^{j\theta_2} + \alpha_4 d_1^*(1+\epsilon)e^{j\theta_4}. \end{aligned} \tag{33}$$

The estimates of the received signal using an MRC receiver with model mismatch distortion from the fingerprinting function present are given as

$$\begin{aligned} \tilde{d}_{1_{AAM}} = &\ \hat{\alpha}_1 e^{-j\hat{\theta}_1}\left(\alpha_1 d_1(1-\epsilon)e^{j\theta_1} + \alpha_3 d_2(1+\epsilon)e^{j\theta_3}\right) \\ &+ \hat{\alpha}_2 e^{-j\hat{\theta}_2}\left(\alpha_2 d_1(1-\epsilon)e^{j\theta_2} + \alpha_4 d_2(1+\epsilon)e^{j\theta_4}\right) \\ &+ \hat{\alpha}_3 e^{j\hat{\theta}_3}\left(-\alpha_1 d_2(1-\epsilon)e^{-j\theta_1} + \alpha_3 d_1(1+\epsilon)e^{-j\theta_3}\right) \\ &+ \hat{\alpha}_4 e^{j\hat{\theta}_4}\left(-\alpha_2 d_2(1-\epsilon)e^{-j\theta_2} + \alpha_4 d_1(1+\epsilon)e^{-j\theta_4}\right) \\ &+ \eta_1, \\ \tilde{d}_{2_{AAM}} = &\ \hat{\alpha}_3 e^{-j\hat{\theta}_3}\left(\alpha_1 d_1(1-\epsilon)e^{j\theta_1} + \alpha_3 d_2(1+\epsilon)e^{j\theta_3}\right) \\ &+ \hat{\alpha}_4 e^{-j\hat{\theta}_4}\left(\alpha_2 d_1(1-\epsilon)e^{j\theta_2} + \alpha_4 d_2(1+\epsilon)e^{j\theta_4}\right) \\ &- \hat{\alpha}_1 e^{j\hat{\theta}_1}\left(-\alpha_1 d_2(1-\epsilon)e^{-j\theta_1} + \alpha_3 d_1(1+\epsilon)e^{-j\theta_3}\right) \\ &- \hat{\alpha}_2 e^{j\hat{\theta}_2}\left(-\alpha_2 d_2(1-\epsilon)e^{-j\theta_2} + \alpha_4 d_1(1+\epsilon)e^{-j\theta_4}\right) \\ &+ \eta_2. \end{aligned} \tag{34}$$

where

$$\begin{aligned} \eta_1 = &\ \alpha_1 e^{-j\theta_1} N_1 + \alpha_2 e^{j\theta_2} N_2^* + \\ &\alpha_3 e^{-j\theta_3} N_3 + \alpha_4 e^{j\theta_1} N_4^*, \\ \eta_2 = &-\alpha_1 e^{j\theta_1} N_2^* + \alpha_2 e^{-j\theta_2} N_1 - \\ &\alpha_3 e^{j\theta_3} N_4^* + \alpha_4 e^{-j\theta_1} N_3, \end{aligned} \tag{35}$$

represent the the combined receiver noise in the estimates of d_1 and d_2, respectively. In (34), $\hat{\alpha}_1, \hat{\alpha}_2, \hat{\alpha}_3, \hat{\alpha}_4$ are the complex channel gain estimates for the intrinsic channel given by (20), produced by the receiver during $\mathbf{H}[2Mk]$, $\hat{\theta}_1, \hat{\theta}_2, \hat{\theta}_3, \hat{\theta}_4$ are the channel phase estimates, and N_1, N_2, N_3, N_4 are the elements of $\mathbf{N}[t]\mathbf{P}^H$. We consider the case where the intrinsic channel component is perfectly coherent over the channel sounding symbol and the fingerprinted symbol, thus the time-variant component $\boldsymbol{\mu}[t]$ of (20) is omitted, i.e. $\boldsymbol{\mu}[\tau_1] = \boldsymbol{\mu}[\tau_0] = \mathbf{0}$, thus in the noiseless case, when $\mathbf{N}[\tau_1] = \mathbf{N}[\tau_0] = \mathbf{0}$, the channel estimates for $t = \tau_1$ and $t = \tau_0$ are equal

$$\hat{\mathbf{H}}[\tau_1] = \quad \hat{\mathbf{H}}[\tau_0], \tag{36}$$

thus the estimates for channel amplitude and phase have perfectly determined the intrinsic channel response, or

$$\hat{\mathbf{H}}[t] = \mathbf{H}[t] = \begin{bmatrix} \hat{\alpha}_1 e^{j\hat{\theta}_1} & \hat{\alpha}_3 e^{j\hat{\theta}_3} \\ \alpha_2 e^{j\hat{\theta}_2} & \hat{\alpha}_4 e^{j\hat{\theta}_4} \end{bmatrix} = \begin{bmatrix} \alpha_1 e^{j\theta_1} & \alpha_3 e^{j\theta_3} \\ \alpha_2 e^{j\theta_2} & \alpha_4 e^{j\theta_4} \end{bmatrix}, \tag{37}$$

leaving only distortions due to the presence of the extrinsic fingerprint. Using (37), after some manipulation, (34) becomes

$$\begin{aligned} \tilde{d}_{1_{AAM}} = &\ (\lambda - \epsilon(\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4))d_1 + \\ &2\epsilon(\alpha_1\alpha_3 e^{j(\theta_3-\theta_1)} + \alpha_2\alpha_4 e^{j(\theta_4-\theta_2)})d_2 + \eta_1, \\ \tilde{d}_{2_{AAM}} = &\ (\lambda - \epsilon(\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4))d_2 - \\ &2\epsilon(\alpha_1\alpha_3 e^{j(\theta_1-\theta_3)} + \alpha_2\alpha_4 e^{j(\theta_2-\theta_4)})d_1 + \eta_2, \end{aligned} \tag{38}$$

From (38) we notice that an AAM-fingerprinted Alamouti code improperly equalized according to outdated CSI (i.e. CSI that does not reflect the distortions introduced by the fingerprinting function), is degraded in amplitude by an amount proportional to ϵ. Specifically, the estimate for d_1 is degraded in amplitude by $\epsilon(-\alpha_1 - \alpha_2)$ and a cross signal is introduced from the d_2 signal proportional to 2ϵ. Similar distortions are experienced for the d_2 symbol, which is also degraded by $\epsilon(-\alpha_1 - \alpha_2)$. These are the worse-case distortions incurred due to channel model estimate miss-match when using (21) as a fingerprinting function, and demonstrates the importance of selecting ϵ when considering receivers with lower performance equalizers. For example, when the equalizer used by a receiver has a particularly slow learning curve, or if there is delay between when the channel is estimated and when this estimate can be used for equalization, the receiver can equalize the channel according to an outdated channel model and thus model mismatch distortions will occur.

We note that when the data symbol $\mathbf{D}[t]$ is equalized and decoded according to current CSI, (10) and (11), the intrinsic and extrinsic channel distortions will be corrected when decoding the symbols $\mathbf{D}[\tau_0]$ and $\mathbf{D}[\tau_1]$. Thus, when channel model mismatch error during the fingerprinted symbol (14) is omitted, $\mathbf{D}[t]$ will be recovered using the MMSE channel estimate according to (16) and (17). The primary

signal estimates for the 2x2 Alamouti code when the antenna amplitude offset is properly corrected by equalization becomes

$$\tilde{d}_1 = \lambda^{(2)} d_1 + \eta_1, \quad \tilde{d}_2 = \lambda^{(2)} d_2 + \eta_2, \quad \lambda^{(2)} = \sum_{i=1}^{L_t N} \alpha_i^2, \tag{39}$$

which is the anticipated performance for the 2x2 MRC Alamouti decoder with the perfect channel estimation assumption.

C. Antenna Phase Modulation (APM)

We now consider a fingerprinting function that introduces a phase offset between the signals to be transmitted by each antenna, denoted with the subscript APM. The fingerprinting function for the 2x2 code can be written

$$\mathbf{F}_{APM}[t] = \begin{bmatrix} e^{-j\epsilon} & 0 \\ 0 & e^{j\epsilon} \end{bmatrix}, \ 0 \le \epsilon < 2\pi. \tag{40}$$

Since the APM fingerprinting function introduces a phase perturbation, we apply the Hadamard product detector (19). The APM fingerprinting function in (40) and equation (20) for the 2x2 code becomes

$$\begin{aligned} \mathbf{Z}_{APM}[\tau_1,\tau_0] &= E\left[\mathbf{Z}_{HAD}[\tau_1,\tau_0]\right] \\ &= E\left[\begin{bmatrix} \alpha_1 e^{j(\theta_1-\epsilon)} & \alpha_3 e^{j(\theta_3+\epsilon)} \\ \alpha_2 e^{j(\theta_2-\epsilon)} & \alpha_4 e^{j(\theta_4+\epsilon)} \end{bmatrix} \circ \begin{bmatrix} \alpha_1 e^{-j\theta_1} & \alpha_3 e^{-j\theta_3} \\ \alpha_2 e^{-j\theta_2} & \alpha_4 e^{-j\theta_4} \end{bmatrix}\right] \\ &= \begin{bmatrix} \alpha_1^2 e^{-j\epsilon} & \alpha_3^2 e^{j\epsilon} \\ \alpha_2^2 e^{-j\epsilon} & \alpha_4^2 e^{j\epsilon} \end{bmatrix}. \end{aligned} \tag{41}$$

Combining all scalar estimates from (41) by averaging the scalar estimates corresponding to the signals received by each antenna and taking the conjugate of the estimates from the second column, the ensemble estimate for ϵ becomes,

$$\begin{aligned} e^{-j\hat{\epsilon}} &= \sum_{j=0}^{N} Z_{APM_{1,j}}[\tau_1,\tau_0] + \sum_{j=0}^{N} Z^*_{APM_{0,j}}[\tau_1,\tau_0] \\ &= \lambda^{(2)} e^{-j\epsilon}, \end{aligned} \tag{42}$$

where the disturbance factor ϵ can be recovered by taking the argument of (42), and $\lambda^{(2)} = \sum_{x=1}^{L_t N} \alpha_x^2$ is the anticipated signal gain for the 2x2 MRC Alamouti decoder with the perfect channel estimation assumption.

From (42) we see that the performance of the test signal $\mathbf{Z}_{APM}[\tau_1,\tau_0]$ depends on the aggregate signal gain of the channel $\lambda^{(2)}$ and the magnitude of the perturbation factor, ϵ. Therefore when using the APM fingerprinting function we conclude that the authentication signal SER can be decreased by increasing ϵ at the transmitter.

The variance of the detection rule (42) can be written,

$$\begin{aligned} &Var\left[\mathbf{Z}_{HAD}[\tau_1,\tau_0]\right] = \\ &\left(\sigma_N^2 + \sigma_T^2\right)^2 \mathbf{1} + 2\left(\sigma_N^2 + \sigma_T^2 + a\sigma_T^2 + a\sigma_T^4\right)\bar{\mathbf{H}}^{(2)}, \end{aligned} \tag{43}$$

where $\mathbf{H}^{(2)} = \mathbf{H} \circ \mathbf{H}^*$ represents the element-wise square operation on the matrix $\mathbf{H}$ and it's conjugate. Therefore, the total variance of the estimate (42) for the case where all elements of $\bar{\mathbf{H}}^{(2)}$ are equal, becomes

$$\sigma_\epsilon^2 = \frac{Var\left[\mathbf{Z}_{HAD}[\tau_1,\tau_0]\right]}{NL_t}. \tag{44}$$

If we select an antipodal signal constellation for (40) with phase perturbation parameter $\epsilon = \pi/2$, i.e.

$$\mathbf{F}[t] \in \left\{ \begin{bmatrix} e^{-j\pi/2} & 0 \\ 0 & e^{j\pi/2} \end{bmatrix}, \begin{bmatrix} e^{j\pi/2} & 0 \\ 0 & e^{-j\pi/2} \end{bmatrix} \right\}, \tag{45}$$

it can be shown that the symbol error rate for the maximum-likelihood fingerprint detector, detecting $\mathbf{F}$ from the received estimate $\hat{\mathbf{F}}$, is

$$P\left[\hat{\mathbf{F}} \neq \mathbf{F}\right] = Q\left(\lambda^{(2)} \sqrt{\frac{2}{\sigma_\epsilon}} \sin\left(\frac{\pi}{2}\right)\right), \tag{46}$$

where $Q(\cdot)$ is the Gaussian tail function. From (44) and (46) we observe that the authentication fingerprint signal SER decreases when N or L_t are increased, potentially allowing for fingerprint BERs lower than the primary signal BER in some channel stationarity conditions.

D. APM Fingerprint Distortion

We now consider worst case distortions present when equalizing the APM-fingerprinted signal according to incorrect channel information as was previously done for the AAM fingerprinting function. The transmitted symbol with fingerprinting function present, (40), becomes

$$\mathbf{X}[t] = \begin{bmatrix} e^{-j\epsilon} & 0 \\ 0 & e^{j\epsilon} \end{bmatrix} \begin{bmatrix} d_1 & -d_2^* \\ d_2 & d_1^* \end{bmatrix} = \begin{bmatrix} d_1 e^{-j\epsilon} & -d_2^* e^{-j\epsilon} \\ d_2 e^{j\epsilon} & d_1^* e^{j\epsilon} \end{bmatrix}, \tag{47}$$

and the received ST signal becomes

$$\mathbf{Y}_{AMP}[t] = \begin{bmatrix} r_1 & r_3 \\ r_2 & r_4 \end{bmatrix} + \mathbf{N}[t]\mathbf{P}^H, \tag{48}$$

where

$$\begin{aligned} r_1 &= \alpha_1 d_1 e^{j(\theta_1-\epsilon)} + \alpha_3 d_2 e^{j(\theta_3+\epsilon)}, \\ r_3 &= -\alpha_1 d_2^* e^{j(\theta_1-\epsilon)} + \alpha_3 d_1^* e^{j(\theta_3+\epsilon)}, \\ r_2 &= \alpha_2 d_1 e^{j(\theta_2-\epsilon)} + \alpha_4 d_2 e^{j(\theta_4+\epsilon)}, \\ r_4 &= -\alpha_2 d_2^* e^{j(\theta_2-\epsilon)} + \alpha_4 d_1^* e^{j(\theta_4+\epsilon)}. \end{aligned} \tag{49}$$

Thus, the signal estimates for d_{P_1} and d_{P_2} using MRC without correcting for the phase perturbation, denoted $\tilde{d}_{P_1}$ and $\tilde{d}_{P_2}$, become

$$\begin{aligned} \tilde{d}_{1_{APM}} &= \hat{\alpha}_1 e^{-j\hat{\theta}_1}\left(\alpha_1 d_1 e^{j(\theta_1-\epsilon)} + \alpha_3 d_2 e^{j(\theta_3+\epsilon)}\right) + \\ &\quad \hat{\alpha}_2 e^{-j\hat{\theta}_2}\left(\alpha_2 d_1 e^{j(\theta_2-\epsilon)} + \alpha_4 d_2 e^{j(\theta_4+\epsilon)}\right) + \\ &\quad \hat{\alpha}_3 e^{j\hat{\theta}_3}\left(-\alpha_1 d_2 e^{-j(\theta_1-\epsilon)} + \alpha_3 d_1 e^{-j(\theta_3+\epsilon)}\right) + \\ &\quad \hat{\alpha}_4 e^{j\hat{\theta}_4}\left(-\alpha_2 d_2 e^{-j(\theta_2-\epsilon)} + \alpha_4 d_1 e^{-j(\theta_4+\epsilon)}\right) + \eta_1, \\ \tilde{d}_{2_{APM}} &= -\hat{\alpha}_1 e^{j\hat{\theta}_1}\left(-\alpha_1 d_2 e^{-j(\theta_1-\epsilon)} + \alpha_3 d_1 e^{-j(\theta_3+\epsilon)}\right) - \\ &\quad \hat{\alpha}_2 e^{j\hat{\theta}_2}\left(-\alpha_2 d_2 e^{-j(\theta_2-\epsilon)} + \alpha_4 d_1 e^{-j(\theta_4+\epsilon)}\right) + \\ &\quad \hat{\alpha}_3 e^{-j\hat{\theta}_3}\left(\alpha_1 d_1 e^{j(\theta_1-\epsilon)} + \alpha_3 d_2 e^{j(\theta_3+\epsilon)}\right) + \\ &\quad \hat{\alpha}_4 e^{-j\hat{\theta}_4}\left(\alpha_2 d_1 e^{j(\theta_2-\epsilon)} + \alpha_4 d_2 e^{j(\theta_4+\epsilon)}\right) + \eta_2. \end{aligned} \tag{50}$$

Using (37), after some manipulation, (50) becomes

$$\begin{aligned} \tilde{d}_{1_{APM}} &= (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4) d_1 e^{-j\epsilon} + \eta_1, \\ \tilde{d}_{2_{APM}} &= (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4) d_2 e^{j\epsilon} + \eta_2, \end{aligned} \tag{51}$$

with η_1 and η_2 given in (35).

From (51) we observe the worst case distortions from the extrinsic APM fingerprint function when equalizing according to outdated CSI for the 2x2 Allmouti code. Here, worst case model mismatch error introduces a phase rotation of $e^{-j\epsilon}$ in $\tilde{d}_{1_{APM}}$, and $e^{j\epsilon}$ in $\tilde{d}_{2_{APM}}$. Because the amount of distortion APM fingerprint is also proportional to ϵ, we note that like the AAM fingerprinting function, care must be taken when choosing ϵ when the performance of equalizers employed by unaware receivers must be considered.

V. A Basic Authentication Message

While Sections III and IV describe the signaling mechanism for our fingerprint function, in this section we give an example of a digital authentication message that can be signaled using the fingerprint function and analyze the authentication performance.

Our fingerprint signaling scheme allows for the modulation of a digital authentication message of arbitrary length, and the fingerprint perturbation ϵ can be selected by the transmitter using discrete symbols from a signal constellation, and using an appropriate bit-to-symbol mapping the receiver can recover each symbol of the message via the AAM or APM detection rule. For example, the transmission and detection of consecutive authentication symbols over ρ fingerprinted blocks using a constelation of order ξ bits-per-symbol will yield a digital authentication message of $\rho\xi$ bits in length.

To address the needs of Dynamic Spectrum Access applications, the digital authentication message embedded in each node's transmission should contain bit fields for the basic self-verifying information of the signal such as the frequency, location, and time the signal is authorized for transmission. We will denote these fields as F, L, and T, respectively. A message hash of these parameters is then digitally signed using a secret key owned by the transmitter and included in the message, while a timestamp denoted TS is also included with the authentication message to prevent future replay of the message by malicious users. The timestamp allows for enforcement of an expiration deadline on the content of the message, and in the event that a previously used authentication message is received, with a timestamp that has passed the expiration deadline, it will be discarded by the receiver. The authentication message for an authorized user U_j, denoted $msg_{U_j,A}$, is given as

$$msg_{U_j,A} = \left\{TS, F, L, T, K_A^+, [Hash_m\,[TS, F, L, T]]_{K_A}\right\}, \tag{52}$$

where $[\cdot]_{K_A}$ is a digital signature of the content within $[\cdot]$ using the private key owned by the authorized users group, the subscript A is used to denote that user U_j is a member of the authorized users group A, K_A^+ is the public key of the authorized users group, and $Hash_m\,[\cdot]$ is message digest of length m for the content within $[\cdot]$. The hash algorithm $Hash_m\,[\cdot]$ can be any of a number of widely used collision-resistant hash algorithms which provide reasonable security against the malicious fabrication of messages. We assume that implementers adhere to modern security best practices when selecting hash algorithms.

A. Decoding of the Basic Authentication Message

To decode the authentication message, the receiver first recovers the all bits of the embedded fingerprint message and then extracts parameters from the payload of the message. Once each field has been extracted, the authenticity of the authorized user's groups' public key K_A^+ is verified from a mutually accepted trust anchor or certificate authority (CA). The receiver then independently verifies $[Hash_m\,[TS, F, L, T]]_{K_A}$ using the authorized user's groups' public key, which is embedded in the authentication message. Malicious forgery of the authentication message is prevented through the signature process and by including this signature as part of the authentication message. The modification of any subset of the authentication message parameters TS, F, L, and T, would cause the message signature to fail validation when it is received, enabling the receiver to detect and discard modified messages.

If the authenticity of K_A^+ and the message signature were both deemed valid, and the operating signal is within the specifications of F, L, and T, it will then be recognized as an authorized user. This authentication messaging system relies on the existence of a *trust anchor*, sometimes referred to as a Certificate Authority (CA), to verify the authenticity of K_A^+.

B. Message Security Evaluation

To be considered secure, cryptographic protocols need resist forgery, modification, deletion, and replay. Since we are considering a broadcast authentication system, where every user is able to decode and subsequently verify the fingerprint message, all notions of privacy are non-applicable since we want every user to have the ability to extract the authentication message.

By leveraging proven cryptographic primitives and best security practices in the design of the keys, message signatures, and message hashes, the probability of making an authentication error is reduced to the probability of a hash collision. A well designed hash algorithm such as SHA-1 will feature a collision probability which is nearly zero in all practical applications, thus preventing the acceptance of incorrect authentication messages. For example, when using a 64-bit message hash a malicious node would require approximately 5.1×10^9 attempts to achieve one collision using a brute force 'birthday' attack. Current best practices when using secure hashing algorithms suggest using at least a 256-bit hash, i.e. SHA-256, further decreasing the probability of an authentication error and making the probability of accepting an attacker-fabricated message virtually impossible.

Because the data payload signal, the pilot signals, and the authentication signal are all transmitted with the same coherent frame of reference, any PHY-layer attack targeting a subset of these components (i.e. an attack on the pilot signal transmissions alone) would cause so much degradation to the user data signal that the attack would be easily detectable. Effectively, at this point the attacker is merely a signal jammer, and jamming style attacks are outside of the scope of this manuscript.

The authentication message $msg_{U_j,A}$ is transmitted as a multi-bit digital signal, the probability of a fingerprint

detection miss is the same as the probability of receiving the entire authentication message with one or more bit errors. Because a single bit error in either the authentication message or the signature will cause the authentication to fail, the probability of missing the authentication message is the same as the probability of a at least one bit error in the message. Therefore for an uncoded binary transmission, the probability that the received authentication message is in error is simply

$$P[m\hat{s}g_A \neq msg_A] = 1 - (1 - P_e)^{B+C}, \qquad (53)$$

where P_e is the bit error rate(BER) in the authentication signal, where B is the total length of the fields $\{TS, F, L, T, K_A\}$ and C is the length of the signature $[Hash_m [TS, F, L, T]]_{K_A}$. The use of forward error correction (FEC) on the authentication signal, combined with a continuously repeated message (i.e. repetition encoding), can further decrease the probability of an authentication miss.

The authentication message in (52) also includes the frequency F that the transmitter is authorized to transmit on, which would presumably be associated with the transmitter's key and recorded by a CA like the FCC. Therefore even if we assume that an adversary can compromise an authorized user's key and forge $\mathbf{F}[k]$ at the PHY-layer, the attacker will be constrained to the frequency or frequencies prescribed by the compromised key. Using a forged $\mathbf{F}[k]$ on a frequency other than the original frequency prescribed by the key will implicate the transmission as a forgery when validating the credentials of the key against the CA's records.

VI. Simulation Results

We now present simulation results for the AAM fingerprinting constellation (28), for different values ϵ and channel AR model parameter a in (9), using the MMSE channel estimator, the 2x2 Alamouti ST code with $M = 4$, and $N = L_t = L_r = 2$. A QPSK constellation was used for the primary signal. In Section V-B we demonstrated that the authentication performance of arbitrary authentication messages can be computed directly from the fingerprint BER, therefore we will use BER in this section to demonstrate fingerprint signaling performance. The results for the AAM fingerprinting function for a fixed $\sigma_T = 0.01$ and values of a equal to 0.7 and 0.9 are presented in Figure 1. We observe that for both values of a, the authentication fingerprint is received with a BER advantage over the primary signal. We also see that the BER for the fingerprint signal is less when $a = 0.9$ than when $a = 0.7$, suggesting that the fingerprint signal performance does indeed depend on correlation between channel estimates in time, determined by the AR-1 model parameter a.

A plot of the BER for both the primary signal and authentication signal is given in Figure 2 for a fixed $a = 0.7$ and values of ϵ equal to 0.45 and 0.47. As the value of ϵ increases, the signal strength for the authentication signal increases, resulting in an improved BER for the authentication signal at the expense of a slight increase in channel estimate MSE for the primary-user. We observe that the AAM fingerprinting function yields an authentication signal BER advantage over the primary signal for $\epsilon = 0.47$, over the range of SNR plotted.

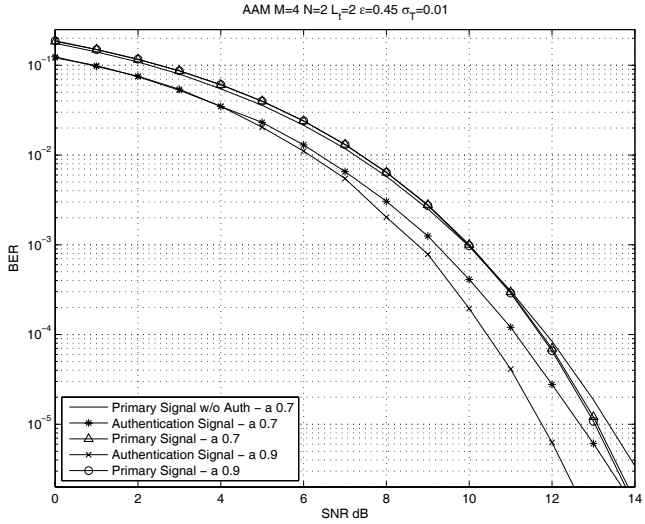


Fig. 1. BER for primary and AAM fingerprint signal for various a.

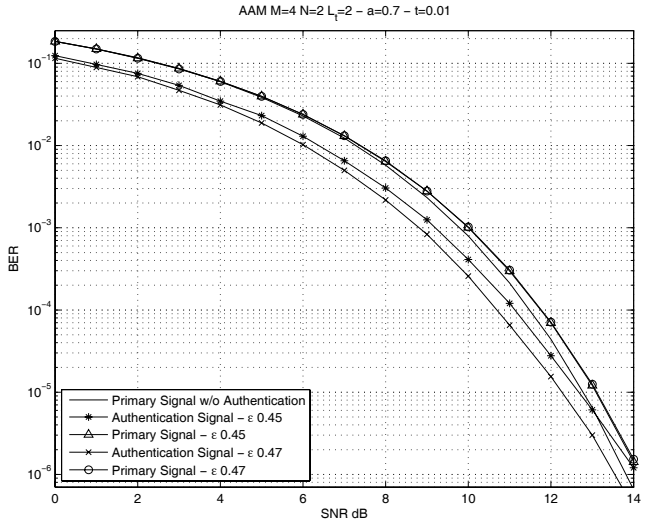


Fig. 2. BER for primary and AAM fingerprint signal for various ϵ.

In Figures 3 and 4 we present results for channel estimate MSE and the worst-case MSE for the simulations depicted in Figures 1 and 2, respectively. The worst-case MSE results represent the additional model error incurred if $\mathbf{Y}[\tau_1]$ were incorrectly equalized using $\mathbf{H}[\tau_0]$ as opposed to $\mathbf{H}[\tau_1]$, as suggested by (38).

We note that worst-case MSE is invariant of the AR-1 model parameter a, as the MSE for $a = 0.7$ and $a = 0.9$ are nearly indistinguishable. From Figure 4 we observe that increasing ϵ results in an increased channel model MSE as expected, and the worst-case error introduced by the fingerprinting function is apparent from the difference between MSE results when the fingerprint is present and when the fingerprint absent.

The results for the APM fingerprinting function for a fixed $\sigma_T = 0.3$ and values of a equal to 0.8 and 0.9, are presented in Figure 5. We observe that like the AAM function, the fingerprint is received with a greater BER advantage over primary signal for $a = 0.9$, suggesting that the APM fingerprint signal performance also depends on correlation between

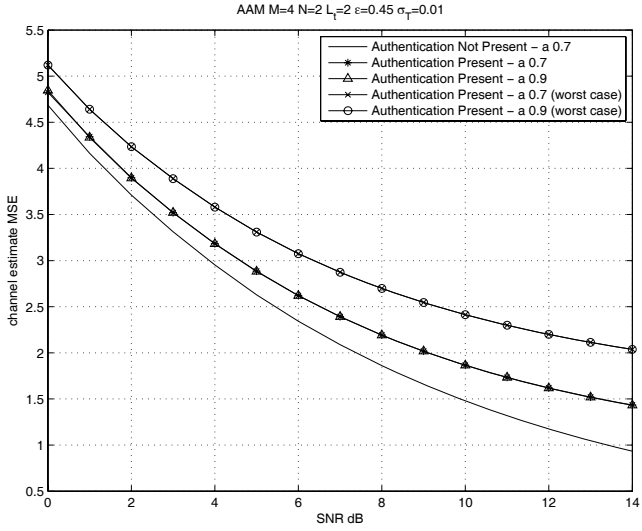


Fig. 3. MSE of the channel estimate with and without AAM fingerprint signal for various a.

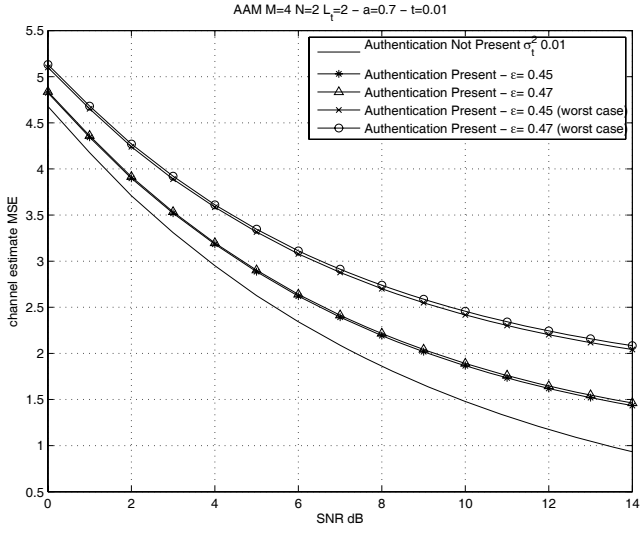


Fig. 4. MSE of the channel estimate with and without AAM fingerprint signal for various ϵ.

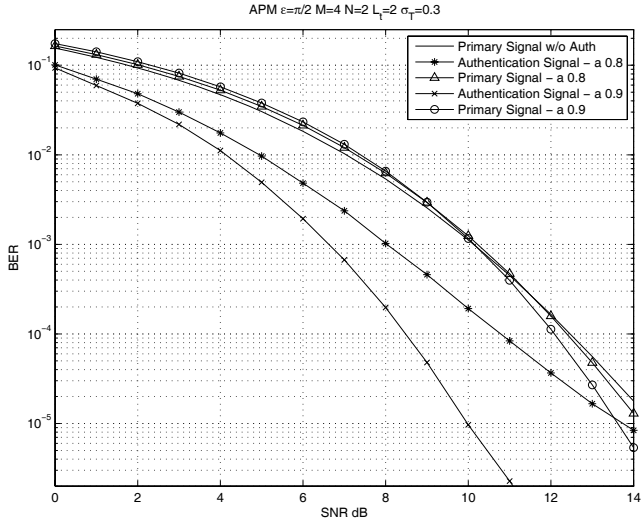


Fig. 5. BER for primary and APM fingerprint signal for various a.

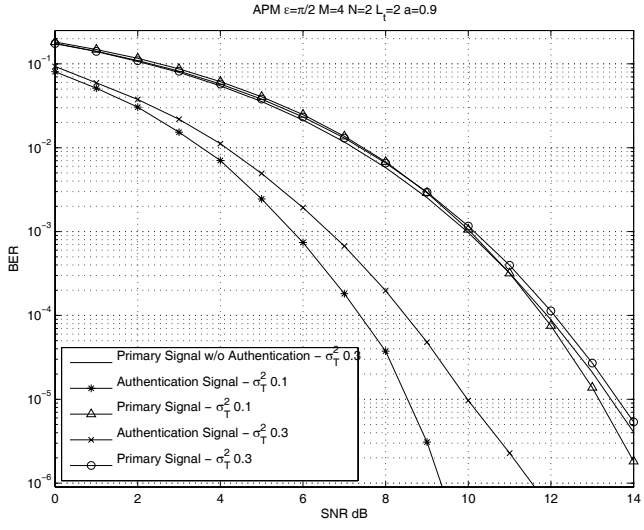


Fig. 6. BER for primary and APM fingerprint signal for various σ_T.

channel estimates in time, as determined by the AR-1 model parameter a. We also observe that in higher SNR, around 8dB, the slope of the BER curve for the authentication behaves differently for the case where $a = 0.8$, when compared to the authentication signal BER curve for $a = 0.9$. In particular, the authentication signal BER curve slope for $a = 0.8$ stops changing after 8dB. This can be explained as follows:

In our time-variant channel model (7), the channel matrix $H_{i,j}[t]$ is a summation of two independent noise processes, $N_{i,j}[t]$, which is a white Gaussian noise process with variance σ_N^2, and a colored Gaussian noise process $\mu_{i,j}[t]$, which is modeled as an AR-1 process driven by $u_{i,j}[t] \sim \mathcal{CN}(0, \sigma_T^2)$. For higher values of SNR, i.e. as σ_N^2 decreases, the dominating noise process when decoding the authentication signals becomes $\mu_{i,j}[t]$, and not $N_{i,j}[t]$. This effect becomes more pronounced as the bandwidth of the time-varying component $\mu_{i,j}[t]$ increases, which is inversely proportional to the AR-1 model parameter a. Thus, for large values of σ_T^2, the performance of the authentication signal degrades more rapidly under high SNR, as the value of a decreases. This is the scenario of rapidly varying channel.

A plot of the BER for both the primary signal and authentication signal is given in Figure 6 for a fixed $a = 0.9$ and values of σ_T equal to 0.1 and 0.3. As the value of σ_T^2 increases, the power of the time-varying channel component increases resulting in a greater channel estimate MSE for both the primary and authentication signal, and a decreased system BER for both signals. We note from Figure 6 that the APM fingerprint signal BER is lower than the primary for the range of SNR simulated.

In Figures 7 and 8 we plot the worst-case mean-squared error of the channel estimate using the APM fingerprinting function, suggested by (51), as was done for the AAM fingerprinting function. We observe the MSE, and worst-case MSE, experienced by the MMSE receiver, as suggested by (51). We note that worst-case MSE is relatively invariant of the AR-1 model parameter a, as the MSE for $a = 0.8$ and $a = 0.9$ are completely overlapping and indistinguishable. From Figure

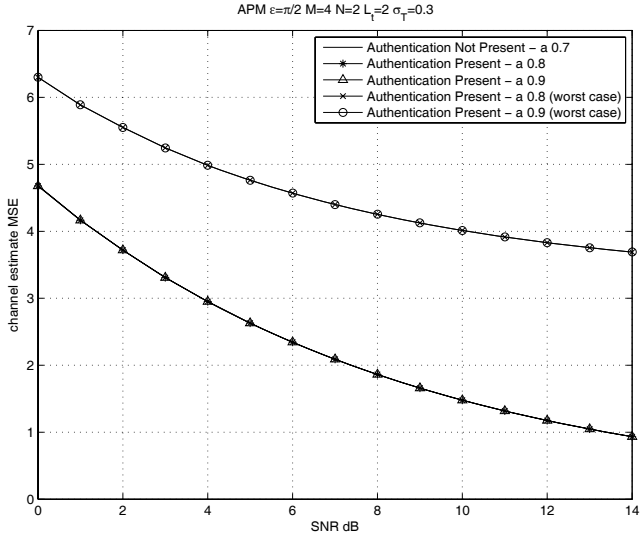


Fig. 7. MSE of the channel estimate with and without APM fingerprint signal for various a.

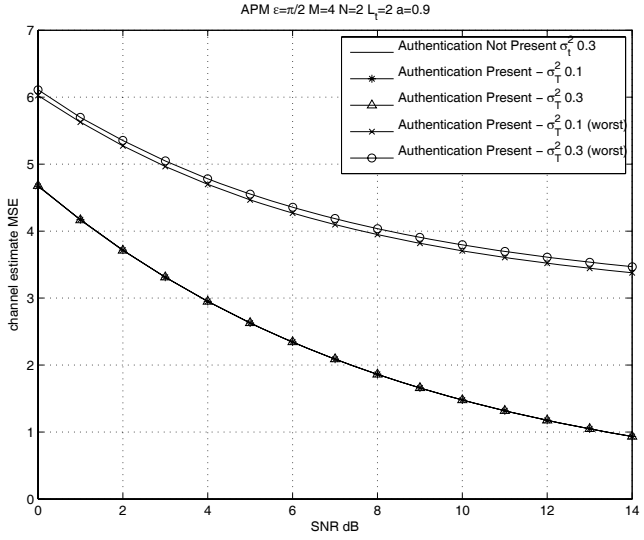


Fig. 8. MSE of the channel estimate with and without APM fingerprint signal for various σ_T.

8 we observe that increasing σ_T^2 results in an increased channel model MSE for worst-case distortions as expected, and the worst-case error introduced by the fingerprinting function is apparent from the difference between MSE results when the fingerprint is present and when the fingerprint absent.

We conclude from these results that the APM fingerprinting function generally has better performance over the AAM fingerprinting function, for larger values of σ_T^2, for given parameters.

VII. Conclusion

In this paper we presented a framework for fingerprinting MIMO transmissions with a digital PHY-layer message for the purpose of transmitter authentication. We demonstrated that the fingerprint signal can be added without modifying the decoding process of unaware, or traditional MIMO receivers. Further, the distortions introduced by the fingerprint can be partially removed by the receiver's equalizer to reduce the degradation in performance of the primary transmission. It was demonstrated that the fingerprint signal can be designed with a BER lower than the primary signal, and that the probability of symbol error for the proposed method improves as the correlation between time-varying channel estimates increases. Our proposed scheme provides the foundation of fingerprint signaling which can be used to embed authentication messages of arbitrary lengths for secure wireless transmissions.

References

[1] T. Clancy and N. Goergen, "Security in cognitive radio networks: threats and mitigation," in *International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, May 2008.

[2] T. Newman and T. Clancy, "Security threats to cognitive radio signal classifiers," in *Virginia Tech Wireless Personal Communications Symposium*, June 2009.

[3] R. Shaukat, S. Khan, and A. Ahmed, "Threats identification and their solution in inter-basestation dynamic resource sharing IEEE-802.22," in *Proc. International Conference on Convergence and Hybrid Information Technology*, Aug. 2008, pp. 609–614.

[4] R. Chen, J. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 25–37, Jan. 2008.

[5] J. Burbank, "Security in cognitive radio networks: the required evolution in approaches to wireless network security," in *International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, May 2008.

[6] C.-S. Lu, *Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property*. IGI Publishing, 2004.

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

[8] M. Morimoto, M. Okanda, and S. Komaki, "A hierarchical image transmission system in fading channel," in *Proc. IEEE 4th International Conference on Universal Personal Communications*, pp. 769–772, Nov. 1995.

[9] L. Wei, "Coded modulation with unequal error protection," *IEEE Trans. Commun.*, vol. 41, pp. 1439–1449, Oct. 1993.

[10] V. Brik, S. Banerjee, and M. Gruteser, "Wireless device identification with radiometric signatures," *ACM MobiCom*, 2008.

[11] P. Yu, J. Baras, and B. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics and Security*, vol. 3, pp. 38–51, Mar. 2008.

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

[13] N. Goergen, T. C. Clancy, and T. R. Newman, "Physical layer authentication watermarks through synthetic channelemulation," in *New Frontiers in Dynamic Spectrum Access Networks*, Apr. 2010.

[14] N. Goergen, W. S. Lin, K. J. R. Liu, and T. C. Clancy, "Authenticating MIMO transmissions using channel-like fingerprinting," in *IEEE GLOBECOM*, Dec. 2010.

[15] C. Pirak, Z. J. Wang, K. J. R. Liu, and S. Jitapunkul, "A data-bearing approach for pilot-embedding frameworks in space-time coded MIMO systems," *IEEE Trans. Signal Process.*, pp. 3966–3979, Oct. 2006.

[16] I. E. Telatar and D. N. C. Tse, "Capacity and mutual information of wideband multipath fading channels," in *IEEE Trans. Inf. Theory*, vol. 46, July 2000.

[17] P. Bello, "Characterization of randomly time-variant linear channels," *IEEE Trans. Commun. Systems*, vol. CS-11, pp. 360–393, Dec. 1963.

[18] M. Herdin, N. Czink, H. Ozcelik, and E. Bonek, "Correlation matrix distance, a meaningful measure for evaluation of non-stationary MIMO channels," in *Proc. IEEE Vehicular Technology Conference*, vol. 1, pp. 136–140, June 2005.

[19] J. Wallace and M. Jensen, "Time-varying MIMO channels: measurement, analysis, and modeling," *IEEE Trans. Antennas and Propag.*, vol. 54, pp. 3265–3273, Nov. 2006.

[20] A. O. Kaya, L. J. Greenstein, and W. Trappe, "Characterizing indoor wireless channels via ray tracing combined with stochastic modeling," *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 4165–4175, Aug. 2009.

[21] S. Alamouti, "A simple transmitter diversity scheme for wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 16, pp. 1414–1458, Oct. 1998.

Nate S. Goergen (S'03) received the Ph.D. degree in the Electrical and Computer Engineering Department, University of Maryland, College Park in 2011, the M.S. degree in Electrical and Computer Engineering from the University of Maryland, College Park in 2010, and the B.S. in Electrical Engineering from Rose-Hulman Institute of Technology in 2004. He was awarded the DoD S.M.A.R.T Scholarship in 2007, the 2010 University of Maryland Invention of the Year Award, and the Jimmy Lin Award for Invention in 2011. His research interests include cognitive radio, signal processing, and physical layer security of wireless signals. His current research is in watermarking approaches for wireless communications.

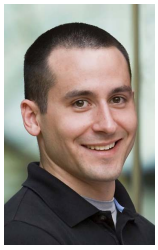
W. Sabrina Lin (M'06) received the Ph.D. degree with the Electrical and Computer Engineering Department, University of Maryland, College Park, where she is a Research Associate. She received the B.S. and M.S. degrees in Electrical Engineering from National Taiwan University in 2002 and 2004, respectively. Her research interests are in the area of information security and forensics, multimedia signal processing and multimedia social network analysis. She received the University of Maryland Future Faculty Fellowship in 2007.

K. J. Ray Liu (F'03) is named a Distinguished Scholar-Teacher of University of Maryland, College Park, in 2007, where he is Christine Kim Eminent Professor of Information Technology. He serves as Associate Chair of Graduate Studies and Research of Electrical and Computer Engineering Department and leads the Maryland Signals and Information Group conducting research encompassing broad aspects of wireless communications and networking, information forensics and security, multimedia signal processing, and biomedical engineering.

Dr. Liu is the recipient of numerous honors and awards including IEEE Signal Processing Society Technical Achievement Award and Distinguished Lecturer. He also received various teaching and research recognitions from University of Maryland including university-level Invention of the Year Award; and Poole and Kent Senior Faculty Teaching Award and Outstanding Faculty Research Award, both from A. James Clark School of Engineering. An ISI Highly Cited Author in Computer Science, Dr. Liu is a Fellow of IEEE and AAAS.

Dr. Liu is President-Elect and was Vice President Publications of IEEE Signal Processing Society. He was the Editor-in-Chief of IEEE Signal Processing Magazine and the founding Editor-in-Chief of EURASIP Journal on Advances in Signal Processing.

His recent books include *Cognitive Radio Networking and Security: A Game Theoretical View*, Cambridge University Press, 2010; *Behavior Dynamics in Media-Sharing Social Networks*, Cambridge University Press (to appear); *Handbook on Array Processing and Sensor Networks*, IEEE-Wiley, 2009; *Cooperative Communications and Networking*, Cambridge University Press, 2008; *Resource Allocation for Wireless Networks: Basics, Techniques, and Applications*, Cambridge University Press, 2008; *Ultra-Wideband Communication Systems: The Multiband OFDM Approach*, IEEE-Wiley, 2007; *Network-Aware Security for Group Communications*, Springer, 2007; *Multimedia Fingerprinting Forensics for Traitor Tracing*, Hindawi, 2005.



T. Charles Clancy (S'02-M'06-SM'10) is the Associate Director of the Ted and Karyn Hume Center for National Security and Technology at Virginia Tech, where he leads the university's educational and research efforts in national security. Prior to joining Virginia Tech, Dr. Clancy led a number of wireless research programs at the Laboratory for Telecommunications Science, at the University of Maryland, emphasizing development in commodity use of software-defined radio. Dr. Clancy's research interests are in the security of wireless communications, particularly spectrum access and waveform robustness.

Dr. Clancy received his PhD in Computer Science from the University of Maryland, College Park, MS in Electrical Engineering from the University of Illinois, Urbana-Champaign, and BS in Computer Engineering from the Rose-Hulman Institute of Technology, Terre Haute, IN. He is a Senior Member of the IEEE.