This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2010 proceedings.

Authenticating MIMO Transmissions Using Channel-Like Fingerprinting

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

Electrical and Computer Engineering
University of Maryland, College Park, MD, 20742, USA

***Abstract*— A framework for introducing an extrinsic fingerprint signal to space-time coded transmissions at the physical-layer is presented, whereby the fingerprint signal conveys a low capacity digital communication suitable for authenticating the transmission and further facilitating secure communications. A novel approach is discussed where the fingerprint signal mimics distortions similar to time-varying channel effects. Specifically, the fingerprint signal is only visible to aware receivers considering previous channel state information (CSI) and is otherwise invisible to a receiver equalizing according to current CSI. An augmented signal is created consisting of the original transmission, or primary message, and the fingerprint message. An example fingerprint signal and detection rule are presented based on a phase-shift keying approach. Simulation results including bit error rate (BER) are presented for both the primary and fingerprint signals using the 2x2 Alamouti code, and authentication signal BERs *lower* than the primary signal are demonstrated.**

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. In general, robust authentication devices are crucial to securing wireless systems and preventing a number of identity attacks to Cognitive Radio (CR) systems [1].

The practice of signal fingerprinting, where new a message conveying the credentials of a data source is appended to the signal, has been successfully applied to multimedia systems allowing for secure transmission of multimedia content. Since very little capacity is required to transmit the authentication message, and since the fingerprint processing mechanism can have completely independent synchronization requirements, robust physical layer fingerprints can be designed allowing for authentication even when the signal itself is unrecoverable due to low signal to noise ratio (SNR) or fading conditions.

In this paper, we consider the fingerprinting of space-time coded (STC) transmissions at the PHY-layer. A number of PHY-layer fingerprinting approaches for wireless digital communications have been investigated, using basic signal superposition methods. For example, in [2] the superposition of low-power pseudo random sequences on digital television transmissions is discussed.

The main disadvantage of blind superposition is that the fingerprint signal appears as additive noise in the primary signal and is fully present when the signal is decoded, decreasing the SNR of the original signal. Instead, we investigate a fingerprinting approach that exploits typical receiver preprocessing algorithms such as channel equalization, with a design approach closely resembling the Category 2 and Category 3 fingerprints described in [3]. These fingerprints are designed according to anticipated channel distortions, and through careful consideration of how the primary signal will be perceived by the recipient, resulting in improved fingerprint designs.

In [4] it was demonstrated that robust PHY-layer fingerprints may be obtained from intrinsic features characteristic of wireless channels, such as unique scattering environments and spatial variability. 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 signal that is applied by the transmitter. The extrinsic fingerprint signal is then used to convey a cryptographically secure digital signature and message digest along with the primary transmission.

In this work we consider the case where the extrinsic fingerprint signal is added at the PHY-layer as an independent digital signal that conveys a cryptographically secure message, thereby leveraging many of the advantages that digital communications and cryptographic primitives have to offer. In [5] the details of an authentication message are considered for the single transmitter broadcast case, where the authentication message conveys self-verifiable information about the transmission such as the frequency, location, and time the transmitter is authorized for transmission.

978-1-4244-5637-6/10/$26.00 ©2010 IEEE

A message digest, or *hash*, of this information is then digitally signed using a pre-shared cryptographic certificate owned by the transmitter that ubiquitously identifies the transmitter within a wireless system. A timestamp is also included to prevent future replay of the message while the use of strong cryptographic methods prevent forgery and replay of the independent digital authentication signal by malicious attackers.

The PHY-layer transmission of the digital fingerprint message for STC signals is the focus of this work.

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 quasi-static, where $\mathbf{H}[t]$ remains constant over the block, or M symbols.

We now briefly describe the pilot-embedding framework presented in [6], which provides the edifice for the construction of $\mathbf{U}[t]$. 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 may 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:

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

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 Liklihood (ML) receiver. These properties imply that $Rank(\mathbf{A}) = N$, $Rank(\mathbf{P}) = L_t$, and the number of time slots M required of the ST symbol $\mathbf{U}(t)$ is $M = Rank(\mathbf{A}) + Rank(\mathbf{P})$. Three basic structures are discussed in [6] for the design of $\mathbf{A}$ and $\mathbf{P}$, including the Time-Multiplexed (TM) structure which generalizes many pilot embedding techniques currently used in implementation. The TM structure is simply

$$\mathbf{A} = \left[\mathbf{0}_{(N \times L_t)}; \mathbf{I}_{(N \times N)}\right], \quad \mathbf{P} = \left[\mathbf{I}_{(L_t \times L_t)}; \mathbf{0}_{(L_t \times N)}\right]. \tag{4}$$

The expanded form of the signal at the receiver (1), with (2) becomes

$$\begin{aligned} \mathbf{Y}[t] =& \mathbf{H}[t]\mathbf{F}[t](\mathbf{D}[t]\mathbf{A} + \mathbf{P}) + \mathbf{N}[t] \\ =& \mathbf{H}[t]\mathbf{X}[t]\mathbf{A} + \mathbf{H}[t]\mathbf{F}[t]\mathbf{P} + \mathbf{N}[t]. \end{aligned} \tag{5}$$

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 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. An MMSE equalizer operating on current channel state information (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-varying 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 $\mathbf{F}[t]$ and will decrease fingerprint detection performance.

Since channel coherence over many blocks is a strong assumption for general time-variant channels, especially

978-1-4244-5637-6/10/$26.00 ©2010 IEEE

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 while higher frequency channel fluctuations will result in degraded performance. Changing our time index to reflect this design, when $t = 2Mk$ and the fingerprint is omitted, $\mathbf{F}[t]$ is replaced by the identity matrix $\mathbf{I}$ for the channel sounding block. When $t = 2Mk - 1$, $\mathbf{F}[t]$ is transmitted. Thus the received signal with the fingerprinting function applied to every other block transmission becomes

$$\mathbf{Y}[t] = \begin{cases} \mathbf{H}[t]\mathbf{U}[t] + \mathbf{N}[t], & t = 2Mk - 1, \\ \mathbf{H}[t]\mathbf{F}[t]\mathbf{U}[t] + \mathbf{N}[t], & t = 2Mk. \end{cases} \quad (6)$$

The authentication fingerprint message is transmitted using the fingerprinting function $\mathbf{F}[t]$, thus proper detection of the fingerprint is based on an assumption of mutual information between the receiver's current and outdated channel estimates for the intervals $\mathbf{H}[2Mk]$ and $\mathbf{H}[2Mk-1]$. When the coherence time of the channel is large the mutual information between $\mathbf{H}[2Mk]$ and $\mathbf{H}[2Mk-1]$ is significant, and the fingerprint function may 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 [7].

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

$$||\mathbf{X}[t]||_F = ||\mathbf{D}[t]||_F = P_o, \quad (7)$$

where $||\cdot||_F$ represents the Frobenius norm. Therefore, according to (6) 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 $\mathbf{Y}[2Mk]$, and when it is omitted, i.e. during $\mathbf{Y}[2Mk-1]$.

Extending the time-varying channel model used in [4] 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 $\bar{H}_{i,j} = E[H_{i,j}[t]]$, a zero-mean time-variant channel gain process $\mu_{i,j}[t]$, and a zero-mean receiver noise component $N_{i,j}[t]$. In this model $\bar{H}_{i,j}$ is the mean of the random variable $H_{i,j}[t]$. Thus, $H_{i,j}[t]$ becomes

$$H_{i,j}[t] = \bar{H}_{i,j} + \mu_{i,j}[t] + N_{i,j}[t]. \quad (8)$$

While in general the channel gain means, $\bar{\mathbf{H}}$, 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 (6).

We model the time-variant portion of the channel response gain for each element of $\boldsymbol{\mu}[t]$ as an independent first-order autoregressive (AR-1) model [4] with average power σ_T^2 over all gain elements $\mu_{i,j}[t]$, or

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

While [4] deals primarily with correlations in the frequency domain between consecutive channel estimates, we consider correlation in the time domain. 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 $\mu_{i,j}[t]$. We consider the case where the AR model coefficient a, and the average noise power σ_T^2 are the same for each independent channel i, j. 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 $E[\mu_{i,j}[t]] = 0, \forall i, j$.

A. Threat Model

With any security scheme a threat model considering the capabilities of adversaries must be developed. If we assume that adversaries are capable of generating a signal via the same methods that $\mathbf{Y}[k]$ is generated, fabrication of a transmission would require forgery of $\mathbf{F}[k]$. Because $\mathbf{F}[k]$ is protected from forgery and replay using cryptographic certificates, a timestamp, and a message signature, protection from these attacks follows from the particular cryptographic primitive chosen. The coding scheme chosen for the message, which may include forward error correction, can be chosen to achieve an arbitrarily high probability of detection for typical SNRs, while the cryptographic key length and certificate are selected to achieve an arbitrarily low probability of false detection in addition to protection against malicious attacks. Due to the numerous parameters, we will use the raw bit error rate (BER) of the received authentication signal as a system performance metric.

The authentication message discussed in [5] also includes the center frequency authorized for the transmission. Therefore even if we assume that an adversary can fully duplicate $\mathbf{F}[k]$, the attacker will be constrained to the frequency or frequencies prescribed by the compromised certificate.

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 (1) for performing channel equalization and further recovering $\mathbf{D}[t]$. By post-multiplying both sides of (6) by $\mathbf{P}^H$ and using the properties in (3), the channel response $\mathbf{H}[t]$ may be estimated

from the received signal during the channel-sounding symbol at $t = \tau_0 = 2Mk - 1$

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

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 $\mathbf{F}[t]$, may be estimated from the received signal (6) during the fingerprinted symbol at $\tau_1 = 2Mk$

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

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

$$\hat{\mathbf{H}}[t] = \begin{cases}\mathbf{H}[t] + \mathbf{N}[t]\mathbf{P}^H, & t = \tau_0 = 2Mk - 1, \\ \mathbf{H}[t]\mathbf{F}[t] + \mathbf{N}[t]\mathbf{P}^H, & t = \tau_1 = 2Mk,\end{cases} \tag{12}$$

where $\mathbf{N}[t]\mathbf{P}^H$ is the normalized projected channel estimate noise. If $\mathbf{N}[t]$ is uniformly distributed Gaussian noise and $\mathbf{P}$ is of proper design, the pilots will be placed such that channel conditions are uniformly estimated resulting in a uniform noise distribution for $\mathbf{N}[t]\mathbf{P}^H$.

A. Data Recovery

After the channel has been estimated via (10) and (11), the next step is the recovery of the transmitted data $\mathbf{D}[t]$. By post-multiplying both sides of (6) by $\mathbf{A}^H$ and using the properties (3), the data signal $\mathbf{D}[t]$ may be extracted from the received signal (6) during the channel-sounding symbol transmitted at $\tau_0 = 2Mk - 1$, i.e.

$$\begin{aligned}\mathbf{Y}[\tau_0]\mathbf{A}^H &= (\mathbf{H}[\tau_0](\mathbf{D}[\tau_0]\mathbf{A} + \mathbf{P}) + \mathbf{N}[\tau_0])\,\mathbf{A}^H \\ &= \mathbf{H}[\tau_0]\mathbf{D}[\tau_0] + \mathbf{N}[\tau_0]\mathbf{A}^H.\end{aligned} \tag{13}$$

We consider here the case where the number of transmit antenna and the number of receive antenna are equal, or $L_r = L_t$. An estimate for the intrinsic channel response $\hat{\mathbf{H}}[\tau_0]$ is produced via (10), and thus the data signal may 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 $t = \tau_0 = 2Mk - 1$ is

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

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

$$\begin{aligned}\mathbf{Y}[\tau_1]\mathbf{A}^H &= (\mathbf{H}[\tau_1]\mathbf{F}[\tau_1](\mathbf{D}[\tau_1]\mathbf{A} + \mathbf{P}) + \mathbf{N}[\tau_1])\,\mathbf{A}^H \\ &= \mathbf{H}[\tau_1]\mathbf{F}[\tau_1]\mathbf{D}[\tau_1] + \mathbf{N}[\tau_1]\mathbf{A}^H,\end{aligned} \tag{16}$$

an estimate for the intrinsic channel response combined with the extrinsic response, $\hat{\mathbf{H}}[\tau_1]\mathbf{F}[\tau_1]$, is produced via (11) and the data signal may 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 data signal at $t = \tau_1 = 2Mk$ becomes

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

We note that from (11) and (17) it has been shown that the data signal $\mathbf{D}[\tau_1]$ may 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 the MMSE 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 shown that the fingerprinted signal may be received by unaware receivers without modification to the channel estimation procedure or equalization device.

B. Fingerprint Detection

We now consider detection of the fingerprint signal given the sequence of channel state information in (12). The Hadamard product, or element-wise product between two matrices, will be considered 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

$$\begin{aligned}E\left[\mathbf{Z}_{HAD}[\tau_1, \tau_0]\right] =& E\left[\left(\mathbf{Y}[\tau_1]\mathbf{P}^H\right) \circ \left(\mathbf{Y}[\tau_0]\mathbf{P}^H\right)^*\right] \\ =& ||\bar{\mathbf{H}}||^2\mathbf{F}[\tau_1],\end{aligned} \tag{18}$$

where $(\circ)$ represents the Hadamard product and $(*)$ represents conjugation. Here the perturbation factor may be extracted from the argument of the product of the individual scalar estimates. We will use this detector in the fingerprint example to follow, and demonstrate its performance.

IV. An Example Digital Fingerprint

We now consider an example fingerprinting function for $\mathbf{F}[t]$, following the energy constraint of (7). In this simple example will we will consider the 2x2 Alamouti code [8] and use the polar representation of the complex valued

intrinsic channel model (8), i.e.

$$\begin{aligned}\mathbf{H}[t] = &\begin{bmatrix}\bar{H}_{0,0}+\mu_{0,0}[t] & \bar{H}_{0,1}+\mu_{0,1}[t]\\ \bar{H}_{1,0}+\mu_{1,0}[t] & \bar{H}_{1,1}+\mu_{1,1}[t]\end{bmatrix}+\begin{bmatrix}N_{0,0}[t] & N_{0,1}[t]\\ N_{1,0}[t] & N_{1,1}[t]\end{bmatrix}\\ =&\begin{bmatrix}\alpha_1 e^{j\theta_1} & \alpha_3 e^{j\theta_3}\\ \alpha_2 e^{j\theta_2} & \alpha_4 e^{j\theta_4}\end{bmatrix}+\begin{bmatrix}\mu_1[t] & \mu_3[t]\\ \mu_2[t] & \mu_4[t]\end{bmatrix}+\begin{bmatrix}N_1[t] & N_3[t]\\ N_2[t] & N_4[t]\end{bmatrix},\end{aligned} \tag{19}$$

where the indices $\{i,j\}$ are serialized to $1,2,\ldots,L_tM$ first row-wise and then collumn-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, $N=L_t=2$.

This simple example fingerprinting function introduces a phase offset between the signals to be transmitted by each antenna, denoted with the subscript APM. The fingerprinting function using the 2x2 code may be written

$$\mathbf{F}_{APM}[t]=\begin{bmatrix}e^{-j\epsilon} & 0\\ 0 & e^{j\epsilon}\end{bmatrix},\ 0\le\epsilon<2\pi. \tag{20}$$

Since the APM fingerprinting function introduces a phase perturbation, we apply the Hadamard product detector (18). The APM fingerprinting function in (20) and equation (19) for the 2x2 code becomes

$$\begin{aligned}\mathbf{Z}_{APM}[\tau_1,\tau_0] &= E\left[\mathbf{Z}_{HAD}[\tau_1,\tau_0]\right]\\ &= E\left[\begin{bmatrix}\alpha_1 e^{j(\theta_1-\epsilon)} & \alpha_3 e^{j(\theta_3+\epsilon)}\\ \alpha_2 e^{j(\theta_2-\epsilon)} & \alpha_4 e^{j(\theta_4+\epsilon)}\end{bmatrix}\circ\begin{bmatrix}\alpha_1 e^{-j\theta_1} & \alpha_3 e^{-j\theta_3}\\ \alpha_2 e^{-j\theta_2} & \alpha_4 e^{-j\theta_4}\end{bmatrix}\right]\\ &= \begin{bmatrix}\alpha_1^2 e^{-j\epsilon} & \alpha_3^2 e^{j\epsilon}\\ \alpha_2^2 e^{-j\epsilon} & \alpha_4^2 e^{j\epsilon}\end{bmatrix}.\end{aligned} \tag{21}$$

Combining all scalar estimates from (21) 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,

$$\begin{aligned}e^{-j\hat{\epsilon}} &= \sum_{j=0}^{N} Z_{APM_{1,j}}[\tau_1,\tau_0]+\sum_{j=0}^{N} Z^*_{APM_{0,j}}[\tau_1,\tau_0]\\ &= \lambda^{(2)}e^{-j\epsilon},\end{aligned} \tag{22}$$

where the disturbance factor ϵ may be recovered by taking the argument of (22), and $\lambda^{(2)}=\sum_{x=1}^{L_tN}\alpha_x^2$ is the anticipated signal gain for the 2x2 MRC Alamouti decoder with the perfect channel estimation assumption.

From (22) 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 may be decreased by increasing ϵ at the transmitter.

The variance of the detection rule (22) may be written,

$$\begin{aligned}Var\left[\mathbf{Z}_{HAD}[\tau_1,\tau_0]\right] =&2\left(\sigma_N^2+\sigma_T^2+a\sigma_T^2+a\sigma_T^4\right)\bar{\mathbf{H}}^{(2)}\\ &+\left(\sigma_N^2+\sigma_T^2\right)^2\mathbf{1},\end{aligned} \tag{23}$$

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 (22) for the case where all elements of $\bar{\mathbf{H}}^{(2)}$ are equal, becomes

$$\sigma_\epsilon^2\mathbf{1}=\frac{Var\left[\mathbf{Z}_{HAD}[\tau_1,\tau_0]\right]}{NL_t}. \tag{24}$$

If we select an antipodal signal constellation for (20) with phase parameter $\epsilon=\pi/2$, i.e.

$$\mathbf{F}[t]\in\left\{\begin{bmatrix}e^{-j\pi/2} & 0\\ 0 & e^{j\pi/2}\end{bmatrix},\begin{bmatrix}e^{j\pi/2} & 0\\ 0 & e^{-j\pi/2}\end{bmatrix}\right\}, \tag{25}$$

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

$$P\left[\hat{\mathbf{F}}\neq\mathbf{F}\right]=Q\left(\lambda^{(2)}\sqrt{\frac{2}{\sigma_\epsilon}}\sin\left(\frac{\pi}{2}\right)\right), \tag{26}$$

where $Q(\cdot)$ is the Gaussian tail function. From (24) and (26) we observe that the authentication fingerprint signal symbol error rate (SER) decreases when N or L_t are increased, potentially allowing for a fingerprint bit error rate (BER) lower than the primary signal BER in some channel stationarity conditions.

V. Simulation Results

We present MATLAB simulation results for the APM fingerprinting constellation (25), for different values σ_T and channel AR model parameters a in (9), using the MMSE channel estimator, the 2x2 Alamouti ST code with $M=4$, TM pilot embedding (4), and $N=L_t=L_r=2$. A QPSK constellation was used for the primary signal. 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 1. A plot of the BER for both the primary-signal and authentication signal is given in Figure 2, this time for a fixed $a=0.7$ and values of σ_T equal to 0.1 and 0.3.

From Figure 1 we observe that the authentication fingerprint BER advantage over primary signal increases with a, suggesting that the APM fingerprint signal performance depends on correlation between channel estimates in time, as determined by the AR-1 model parameter a. As the value of σ_T^2 increases in Figure 2, the power of the time-varying channel component increases resulting in a greater channel estimate MSE for both the primary and authentication signal and decreased system BER for both signals. We note from Figure 1 and Figure 2 that the fingerprint signal BER is lower than the primary for the range of SNRs simulated.

978-1-4244-5637-6/10/$26.00 ©2010 IEEE

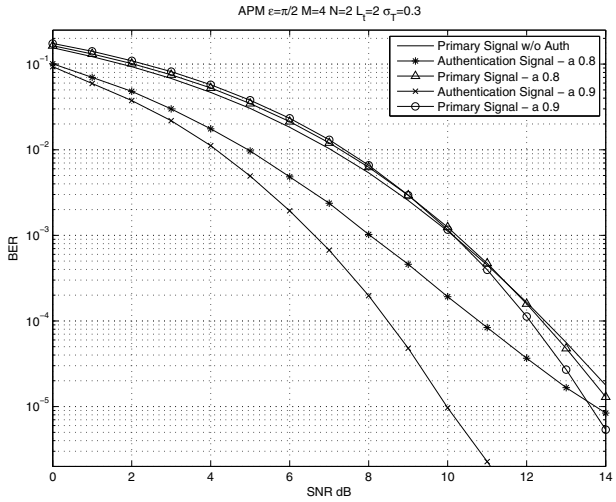

Fig. 1. BER for primary and fingerprint signal for various a

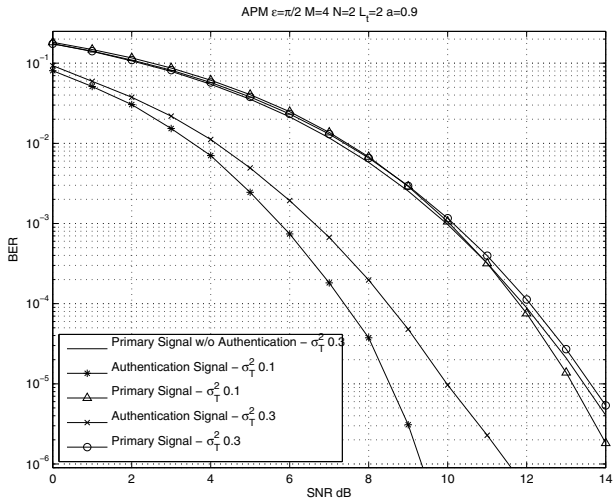

Fig. 2. BER for primary and fingerprint signal for various σ_T

Figure 3 presents channel estimate MSE and the worst-case MSE results for the simulation depicted in Figure 1. The worst-case MSE results in Figure 3 demonstrate the additional model error incurred if $\mathbf{Y}[\tau_1]$ were incorrectly equalized using $\mathbf{H}[\tau_0]$ as opposed to $\mathbf{H}[\tau_1]$. MSE results for Figure 2 are omitted due to space considerations.

From Figure 3 we note that MSE is relatively invariant of the AR-1 model parameter a, as the MSE for $a = 0.7$ and $a = 0.9$ are overlapping and indistinguishable.

VI. Conclusion

We have demonstrated that the presented framework facilitates transmission of a digital fingerprint message without requiring the modification of unaware receivers. Further, the distortions introduced by the fingerprint are

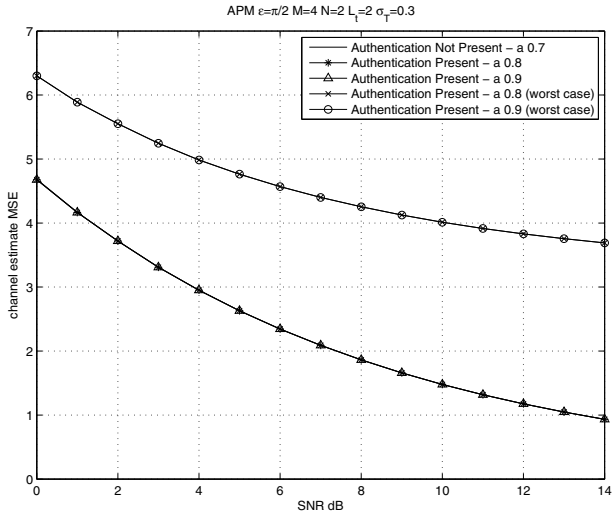

Fig. 3. MSE of the channel estimate with and without APM fingerprint signal for various a

partially removed by the receiver's equalizer, as demonstrated by the simulation results for the primary signal with and without the fingerprint present. Through simulation, it was demonstrated that the fingerprint signal may be received 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. Analysis of more STC code designs remains future work.

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 (Crowncom'08)*, May 2008.

[2] X. Wang, Y. Wu, and B. Caron, "Transmitter identification using embedded pseudo random sequences," *IEEE Transactions on Broadcasting*, vol. 50, pp. 244–252, September 2004.

[3] I. Cox, M. Miller, and A. McKellips, "Watermarking as communications with side information," *Proceedings of the IEEE*, vol. 87, pp. 1127–1141, July 1999.

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

[5] N. Goergen, T. C. Clancy, and T. R. Newman, "Physical layer authentication watermarks through synthetic channelemulation," in *New Frontiers in Dynamic Spectrum Access Networks (DySPAN'10)*, April 2010.

[6] 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," in *IEEE Transactions on Signal Processing*, October 2006, pp. 3966–3979.

[7] P. Bello, "Characterization of randomly time-variant linear channels," *IEEE Transactions on Communication Systems*, vol. CS-11, pp. 360–393, December 1963.

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