Physical-Layer Authentication

Paul L. Yu, John S. Baras, *Fellow, IEEE*, and Brian M. Sadler, *Fellow, IEEE*

***Abstract*—Authentication is the process where claims of identity are verified. Most mechanisms of authentication (e.g., digital signatures and certificates) exist above the physical layer, though some (e.g., spread-spectrum communications) exist at the physical layer often with an additional cost in bandwidth. This paper introduces a general analysis and design framework for authentication at the physical layer where the authentication information is transmitted concurrently with the data. By superimposing a carefully designed secret modulation on the waveforms, authentication is added to the signal without requiring additional bandwidth, as do spread-spectrum methods. The authentication is designed to be stealthy to the uninformed user, robust to interference, and secure for identity verification. The tradeoffs between these three goals are identified and analyzed in block fading channels. The use of the authentication for channel estimation is also considered, and an improved bit-error rate is demonstrated for time-varying channels. Finally, simulation results are given that demonstrate the potential application of this authentication technique.**

***Index Terms*—Authentication, modulation, superimposed signaling, watermarking.**

I. Introduction

THE concept of security encapsulates a set of ideas that includes authentication, integrity, and secrecy. This paper focuses on the authentication aspect of security; namely, can a node be identified solely by its transmission characteristics? We show that the answer is yes, subject to specifically identified tradeoffs in the stealth, robustness, and security of the system. For an authentication system, the uniqueness and nonreproducibility of the identification signal are of the utmost importance.

In conventional digital communications systems, a sender uses a message signal to transmit message symbols to a receiver. The sender and receiver agree upon a transmission scheme such that the mapping between signals and symbols is unique and known by both parties. The framework presented here extends the conventional communications system to transmit an additional authentication signal concurrently with messages. The authentication signal is subject to the same constraints as the message signal and, hence, unlike a spread-spectrum signal, can avoid using extra bandwidth. The authentication provides a security mechanism supplemental to those present at higher layers. With programmable radios, these modifications can be made at low cost.

This paper diverges from much of the previous work. Research in authentication systems and mechanisms have mostly focused above the physical layer. There are two paradigms of adding authentication: multiplexing or embedding. Some examples of multiplexed authentication are message authentication codes or authentication protocols that require a series of messages devoted to authentication. An overview of these methods may be found in [1] and in [2, Ch. 9 and 10]. The advantage of these methods is that the authentication is received with the same quality as the data. However, data throughput is penalized since some of the bits carry authentication instead of data.

In 1972, Cover [3] analyzed broadcast channels and demonstrated that high joint rates of transmissions are best achieved with simultaneous, as opposed to time-multiplexed, transmissions. Digital watermarking follows the paradigm of embedded signalling by modifying the data in a controlled manner that provides additional information to the receiver. Authentication may be transmitted in this manner [4], [5] and the addition is stealthy. Unlike the multiplexing approach, embedding additional information degrades the data quality [6]. Much of the research in digital watermarking has focused on watermarking multimedia data and minimizing the distortion at the receiver in terms of human perception.

At the physical layer, there has been work in authenticating the sender and receiver based on prior coordination or secret sharing, where the sender is authenticated if the receiver can successfully demodulate and decode the transmission. In this light, spread-spectrum techniques, such as direct sequence and frequency hopping, may be viewed as examples of physical-layer authentication systems [7]. While these techniques are covert and provide robustness to interference, they achieve this at the cost of bandwidth expansion and allow only authenticated parties with knowledge of the secret to participate in communications.

Suppose that we want to add authentication to a system in a stealthy way so that users unaware of the authentication can continue to communicate without any modifications to the hardware or protocol. The need for such stealth arises, for example, when authentication is piggybacked onto an existing system. Our approach to authentication exists at the physical layer, and may be used together with spread-spectrum methods or other security schemes at the higher layers to provide a more secure system.

The idea of transparently adding information at the physical layer has been discussed for some specific cases. Supangkat *et al.* [8] proposed one such authentication scheme for telephony where an encrypted hash of the conversation is added back into the signal. Similarly, Kleider *et al.* [9] proposed a scheme where a low-power watermark signal is added to the data signal with spread-spectrum techniques. Wang *et al.* [10] proposed a scheme for broadcast television where each transmitter adds a unique low-power signal to its transmissions in

Manuscript received July 27, 2006; revised October 16, 2007. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Nasir Memon.

P. L. Yu and J. S. Baras are with the Institute for Systems Research, University of Maryland, College Park, MD 20742 USA (e-mail: paulyu@isr.umd.edu; baras@isr.umd.edu).

B. M. Sadler is with the Army Research Lab, Adelphi, MD 20783 USA (e-mail: bsadler@arl.army.mil).

Digital Object Identifier 10.1109/TIFS.2007.916273

order to prove its identity to the receivers. The transparent transmission of data may also be realized by using multiresolution transmissions, where varying levels of protection are guaranteed for multiple data streams [11]–[13]. With this idea, the data symbols are sent with a high rate while the authentication is sent with a lower rate. Multiresolution (also known as asymmetric or nonuniform) constellations, where important data signal points are far apart and less important signal points are close together, can be used for this purpose.

Authentication at the physical layer may be viewed as a special use of pilot symbols, since the authentication signal is verified and, therefore, known at the receiver. However, a subtle difference arises since the authentication signal may or may not be present. Pilots are either superimposed (SI) or time division multiplexed (TDM) with the messages. Dong *et al.* [14] showed that SI schemes can outperform TDM schemes when the channel becomes sufficiently time varying. For a packet-based multicarrier system, Kleider *et al.* [15] showed that SI pilots can be utilized for channel acquisition while incurring only a 1-dB penalty when compared to a TDM training scheme. Thus, the idea of superimposing the data for transparency is motivated by previous work on channel estimation and authentication that provides specific examples of success. Our work unifies and generalizes many of the previous methods.

This paper introduces a broad analytical framework for describing physical-level authentication systems that do not require excess bandwidth. Using this setup, we analyze the stealth, robustness, and security of the scheme. The stealth of a scheme describes how covert the authentication is to a bystander. The bystander should not be able to detect that the signal is anomalous, nor should it detect any change in his or her own performance as a result of the scheme. The robustness of a scheme describes the resistance of the authentication to interference. Finally, the security of a scheme describes the inability of the adversary to mount successful attacks. Fundamental performance and tradeoffs are characterized between these desirable system characteristics. We also consider how the authentication may be used to improve channel estimation and demonstrate how bit-error rates may be lowered in time-varying channels.

II. Proposed Scheme

A. Scenario

In this paper, we consider the scenario depicted in Fig. 1 where four nodes share a wireless medium. Alice sends messages to Bob using reference signals while Carol and Eve listen. This network has no privacy, so Carol and Eve can understand what Alice is sending to Bob. Now suppose that Alice and Bob agree on a keyed authentication scheme that allows Bob to verify that the messages he receives are from Alice. In order to authenticate, Alice sends a proof of authentication, called a tag,[1] together with each message for Bob's verification. We call the transmitted signal under this scheme as the tagged signal. The tags reflect knowledge of the key shared between Alice and Bob.

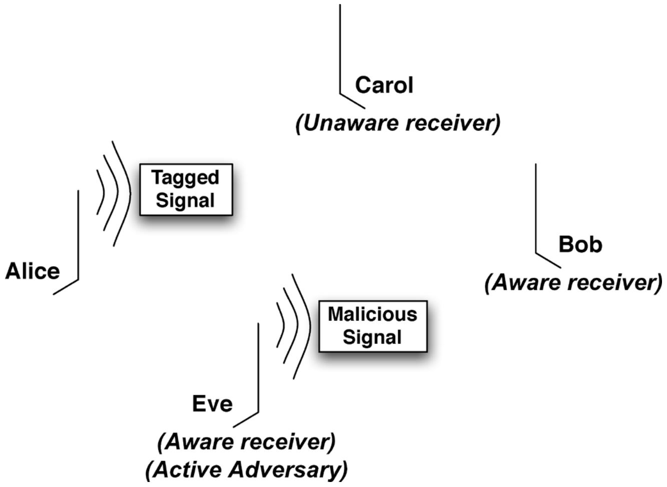


Fig. 1. Scenario with Alice, Bob, Carol, and Eve.

Carol does not know the scheme and cannot authenticate Alice's messages, but she still can recover the messages. Eve knows the scheme, but without the secret key, she also cannot authenticate Alice's messages. We say that Bob and Eve are aware receivers and Carol is an unaware receiver. A scheme has stealth if it: 1) does not significantly impact unaware receivers and 2) is not easily detectable. Note that we are not adding any privacy to the transmissions because we allow unaware receivers to continue message decoding.

Authentication is a security mechanism and we must therefore consider the possible attacks on it. Assume that Eve is an adversary that is aware of the scheme but does not know the secret key. Eve wishes to disrupt the authentication process by causing Bob to either reject authentic messages or accept inauthentic messages. We say that the authentication scheme is defeated when Eve can achieve her goals above a certain small probability ϵ. Eve plays an active role and can inject her own malicious signals into the medium. The tags are commonly dependent on the message so that unauthorized modifications to the message or tag can be detected. Authentication is useful only when it is difficult for Eve to defeat the scheme by creating valid tags for her messages (impersonating), modifying Alice's messages without Bob's knowledge (tampering), or corrupting the tag so that Bob cannot verify authenticity (removing). When it is difficult for Eve to defeat the scheme, the scheme is said to be secure.

Since the transmissions are present in random fading environments, it is highly desirable that the scheme be resistant to channel and noise effects. A scheme that is able to continue operation in the midst of interference is called robust.

B. Reference System

In this paper, we consider single-antenna transceivers transmitting narrowband signals in flat fading channels. We introduce the reference system as the baseline communications system upon which we build our proposed scheme. We refer the reader to Table I for a table of our notation.

1) Signal Model: The sender wants to transmit a message to the receiver so that it can be recovered and understood. When the message must pass through a random channel, the sender codes and modulates the message to protect against errors.

[1] We use the term "tag" to refer to the authentication signal that is superimposed at the physical layer.

TABLE I
TABLE OF SYMBOLS

Message Symbols	$\mathbf{b}$
Message Signal	$\mathbf{s}$
Tag Signal	$\mathbf{t}$
Reference Signal	$\mathbf{x} = \mathbf{s}$
Tagged Signal	$\mathbf{x} = \rho_s \mathbf{s} + \rho_t \mathbf{t}$
Channel	$\mathbf{h}$
Noise	$\mathbf{w}$
Received Signal	$\mathbf{y} = \mathbf{h} \cdot \mathbf{x} + \mathbf{w}$

Messages are blocks of M symbols denoted by $\mathbf{b} = \{b_1, \ldots, b_M\}$. We assume that the message symbols $\{b_k\}$ are independent, identically distributed (i.i.d.) random variables. The encoding function $f_e(\cdot)$ encapsulates any coding, modulation, or pulse shaping that may be used. The resulting message signal is $\mathbf{s} = f_e(\mathbf{b})$. The transmitted signal is denoted by $\mathbf{x} = \{x_1, \ldots, x_L\}$; in the case where the sender only transmits messages, we have $\mathbf{x} = \mathbf{s}$. We refer to this as the reference signal and will compare it with the tagged signal in the sequel. We assume that

$$E[x_k] = 0 \tag{1}$$

$$E|x_k|^2 = \sigma_x^2 = 1 \tag{2}$$

$$E|\mathbf{x}|^2 = E\left(|x_1|^2 + \ldots + |x_L|^2\right) = L. \tag{3}$$

Then, the message signal also satisfies $E[s_k] = 0$ and $E|\mathbf{s}|^2 = L$.

2) Channel Model: We assume a Rayleigh block fading channel so that different message blocks experience independent fades. The channel for the ith block is h_i, a complex zero-mean Gaussian variable with variance σ_h^2. The receiver observes the block

$$\mathbf{y}_i = h_i \cdot \mathbf{x}_i + \mathbf{w}_i \tag{4}$$

where $\mathbf{w} = \{w_1, \ldots w_L\}$ and $w_k \sim N(0, \sigma_w^2)$ is white Gaussian noise. The average signal-to-noise ratio (SNR) is $\overline{\gamma} = \sigma_h^2 / \sigma_w^2$, and the SNR experienced by each block γ is Rayleigh distributed with density

$$p(\gamma) = \frac{1}{\overline{\gamma}} e^{-\gamma/\overline{\gamma}}. \tag{5}$$

When the SNR γ_i falls below a certain threshold, say γ^0, the ith message block becomes unacceptably corrupted. The outage probability is the fraction of time that this occurs. The outage probability P_{out} is fixed by setting $\overline{\gamma}$

$$P_{\text{out}} = \int_0^{\gamma^0} p(\gamma) d\gamma = 1 - e^{-\gamma^0/\overline{\gamma}} \tag{6}$$

$$\overline{\gamma} = \frac{-\gamma^0}{\ln(1 - P_{\text{out}})}. \tag{7}$$

3) Channel Estimation: A block diagram of the unaware receiver is found in Fig. 2.

We assume that the channel is constant for the duration of the block. While this may not be strictly true, it is a reasonable assumption for slow fading channels. Pilot symbols are typically used to aid in channel estimation, and we insert them in the middle of the block as in Global System for Mobile Communications (GSM). (We use this as a representative pilot scheme, however, we emphasize that our framework is easily generalized to other cases). For the pilot symbols $\mathbf{p}$ and their observations $\mathbf{y_P}$, the MMSE channel estimate is simply

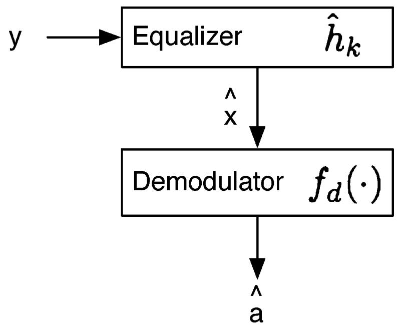


Fig. 2. Block diagram of the unaware receiver.

$$\hat{h} = \frac{1}{|\mathbf{p}|^2} \mathbf{p}^H \mathbf{y_P} \tag{8}$$

where $(\cdot)^H$ is the Hermitian transpose. We assume that $\sigma_p^2 = E|p_k|^2 = \sigma_x^2 = 1$.

4) Message Recovery: The unaware receiver uses its channel estimate to estimate the ith message signal

$$\hat{\mathbf{x}}_i = \frac{\hat{h}_i^*}{|\hat{h}_i|^2} \mathbf{y}_i. \tag{9}$$

It then uses $f_d(\cdot)$ to recover the message symbols

$$\hat{\mathbf{b}}_i = f_d(\hat{\mathbf{x}}_i). \tag{10}$$

C. Proposed System With Authentication

The proposed authentication system builds upon the reference system introduced in Section II-B.

1) Signal Model: The sender wants to transmit the authentication tag $\mathbf{t}$ together with the message $\mathbf{s}$ so the receiver can verify his or her identity. In general, the tag is a function of the message $\mathbf{s}_i$ and the secret key $\mathbf{k}$

$$\mathbf{t}_i = g(\mathbf{s}_i, \mathbf{k}). \tag{11}$$

The tag is padded (if necessary) to the message length and simultaneously transmitted. The tagged signal is (see Fig. 3)

$$\mathbf{x}_i = \rho_s \mathbf{s}_i + \rho_t \mathbf{t}_i \tag{12}$$

where $0 < \rho_s, \rho_t < 1$.

As with the message signal, we assume the tags satisfy $E[t_k] = 0$ and $E|\mathbf{t}|^2 = L$. We also assume that $E[\mathbf{s^H t}] = 0$ so that we can interpret ρ_s^2 and ρ_t^2 as energy allocations of the message and tag, respectively. Note that we are not forcing each tag to be orthogonal to its corresponding message, but

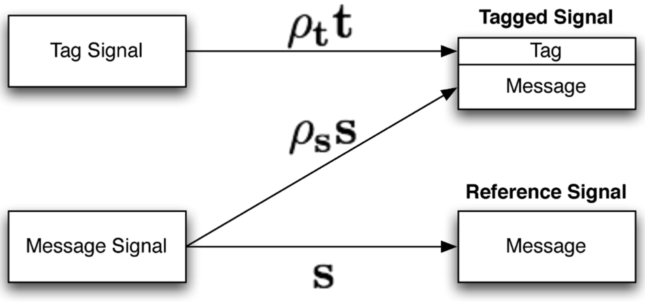


Fig. 3. Construction of reference and tagged signals.

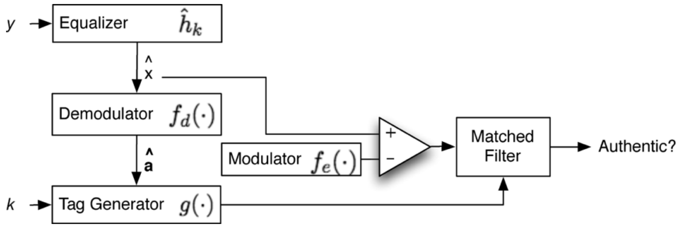


Fig. 4. Block diagram of the aware receiver.

rather that the pair be statistically uncorrelated.[2] An appropriate $g(\cdot)$ would make the message and tag appear uncorrelated (but not independent). We have the constraint $\rho_s^2 + \rho_t^2 = 1$ because (3) must be satisfied for both tagged and reference signals. In the case where $\rho_s^2 = 1$, the transmitted signal does not contain any authentication tag and $\mathbf{x}_i = \mathbf{s}_i$.

We introduce the terminology message-to-interference ratio (MIR) and tag-to-noise ratio (TNR) to facilitate future discussion

$$\begin{aligned}\mathrm{MIR}\left(\rho_s^2, \gamma_i\right) &= \frac{\rho_s^2 |h_i|^2}{\rho_t^2 |h_i|^2 + \sigma_w^2} \\ &= \frac{\rho_s^2 \gamma_i}{\rho_t^2 \gamma_i + 1} \qquad (13)\\ \text{and } \mathrm{TNR}\left(\rho_t^2, \gamma_i\right) &= \rho_t^2 |h_i|^2 / \sigma_w^2 = \rho_t^2 \gamma_i. \qquad (14)\end{aligned}$$

The reference system devotes all of the signal energy to the message [i.e., $\rho_s^2 = 1, \rho_t^2 = 0$, and, therefore, $\mathrm{MIR}(\rho_s^2, \gamma_i) = \gamma_i$ and $\mathrm{TNR}(\rho_t^2, \gamma_i) = 0$ ($-\infty$ dB]. The proposed system divides the signal energy between the message and tag so that with $0 < \rho_s^2$, $\rho_t^2 < 1$, $\mathrm{MIR}(\rho_s^2, \gamma_i) < \gamma_i$, and $\mathrm{TNR}(\rho_t^2, \gamma_i) > -\infty$ dB.

2) Channel Model and Estimation: We assume the same channel model as in Sections II-B2 and II-B3. Since the energy allocation is different for the proposed scheme, the pilot symbols are modified so that decision regions remain valid. Since $\mathrm{MIR} < \mathrm{SNR}$ for our proposed scheme, the pilot symbols should be scaled accordingly with ρ_s. For amplitude insensitive modulations, such as 4-QAM or BPSK, this is not necessary.

3) Message Recovery: A block diagram of the aware receiver is found in Fig. 4.

The aware receiver is an enhanced version of the unaware receiver. Message recovery may proceed as in Section II-B4. However, if we make some additional assumptions, the aware receiver may do better. We see from Section II-B4 that the unaware receiver treats all observations the same way. This may be suboptimal when two classes of signals may be observed. Since the aware receiver knows that a tag may be present, it can remove the tag prior to message recovery and, hence, reduce the error, provided that 1) it knows the tag exactly and 2) the tag is present.

Recall from (11) that the tag is generated from the secret key and the message. When the message is recovered without error, Bob can generate the tag because he has the secret key. Even if the message is recovered with errors, in some cases, the tag can be correctly generated if the tag generating function $g(\cdot)$ has some robustness against the message error. In the extreme case, the tag is independent of the message and maximally robust in this sense. However, as we will discuss in Section III-C, this is inadequate for security. A reasonable compromise can be reached by having the tag depend on the message number i. Since the message numbers are known, the receiver is always able to generate valid tags using this scheme.

Section II-C4 details how the tag is detected. If the tag is detected and estimated, then the aware receiver may choose to remove it from the received signal [compared with (12)]

$$\hat{\mathbf{b}}_i^{+} = f_d\left(\frac{1}{\rho_s}[\hat{\mathbf{x}}_i - \rho_t \mathbf{t}_i]\right). \qquad (15)$$

4) Authentication: In addition to recovering the message, the aware receiver also decides on the authenticity of the signal. If the receiver decides that the observation demonstrates knowledge of the key, then it authenticates the sender. Otherwise, the signal is not authenticated.

After estimating the channel, the receiver proceeds to perform message estimation and obtains $\hat{\mathbf{s}}_i$. With the secret key, it can generate the estimated tag $\hat{\mathbf{t}}_i$ using (11) and look for it in the residual $\mathbf{r}_i$. The tag can be generated without error even when $\hat{\mathbf{s}}_i$ contains some error when $g(\cdot)$ is robust against input error. For example, robust hash functions [16], [17] are suitable for this purpose

$$\begin{aligned}\hat{\mathbf{t}}_i &= g(\hat{\mathbf{s}}_i, \mathbf{k}) \qquad (16)\\ \mathbf{r}_i &= \frac{1}{\rho_t}\left(\hat{\mathbf{x}}_i - \rho_s f_e(\hat{\mathbf{b}}_i)\right). \qquad (17)\end{aligned}$$

We perform a threshold test with hypotheses

$$\begin{aligned}H_0 &: \quad \hat{\mathbf{t}}_i \text{ is not present in } \mathbf{r}_i \qquad (18)\\ H_1 &: \quad \hat{\mathbf{t}}_i \text{ is present in } \mathbf{r}_i. \qquad (19)\end{aligned}$$

We obtain our test statistic τ_i by match filtering the residual with the estimated tag. When we assume perfect channel estimation ($\hat{h}_i = h_i$), message recovery ($\hat{\mathbf{s}}_i = \mathbf{s}_i$), and tag estimation ($\hat{\mathbf{t}}_i = \mathbf{t}_i$), the statistic when the tagged signal is received is

$$\begin{aligned}\tau_i | H_1 &= \mathbf{t}_i^H \mathbf{r}_i \\ &= |\mathbf{t}_i|^2 + \frac{\hat{h}_i^*}{\rho_t |\hat{h}_i|^2} \mathbf{t}_i^H \mathbf{w} \\ &= |\mathbf{t}_i|^2 + v_i \qquad (20)\end{aligned}$$

[2] The effect of orthogonality on bandwidth is discussed in Section III-A1.

where conditioned on $\mathbf{t}_i$, v_i is a zero-mean Gaussian variable with variance $\sigma_{v_i}^2 = L\sigma_w^2/\rho_t^2|h_i|^2 = L/\rho_t^2\gamma_i$. When the reference signal is received, the statistic is

$$\begin{aligned}\tau_i|H_0 &= \left(\frac{1-\rho_s}{\rho_t}\right)\mathbf{t}_i^H\mathbf{s}_i + \frac{\hat{h}_i^*}{\rho_t|\hat{h}_i|^2}\mathbf{t}_i^H\mathbf{w} \\ &= \left(\frac{1-\rho_s}{\rho_t}\right)\mathbf{t}_i^H\mathbf{s}_i + v_i \end{aligned} \tag{21}$$

and $E[\tau_i|H_0] = 0$ since we assume $E[\mathbf{s}_i^H\mathbf{t}_i] = 0$.

The decision of authenticity δ_i for the ith block is made according to

$$\delta_i = \begin{cases} 0, & \tau_i < \tau_i^0 \\ 1, & \tau_i \geq \tau_i^0 \end{cases}. \tag{22}$$

The threshold τ_i^0 of this test is determined for a false alarm probability α according to the distribution of $(\tau_i|H_0)$

$$\tau_i^0 = \arg\min_{\tau} \Phi\left(\tau/\hat{\sigma}_{v_i}\right) \geq 1-\alpha \tag{23}$$

where $\Phi(\cdot)$ is the standard Gaussian cumulative distribution function and we estimate the SNR $\hat{\gamma}_i = |\hat{h}_i|^2/\sigma_w^2$ and $\hat{\sigma}_{v_i}^2 = L/\rho_t^2\hat{\gamma}_i$. The probability of detection for the ith tag is

$$P_i = 1 - \Phi\left(\left(\tau_i^0 - L\right)/\sigma_{v_i}\right) \tag{24}$$

and the probability of detection of a randomly chosen tag with a random channel realization is

$$P = \int P_i p(\gamma)d\gamma = E[P_i] \tag{25}$$

where $p(\gamma)$ is the probability density of γ given in (5).

III. Properties

We examine how the scheme proposed in Section II-C can achieve the properties of stealth, robustness, and security. We elaborate on the definitions and provide performance estimates.

A. Stealth

There are two aspects of a stealthy scheme. First, it should be covert: the presence of the scheme should not be easily detectable or obvious. Second, it should be unobtrusive: it should not have a noticeable effect on the unaware receivers' ability to recover messages.

1) Covertness: Consider how the unaware receiver may decide if the observed signal is anomalous. By definition, an anomalous signal has characteristics that are deviant from the reference signal. For example, signals are often constrained to occupy a certain frequency band. If a signal leaks out of its allocated band, then the receiver can identify it as anomalous. Therefore, the tagged signal should respect the same bandwidth constraints as the reference signal. In the proposed setup, the tags are superimposed onto the messages (12), and we assume that the tags and messages are uncorrelated. Note that we do not enforce orthogonality for each (message, tag) pair. It is known that the bandwidth efficiency (bits per Hertz) of orthogonal signaling is low: for a given rate, the required bandwidth is relatively high compared to nonorthogonal signaling [7]. A slight bandwidth expansion that is dependent on ρ_s^2 may be observed. Since the tags are very low bit rate, the expansion will be small. Also, by reducing the message energy, some bandwidth becomes available for signaling the tag.

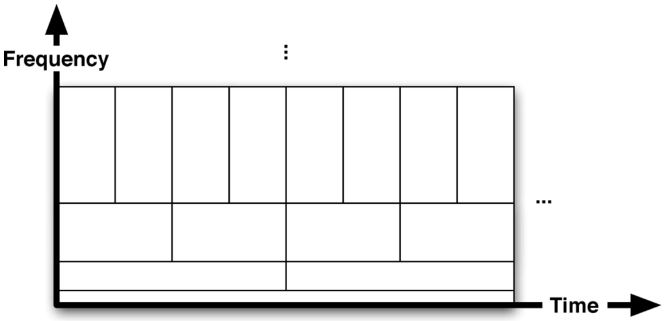


Fig. 5. Wavelet tiling of the time–frequency plane.

Rather than relying solely on the power allocation to constrain bandwidth, we can also use a basis decomposition (e.g., wavelets) to control the bandwidth of the tag. The wavelet transform gives a constant-Q tiling of the time–frequency plane, where every tile has bandwidth with constant proportion to the others. Fig. 5 illustrates the concept. A common implementation of the transform uses filter banks. We focus on this particular approach as a concrete exposition. Consider the sampled signal $\mathbf{x} = \{x_1, x_2, \ldots, x_L\}$. The wavelet transform passes the signal through two filters simultaneously—one highpass $h_1[\cdot]$ and one lowpass $h_0[\cdot]$, and then downsamples the outputs by 2. The downsampled output of the highpass filter is the level 1 detail coefficients, and the downsampled output of the lowpass filter is the level 1 approximation coefficients. The filter and downsampling is repeated with the approximation coefficients to yield additional levels of detail and approximation coefficients. The further analysis of the approximation coefficients is a characteristic of the wavelet transform and provides multiresolution signal representation.

We refer to the coefficient level as the scale, and note that large scales correspond to low frequencies. For a signal with small bandwidth, most of the energy will reside in the large-scale coefficients. For a signal with large bandwidth, however, energy will be spread across the smaller scales as well. Thus, for covertness, we place tag energy only in the appropriate scales depending on the signal. The tag signal may be synthesized from the coefficients by upsampling by 2 and filtering with impulse responses $g_1[n] = h_1[-n]$ and $g_0[n] = h_0[-n]$. The details of the analysis and synthesis filters are outside the scope of this paper, but a good tutorial may be found in [18]. With any finite support wavelet, some spectral leakage will occur. However, we place tag energy only in the coefficients where the message has energy also. Since we reduce the message energy and superimpose tag energy, the bandwidth should not be greatly perturbed with appropriate power allocation.

The receiver may also flag the signal as anomalous if the noise statistics are significantly different from what is expected.

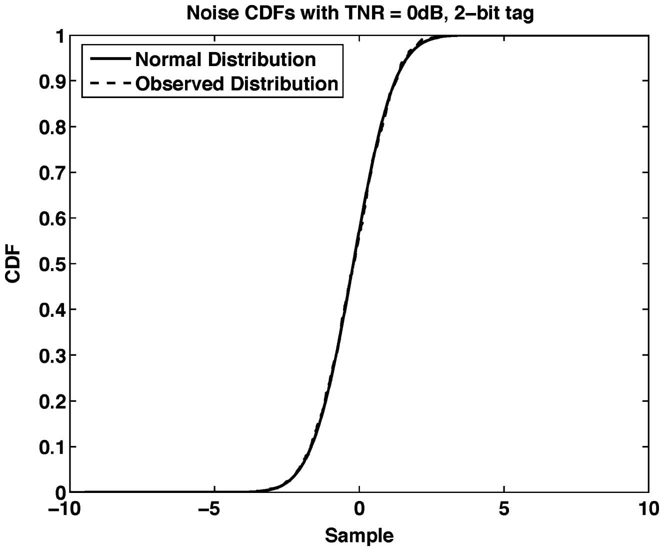


Fig. 6. Cumulative distribution functions for 2-b tag when $\mathrm{TNR} = 0$ dB. Lilliefors test does not detect the anomalous signal at a significance level 0.01.

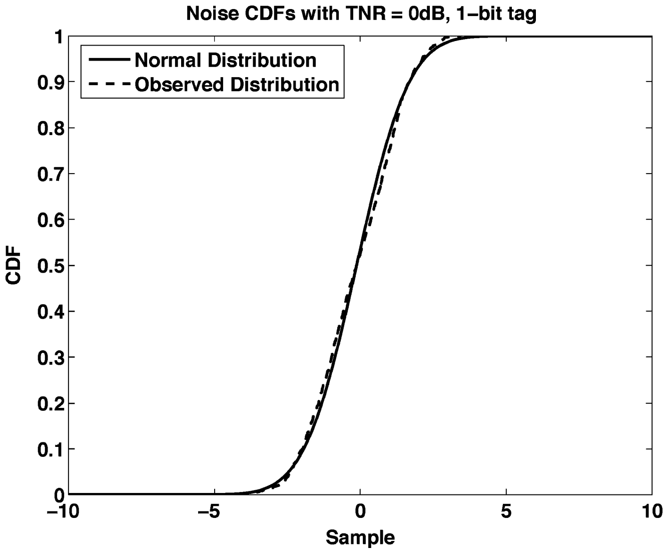


Fig. 7. Cumulative distribution functions for the binary tag when $\mathrm{TNR} = 0$ dB. Lilliefors test detects the anomalous signal at a significance level 0.01.

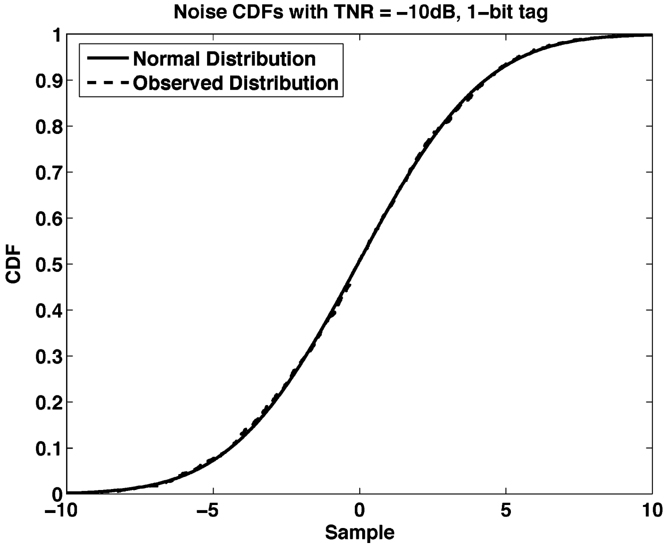


Fig. 8. Cumulative distribution functions for binary tag when $\mathrm{TNR} = -10$ dB. The Lilliefors test does not detect the anomalous signal at a significance level 0.01.

Goodness-of-fit tests, such as the Kolmogorov–Smirnov or Lilliefors tests, provide a well-known class of anomaly detection algorithms. All such tests give decisions with certain false alarm probabilities. Therefore, for a scheme to be covert, the estimated noise should be able to pass these goodness-of-fit tests without a significantly higher rate of alarm. Noise is generally assumed to be within a family of distributions with unknown parameters that must be estimated from the signal. It is within these unknown parameters that we covertly place the authentication tags. For example, if the tag is a Gaussian distributed signal, the residual is a sum of two Gaussians variables and, hence, distribution tests are insufficient to distinguish its presence.

Next, we consider the effect of tag energy on detectability. For a simple experiment, we ignore the effects of the channel, and suppose that the tag symbol t_k is 2o b and can take one of the values $\{-1.51, -0.453, .453, 1.51\}$ with respective probabilities $\{0.163, 0.327, 0.327, 0.163\}$. This is the MMSE four-level quantizer for a Gaussian random variable with zero mean and unit variance [7]. The tag is observed in AWGN $y_k = t_k + w_k$. Let the TNR be defined as σ_t^2/σ_w^2 where $\sigma_t^2 = E|t_k|^2$. The receiver tests to see if the observation is Gaussian or not by using the Lilliefors test. This goodness of fit test compares the empirical cumulative distribution function (CDF) with the normal CDF with mean and variance estimated from the observations. Fig. 6 shows the empirical versus normal CDFs when the 1000 2-b i.i.d. tag symbols are drawn and observed with $\mathrm{TNR} = 0$ dB. The Lilliefors test at significance level $\alpha = 0.01$ is unable to distinguish between the CDFs and indicates that the observation is not anomalous.

Now suppose that each tag symbol is represented by one of two equiprobable and polar values $\pm\sigma_t$. Fig. 7 shows the empirical versus normal CDFs when the tag has 1-b symbols and $\mathrm{TNR} = 0$ dB. This time, the Lilliefors test flags the observation as anomalous with significance level $\alpha = 0.01$. However, when we lower the TNR to -10 dB in Fig. 8, the observed CDF becomes indistinguishable from the normal distribution. These examples demonstrate that we can improve covertness by transmitting the tag at low power or by making the tag follow a noise-like distribution.

2) Impact on the Unaware Receiver: When the tag is indistinguishable from noise (Section III-A1), we may treat it as noise without much loss of precision. We now consider how the outage probability increases when the tag energy increases. Consider the SNR threshold γ^0 defined in Section II-B2. With tagged signals, an outage occurs whenever the MIR falls below γ^0 and, hence, the outage probability becomes

$$P_{\mathrm{out}}^m = 1 - e^{-\gamma^m/\bar{\gamma}} \leq P_{\mathrm{out}} \tag{26}$$

where γ^m satisfies $\gamma^0 = \mathrm{MIR}(\rho_s^2, \gamma^m)$.

Suppose that we fix $P_{\mathrm{out}} = 0.05$. Fig. 9 shows the probability density of the MIR for different ρ_s^2 when $\gamma^0 = 6$ dB. As power

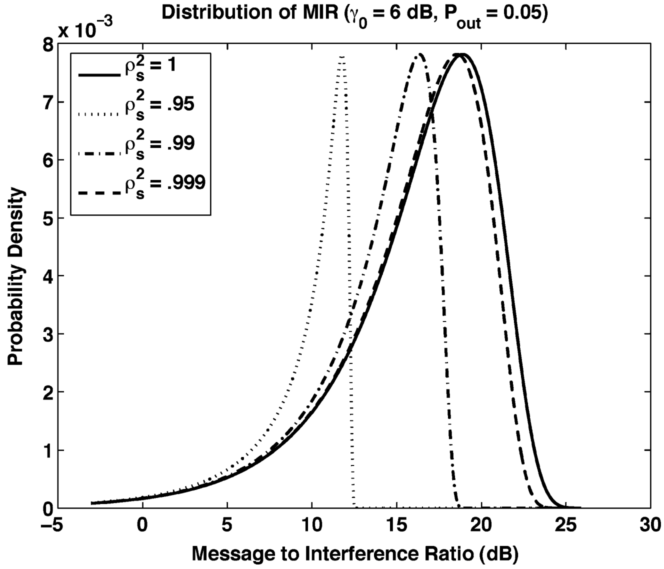


Fig. 9. Probability density of message to interference ratios for tagged signals in Rayleigh fading, $\overline{\gamma} = 18.9$ dB.

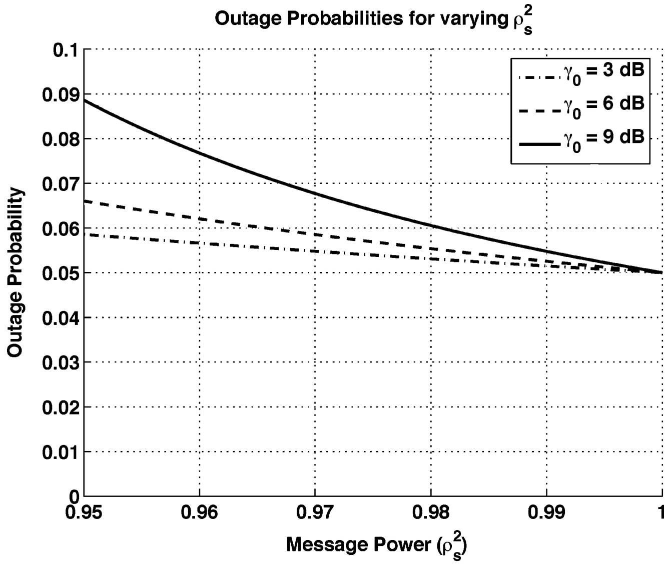


Fig. 10. Outage probabilities for various γ^0 with outage probability $P_{\text{out}} = 0.05$. Higher SNR requirements are more sensitive to the reduction in ρ_s^2.

is allocated away from the message, lower SNRs become more probable, leading to more frequent outages.

Fig. 10 shows the outage probabilities as a function of ρ_s^2 for $\gamma^0 = 3$, 6, and 9 dB. The outage probability is less sensitive to changes in ρ_s^2 for low γ^0. In any case, high message energy allocation keeps the outage probability close to P_{out}.

Thus, though the authentication is covert at any power when it is distributed as noise, at high power, it has a large impact on the unaware receiver. It is only for low tag power that the impact is small, regardless of how covert it is. Hence, the most important parameter for stealth is a small ρ_t^2, which leads to a covert signal with low TNR and high MIR. The potential difficulty of detecting a low power tag is overcome with coding, which is treated next.

B. Robustness

A robust scheme is resistant to channel and noise effects and can continue the authentication process in the midst of interference. With our channel assumptions (Section II-B2), each block suffers a random fade which affects the SNR γ_i. Our authentication process fixes the false alarm probability at α but the detection probability varies with the SNR. Additive noise and jamming signals also decrease the SNR. Thus, the fading channel, combined with noise and other interference, present difficulties to the authentication.

One possible method of improving robustness is to increase the power of the transmission signal to raise the average SNR $\overline{\gamma}$. This lowers the probability of unsuitably low SNRs, but is not always feasible. Alternatively, we may extend the authentication process to consider many blocks together instead of each block separately.Since we assume a Rayleigh block fading channel model, each block experiences independent fades, and conditioned on the authenticity of the signal, the authentication decisions are independent events as well.

Let $x = \sum_i \delta_i$ tally the number of detected tags in K blocks. When no tag is sent, the probability of detecting more than k_0 tags is

$$p(x > k_0 | H_0) = \sum_{i=k_0+1}^{K} B(i; K, \alpha) \tag{27}$$

where $B(x; n, p)$ is the binomial probability mass function of obtaining exactly x successes in n identical and independent trials with the probability of success p. For the extended test, we compare x with a threshold k_0 that is set so that the false alarm probability does not exceed the new false alarm probability α_K

$$k_0 = \arg\min_j \left[\sum_{i=j+1}^{K} B(i; K, \alpha) < \alpha_K \right]. \tag{28}$$

The Neyman–Pearson test gives the probability of deciding H_1 as

$$\delta_K = \begin{cases} 1, & x < k_0 \\ \pi, & x = k_0 \\ 0, & x > k_0 \end{cases} \tag{29}$$

where p is the randomization of the detection rule and is given by

$$\pi = \frac{\alpha_K - p(x > k_0 | H_0)}{p(x = k_0 | H_0)}. \tag{30}$$

For a randomly selected group of K tagged signal blocks, the probability of correctly deciding H_1 is simply

$$p(x > k_0 | H_1) = (1 - \pi) B(k_0; K, P) + \sum_{i=k_0+1}^{K} B(i; K, P) \tag{31}$$

where P is the probability of detection for a randomly observed block [see (25)].

There is a fundamental tradeoff between robustness and security. When a scheme is made more robust in this manner, we are allowing more errors to be made in the tag detection before rejecting an authentic signal. However, this gives the adversary more opportunity to inject malicious blocks that may be accepted as authentic. We will discuss the security issues in the next section.

C. Security

A secure scheme is resistant to adversarial attacks. First, we define the adversary model and then we examine the security of our proposed scheme.

1) Adversary Model: Eve the adversary is an aware receiver and knows the authentication scheme that Alice and Bob are using. However, she does not know the secret key. She is an active opponent and can transmit her own signals that are observable by Bob. However, under our assumptions, it is impossible for Eve to coherently disrupt Alice's signals. The reason is that any error in estimating the propagation delay, multipath, and possibly mobility between Alice, Bob, and herself will result in noncoherent interruption. Thus, though Eve may try to modify certain symbols by overpowering Alice's signal with her malicious signal, she will only corrupt the signal incoherently. Hence, Eve can transmit her own blocks, or noncoherently interfere with Alice's blocks, but cannot arbitrarily modify Alice's signals en route in a controlled manner. This is a fundamental restriction at the physical layer of a mobile wireless system.

To defeat the authentication scheme, Eve must be able to cause Bob to 1) reject authentic messages or 2) accept inauthentic messages with nonzero probability. In order to succeed with goal 1), Eve needs to remove or corrupt the authentication tag, and to succeed with goal 2), Eve needs to have her malicious block accepted by Bob since she is unable to intelligently alter Alice's messages.

2) Jamming Attacks: One way that Eve can try to remove the authentication tag is through corruption. She can do this by transmitting a jamming signal while Alice is transmitting to Bob in an attempt to mask the tag. This signal may be viewed as a degradation in SNR and, hence, may be combatted by increasing the strength of the authentication test as discussed in Section III-B, or through conventional physical-layer methods of cochannel interference rejection.

3) Replay Attacks: Eve may be interested in having Bob accept inauthentic messages (i.e., the messages that someone other than Alice transmits). Eve can simply replay a message that Alice transmitted in the past in what is called a replay attack. However, since we assume the tag is time-varying (11), Bob will not accept it again.

4) Impersonation Attacks: Eve may try to create her own messages and tags that she hopes will be accepted by Bob. In this way, she impersonates Alice. The probability that Eve's message will be authenticated depends on the authentication performed by Bob. When the authentication considers multiple blocks and requires a certain number of tags to be verified, Eve may be able to have her block accepted even if it does not contain a valid tag. Suppose that Bob requires at least k tag detections in K blocks to authenticate. When only Alice transmits to Bob, the detection probability is simply $\sum_{i=k}^{K} B(i;K,P)$. However, when Eve inserts her own block, a tag is detected in the block with probability α. The new detection probability is then $\sum_{i=k}^{K} B(i;K-1,P) + \alpha B(k-1;K-1,P)$.

Realistically, there would be additional safeguards at the other layers to prevent malicious messages from being accepted in the midst of authentic messages. For example, the authentication requires multiple blocks only when a single block is insufficient to provide an accurate decision. This case indicates a noisy channel and, hence, the messages would be coded across multiple blocks as well, for example, by using an erasure code. In such cases, malicious blocks will be either detected or discarded, but will not have an impact on the decoded messages.

However, in the original scheme (Section II-C4), each message is required to have a valid tag. Since Eve does not have the secret key, she must generate valid tags based on her observations. In other words, she must predict future tags. Tag prediction is resisted by having a key $\mathbf{k}$ with reasonable entropy and a suitable tag generation function $g(\cdot)$. For example, $g(\cdot)$ may be a pseudorandom number generator seeded by $\mathbf{k}$. The output of the generator appears to be random and difficult to predict by design. The subsets of the output can be used as the tags.

Eve may take a more direct approach and attempt to gain information about the secret key. In the worst case, Eve can completely recover $\mathbf{k}$ and impersonate Alice at will. With a K-bit secret key, one of up to 2^K distinct tags will be assigned to a given message. If the tags are observed without noise and the observation length is sufficiently large, the key may be recovered without error.

However, the tags are always observed with noise, and the key recovery becomes probabilistic. Intuitively, the key can be recovered with high probability when the noise is minimal but with lower probability when the noise is more powerful. This is a fundamental difference between our proposed scheme and previous work in authentication: we capitalize on the noise to hide the authentication tags and protect the key from discovery.

To state the key recovery problem precisely, we introduce equivocation as our central measure for key security. Equivocation [19], [20] is the entropy of the key given all past observations

$$\Delta_i \triangleq H(\mathbf{k}|\mathbf{y}_i, \mathbf{y}_{i-1}, \dots \mathbf{y}_1). \tag{32}$$

When there is no noise and sufficiently many blocks are observed, we have $\Delta_i = 0$, $i < \infty$, and key recovery is guaranteed in finite time. In the presence of noise, however, the equivocation is nonzero for finitely many observations and, hence, the probability of key recovery is strictly less than unity. As the noise becomes more powerful, the equivocation is near its upper bound $\Delta_i \approxeq H(\mathbf{k})$, $i < \infty$ and approaches zero very slowly. Assuming uniformly distributed keys, the probability of key recovery is about 2^{-K} for finite i, the same as a random guess.

To get a feel for the equivocation present in our system, we revisit the simple example introduced in Section III-A1 and consider the equivocation of a tag symbol. Again, each tag symbol is represented by one of two equiprobable and polar values $\pm\sigma_t$ and is observed in AWGN $y_k = t_k + w_k$. The TNR is σ_t^2/σ_w^2. Eve determines which tag symbol was sent by performing a sign

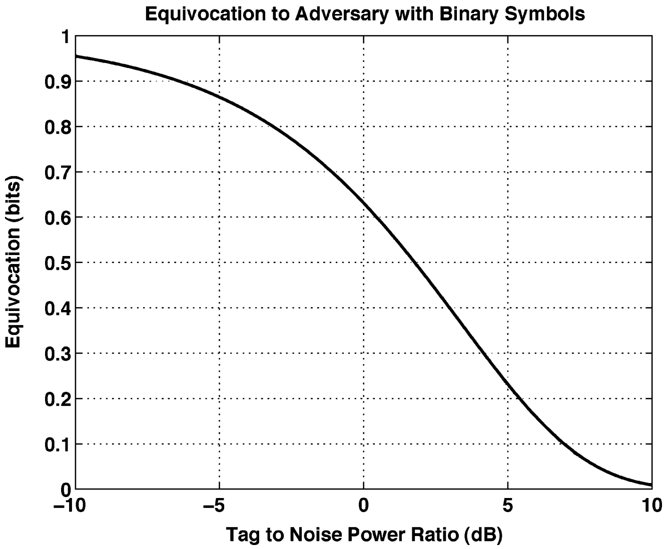


Fig. 11. Equivocation of the binary tag signal to the adversary for varying TNR. Low TNR yields high equivocation.

test on y_k. The probability of error is simply $p_e = \Phi(-\sigma_t/\sigma_w)$. The equivocation of the decision is given by the binary entropy

$$H(t_k|y_k) = p_e \log_2 \frac{1}{p_e} + (1-p_e)\log_2 \frac{1}{(1-p_e)}. \tag{33}$$

At low TNR, the equivocation of the transmitted symbol is quite high as seen in Fig. 11. As the equivocation approaches unity, no information is gained about the tag symbol.

We now consider how Eve may attempt to recover the key. She estimates the residual by removing the message from $\mathbf{y}_i$. Since Eve estimates each tag symbol with some nonzero error, her search space for the key expands depending on the tag symbol equivocation. A straightforward solution is to compute the tags corresponding to each possible key (there are 2^K), then select the key that generates the signal most similar to the residual. This is the brute force method. However, with a sufficiently large K, this is impractical since Eve will run into computation and memory restraints. The remaining alternative is to attempt the inversion of $g(\cdot)$.

When the image of $g(\cdot)$ is observed with sufficient length and without noise, Eve may be able to recover the key in reasonable time. This would be a real concern in the higher layers. However, we use $g(\cdot)$ in the physical layer where the tag is never known without error. The adversary has no choice but to spread its key recovery efforts among the probable tags. For binary tag symbols, the number of possible transmitted words doubles as each tag symbol is estimated. The receiver must prune the possibilities to consider only the more probable tags; otherwise, all possible tags would be considered.

The set of probable tags depends on the tag symbol error probability p_e. When p_e is small, the paths that include few errors should be considered more probable, while the opposite is true when p_e is large. For example, suppose that the receiver estimates the tag sequence 000. When p_e is small, the most likely transmitted sequence is 000, and the second most likely sequences are $\{001, 010, 100\}$. The least likely transmitted sequence is 111. If we have a length-L observation and choose to consider paths with k or fewer errors, we expand the search space by $\sum_{i=0}^{k} \binom{L}{i}$, which is a polynomial factor for fixed k.

Because of Eve's uncertainty in her estimation of tag symbols, the search space for the secret key expands significantly. As long as the secret key has sufficient entropy to resist brute force attacks and the tag has low power, it becomes very difficult for Eve to recover the key.

IV. System Tradeoffs

A. Tradeoffs

We illustrate the tradeoffs of the scheme by studying an example.

Consider a system where the message symbols are i.i.d. equiprobable binary variables. The message is coded with a rate 1/2 Hamming code and then modulated with binary phase-shift keying (BPSK) and a root raised cosine pulse shape (with rolloff factor 0.5). The block length L is determined by the coherence time of the channel. We insert a 16-b pilot sequence in the middle of the block for channel estimation.

We use the Haar (or, equivalently, the Daubechies 2) wavelet to decompose the BPSK signal prior to pulse shaping. We use one level of wavelet decomposition and use all L possible coefficients to describe the tags. The spectrum is slightly perturbed and managed by pulse shaping. The tag energy is distributed as follows. The ith tag is generated from the L-bit output of a pseudorandom number generator (PRNG) $g(\cdot)$ using $\mathbf{k}+i$ as its seed. The L bits are mapped to ±1 so that $E|\mathbf{t}|^2 = L$. Without loss of generality, we assume $\mathbf{k} = 0$. The tag is therefore

$$\mathbf{t}_i = \{g(i)\}_{L\,\text{bits}}. \tag{34}$$

Over a fading block, we therefore have a constant $\text{TNR} = \rho_s^2 \gamma_i$ for each coefficient.

With the aforementioned parameters in place, the system chooses to operate with a given power allocation ρ_s^2 and uses a detection test with certain false alarm and detection probabilities. To give a preview of the results, ρ_s^2 is the major parameter that affects all three properties: stealth, robustness, and security. Stealth and security require low tag energy, while robustness requires the opposite. However, these requirements are able to find common ground when the detection test is chosen appropriately. When a power allocation gives insufficient power to the tag, the authentication probability of a single tag may be unacceptably low. This problem is easily addressed by extending the authentication decision to consider multiple blocks instead. We elaborate on this discussion by considering the three properties in turn.

B. Stealth

We consider the impact of the scheme on the unaware receiver by observing the increase in outage probability and BER. The outage probability is shown in Fig. 10 as a function of ρ_s^2 for various minimum SNR γ^0. The outage probability is fixed at 0.05. When the requirements of the channel are less stringent (higher γ^0), there is more flexibility in the allocation of power to the tag. For example, when $\gamma^0 = 9$ dB, we can allocate 2%

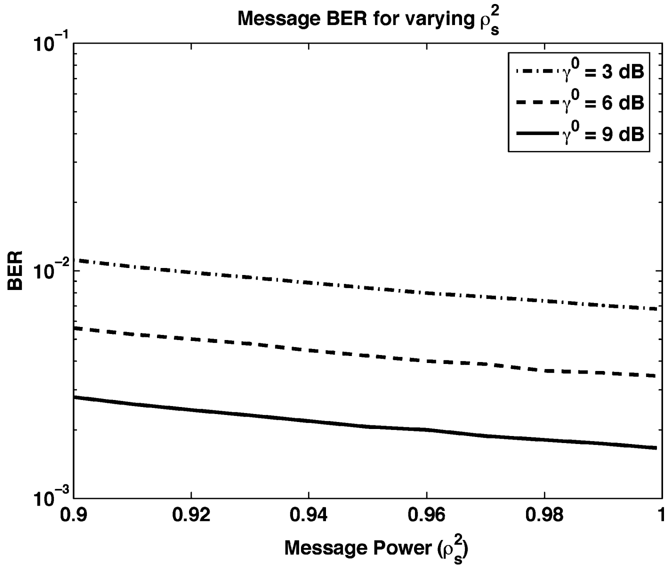


Fig. 12. BER for tagged signals in Rayleigh fading for various γ^0 with outage probability $P_{\text{out}} = 0.05$.

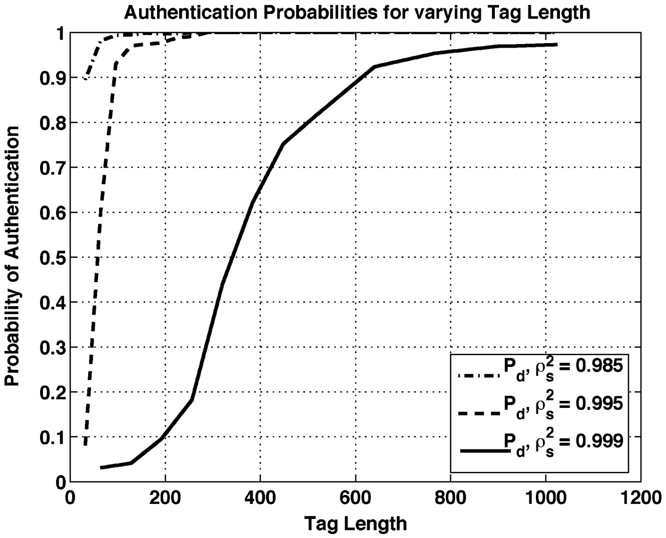


Fig. 13. Authentication probabilities for $\rho_s^2 \in \{0.985, 0.995, 0.999\}$ over a single tag with false alarm probability $\alpha = 0.01$. We assume the tag length coincides with channel coherence time. Lower ρ_s^2 is more robust to short coherence times.

of the power to the tag without pushing the outage probability over 0.06. However, when $\gamma = 6$ or 3 dB, we can allocate more than 4 or 5% of the power. The outage probability is therefore dependent on power allocation and the SNR requirements with increased sensitivity for stricter requirements.

The BER for the unaware receiver is shown in Fig. 12 as a function of ρ_s^2 for various minimum SNR γ^0. The outage probability is fixed at 0.05. The baseline BER is the point where $\rho_s^2 = 1$, because no power is allocated to the tag. We note that the BER curves are rather flat where ρ_s^2 is near 1. This gives us the flexibility of choosing from a range of possible power allocations. As shown before in the outage probabilities, stricter SNR requirements (γ^0) restrict the power allocations.

As discussed in Section III-A1, the Lilliefors test is unable to detect anomalous signals for ρ_s^2 near 1. Thus, the requirements given by the outage probabilities and BER are harmonious and advocate high ρ_s^2. Suppose that $\gamma^0 = 6$ dB and we can tolerate a BER of $4 * 10^{-3}$ ($\rho_s \geq 0.98$) and an outage probability of 0.055 ($\rho_s \geq 0.985$). Thus, we satisfy both constraints with $\rho_s^2 = \max(0.98, 0.985)$ and, hence, we can safely allocate up to 1.5% of the power to signal the tag while satisfying the constraints of stealth.

C. Robustness

While stealth requires low tag power, robustness requires sufficient tag energy for reliable detection. The tag energy is dependent on two factors: tag power and tag length. When the tag length exceeds the block length, the authentication decision would consider multiple tags. The effect of tag length on the authentication probability is shown in Fig. 13 for various power allocations ρ_s^2. Here, we assume that the tag is as long as a single fading block. The minimum SNR is $\gamma^0 = 6$ dB with outage probability 0.05.

For a fixed ρ_s^2, the energy of the tag increases and, hence, the authentication performance improves with increasing the block length, so the performance is tied directly to the coherence time of the channel. Consider the situation when $\rho_s^2 = 0.999$ and the false alarm probability is $\alpha = 0.01$. When $L = 1024$ symbols, the tag detection probability is 0.973, while it drops to 0.811 when $L = 512$. Though the channel coherence time is out of our control, we can code across blocks by authenticating only when at least two tags are detected out of four blocks. With this rule, the new authentication probability is 0.978 and the false alarm probability is 0.0006 (using (31) and (27), respectively).

D. Security

When multiple blocks are used for the authentication, the additional robustness gives the adversary more opportunities to pass inauthentic blocks to Bob. The tradeoff between robustness and security is fundamental—by allowing more errors in the authentication process, Eve has a better opportunity to sneak in her own messages. However, we suggest that Eve's impersonation attempts are futile when messages are coded across blocks, which is typically incorporated in the presence of block fading to mitigate outage effects. Hence, Eve's message will be decoded as part of a larger stream, and will be either corrected or discarded by the decoder. Eve must therefore be able to convince Bob to accept a stream of tagged messages, something that is very difficult when she does not know the secret key.

The security of the scheme is demonstrated by its stealth and the analysis in Section III-C. For a fixed ρ_s^2, the TNR is different for every realization of the channel. When $\overline{\gamma} = 18.9$ dB, we have $E[\gamma] = \sqrt{\pi/2\overline{\gamma}} = 19.88$ dB $= 97$. The expected TNR when $\rho_s^2 = 0.985$ is $\text{TNR}(0.015, 97) = 1.6$ dB. From Fig. 11, the corresponding equivocation is 0.51 b/coefficient. For $\rho_s^2 = 0.995$ and 0.999, the corresponding equivocations are, respectively, 0.79 and 0.95 b/coefficient. Since each coefficient contains a single bit of tag information, equivocations near 1 keep adversaries in confusion about the tag, and, hence, their search space grows by nearly the worst case 2^L per block.

Of course, assuming that Eve is able to estimate the tags, she still must break the tag generation in order to perform her attacks. Thus, we see that the scheme has two levels of defense: Eve has difficulty understanding the stealthy transmissions, and even if she can correct any errors in her observation, she still has the nontrivial task of breaking the tag generation.

E. Operating Point

The choice of parameters is guided by the relative importance of stealth, robustness, and security. In our example system, we see that our stealth requirements are satisfied when $\rho_s^2 \geq 0.985$. If we choose the minimum acceptable $\rho_s^2 = 0.985$, then we see from Fig. 13 that the authentication is robust to even short coherence times, with authentication probabilities above 0.99 for $L >$ 96 b. The corresponding equivocation for this power allocation is 0.51 b/coefficient. If the tag generation function is reasonably difficult to break, then this equivocation is acceptable. However, if we want to transmit the tags in near perfect secrecy, we must increase the equivocation by increasing ρ_s^2.

Suppose that we set $\rho_s^2 = 0.999$. In this case, the tag has a minimal impact on BER and outage probability, and the equivocation rises to 0.95 b/coefficient. However, the tag detection probability over a single tag is decreased depending on L. For all but relatively long coherence times ($L > 1024$), the authentication probability should be increased by using multiple blocks for the decision. When the coherence time is short, many blocks may be necessary: in the case where $L = 256$, the authentication probability of 0.99 requires that at least 1 tag be detected out of 23 blocks. (As discussed in Section III-C, this situation is not usually vulnerable to impersonation attacks because of message coding across blocks). A decision is then made after $256 * 23 = 5888$ b in comparison to after 1024 b in the long coherence time situation.

V. Extension to Time-Varying Fading Channels

A natural question that may arise is how well the scheme works in fast fading channels. To tackle this question, we introduce another channel model and the associated channel estimation algorithm. We find that the aware receiver can even improve his or her message recovery by treating the authentication tag as pilot symbols, and we detail the necessary changes.

A. Channel Model

Instead of the channel used in Section II-B2, we use a Gauss–Markov channel model to describe fast flat fading [21]. Rather than assuming a constant fade for each block of symbols, each symbol suffers a different but correlated fade. The channel for the kth symbol is

$$h_k = ah_{k-1} + u_k \tag{35}$$

where a is the fading correlation coefficient and $u_k \sim N(0, \sigma_u^2)$, where $\sigma_u^2 = (1-a^2)\sigma_h^2$. The fading correlation coefficient characterizes how quickly the channel fades: large values (close to unity) model slow fading channels while small values model fast fading channels. After passing through the channel, the receiver observes the signal $\mathbf{y}$

$$y_k = h_k x_k + w_k \tag{36}$$

$$\mathbf{y}_i = \mathbf{h}_i \cdot \mathbf{x}_i + \mathbf{w}_i \tag{37}$$

where as before $w_k \sim N(0, \sigma_w^2)$ is white Gaussian noise. Note that we still treat the message in blocks but now the channel is a vector $\mathbf{h} = \{h_1, \cdots, h_L\}$. The average SNR is $\overline{\gamma} = \sigma_h^2 / \sigma_w^2$.

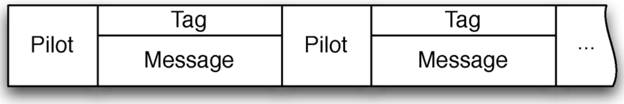


Fig. 14. TDM pilot placement.

B. Channel Estimation

By modeling the channel as an AR-1 process, we are able to use the Kalman filter to provide the linear minimum mean square error (MMSE) channel estimate. We use periodic pilot symbols to aid channel estimation but we use them more frequently because the channel is fast fading. We have T_p pilot symbols preceding every cluster of T_d data (i.e., message and tag) symbols and we let $T = T_p + T_d$. Thus, pilots are inserted into $\mathbf{x}$ such that $\{x_k\}|_{(k \bmod T < T_p)}$ are pilots and the rest are data (see Fig. 14).

The channel estimation is slightly different depending on if the tag presence is unknown or if it is assumed to be present. The presence is unknown, for example, by the unaware receiver, the aware receiver without the key, or the aware receiver who has not been able to verify it yet. However, once the intended receiver verifies the presence, it may use the tag as extra information to estimate the channel.

1) Tag Presence Unknown: The equations for channel state (35) and observation (4) are used to construct the filter. The filter trains itself to make increasingly accurate estimates while it is receiving the pilot symbols p_k. We have the following filter update equations during the training period $(k \bmod T < T_p)$ [14]:

$$[\text{Kalman gain}]K_k = \frac{\left(a^2 M_{k-1} + \sigma_u^2\right) p_k}{\sigma_w^2 + \left(a^2 M_{k-1} + \sigma_u^2\right) \sigma_p^2} \tag{38}$$

$$[\text{Estimate}]\hat{h}_k = a\hat{h}_{k-1} + K_k(y_k - a\hat{h}_{k-1} p_k) \tag{39}$$

$$[\text{MMSE}]M_k = (1 - K_k p_k) \cdot \left(a^2 M_{k-1} + \sigma_u^2\right). \tag{40}$$

When the training period is over, the filter estimates the channel based on the AR-1 model (35). The update equations during the data period $(k \bmod T \geq T_p)$ are

$$\begin{aligned}[\text{Channel Estimate}]\hat{h}_k &= a\hat{h}_{k-1} \\ [\text{MMSE}]M_k &= a^2 M_{k-1} + \sigma_u^2 .\end{aligned}$$

The channel estimate for the ith block is the vector $\hat{\mathbf{h}}_i$.

2) Tag Assumed Present: The aware receiver with the secret key can potentially obtain a better channel estimate than the unaware receiver. Recall that for authentication, our authentication tags must be known at the receiver. Therefore, they may be used for channel estimation in exactly the way as pilot symbols, provided that the tag is indeed present. The receiver who uses this information operates as follows. As soon as it can generate the estimated tag using (16), it uses $\hat{\mathbf{t}}_i$ to adaptively track the channel during data symbol reception. Since the channel estimation does not change during the pilot symbol reception, (38)–(40) do not change.

When the data symbols are received, however, the Kalman filter continues to update and track the signal by using the tag which it decides is present. Assuming that the estimated tag is present, we rewrite the observation

$$\begin{aligned} y_k &= \rho_s h_k s_k + \rho_t h_k t_k + w_k && (41)\\ &= \rho_t h_k t_k + v_k. && (42) \end{aligned}$$

Note that $v_k \sim N(0, \rho_s^2\sigma_h^2 + \sigma_w^2)$. The update equations during the training period $(k \bmod T < T_p)$ are [14]

$$\begin{aligned} [\text{Kalman gain}]K_k &= \frac{\left(a^2M_{k-1}+\sigma_u^2\right)\rho_t t_k}{\sigma_v^2 + \left(a^2M_{k-1}+\sigma_u^2\right)\rho_t^2} && (43)\\ [\text{Estimate}]\hat{h}_k &= a\hat{h}_{k-1} + K_k(y_k - a\rho_t\hat{h}_{k-1}t_k) && (44)\\ [\text{MMSE}]M_k &= (1-\rho_t K_k t_k)\cdot\left(a^2M_{k-1}+\sigma_u^2\right). && (45) \end{aligned}$$

Comparing (43)–(45) with (38)–(40) reveals that σ_w^2 is replaced with σ_v^2 and p_k is replaced with $\rho_t t_k$. The channel estimate that assumes the tag is present for the ith block is the vector $\hat{\mathbf{h}}_i$.

C. Message Recovery

1) Tag Presence Unknown: As before, the receiver uses its channel estimate $\hat{\mathbf{h}}$ to estimate the message signal

$$x_k = \frac{\hat{h}_k^*}{|\hat{h}_k|^2} y_k \qquad (46)$$

and uses (10) to recover the message symbols as before.

2) Tag Assumed Present: If the receiver decides that the tag is present, not only can it remove it prior to message estimation, it can also use the improved channel estimate $\hat{\mathbf{h}}_i^+$. The estimated message signal is then

$$x_k = \frac{1}{\rho_s}\left(\frac{\left(\hat{h}_k^+\right)^*}{\left|\hat{h}_k^+\right|^2} y_k - \rho_t t_k\right) \qquad (47)$$

and uses (10) to recover the message symbols as before.

D. Authentication

The authentication process remains unchanged. Of course, the channel estimate used in the tag detection should not use the tag as pilot symbols; otherwise, the reasoning is circular (testing the tag presence while assuming that it is there for channel estimation).

E. Example and Results

We consider a system where messages are modulated with BPSK with a root-raised cosine pulse shape (rolloff $\alpha = 0.5$). We do not code the message symbols. We set the length of the transmitted blocks to be $L = 4096$ b. Two pilot symbols precede every cluster of eight message and tag symbols ($T_p = 2$, $T_d = 8$). The tag is generated with a PRNG as in Section IV. The message and tag are then modulated, scaled with $\rho_s^2 = 0.995$, and transmitted through the time-varying channel with $a = 0.995$.

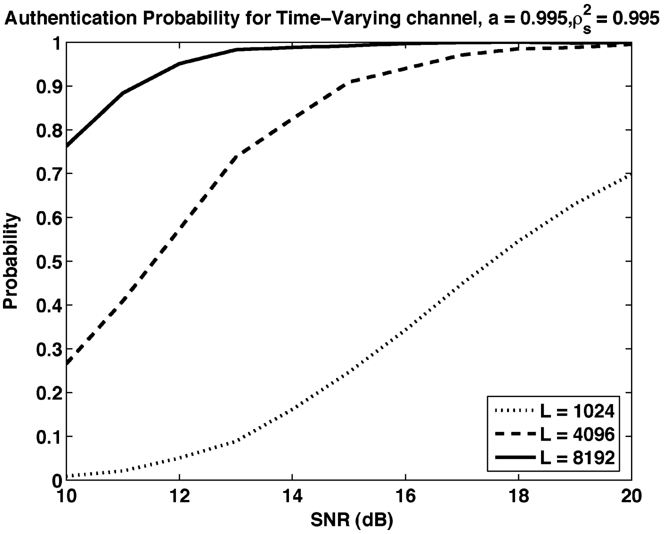


Fig. 15. Probability of tag detection for various tag lengths with a time-varying channel with fading coefficient $a = 0.995$ and false alarm probability $\alpha = 0.01$, $\rho_s^2 = 0.995$.

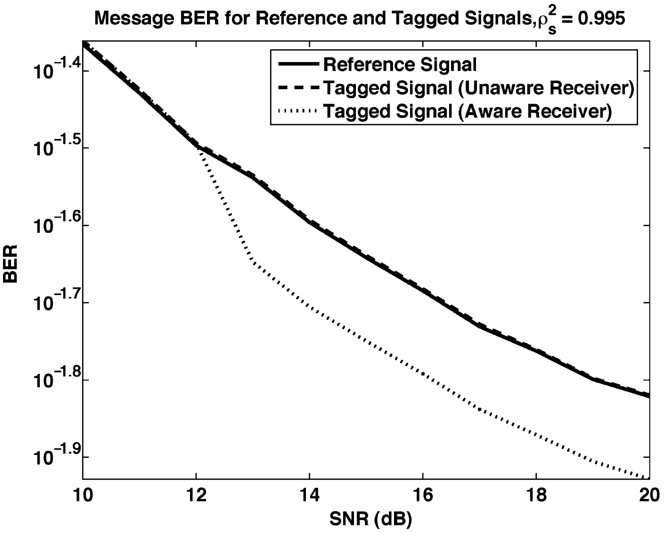


Fig. 16. BER in the time-varying channel versus $\overline{\gamma}$ for unaware, aware receivers with tag length $L = 4096$ and fading coefficient $a = 0.995$, $\rho_s^2 = 0.995$.

The detection and probabilities for various tag lengths L are shown in Fig. 15. The tags are more easily detected at higher SNRs and for longer tag lengths. The BER versus SNR is shown in Fig. 16 for the particular case of $L = 4096$. Note that the performance of the aware and unaware receivers coincides when the tag is not taken into account. However, when the tag is assumed to be present, the aware receiver with the key is able to decode the messages with lower BER. The decrease in BER is not apparent at low SNRs because the tags are not detected and, hence, the improved channel estimate is not used. Of course, at higher SNRs, the tags are detected more often and the alternate channel estimate can be used.

VI. Conclusion

A flexible framework for describing and analyzing a large family of physical-layer authentication schemes that can be built over existing transmission systems is presented. Authentication information is sent concurrently with data without requiring extra bandwidth or transmission power. With these constraints, energy is allocated away from the data signal to the authentication signal, thereby increasing the probability of data recovery error. However, with a long enough authentication codeword, a useful authentication system can be achieved with very slight data degradation. Additionally, by treating the authentication tag as a sequence of pilot symbols, the data recovery can actually be improved by the aware receiver. An interesting extension to the framework considers how cross-layer designs may strengthen node security. Authentication policies based on the authentication mechanism may adapt according to the environment for example.

References

[1] G. J. Simmons, "A survey of information authentication," *Proc. IEEE*, vol. 76, no. 5, pp. 603–620, May 1988.

[2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone*, Handbook of Applied Cryptography*. Boca Raton, FL: CRC, 2001.

[3] T. M. Cover, "Broadcast channels," *IEEE Trans. Inf. Theory*, vol. IT-18, no. 1, pp. 2–14, Jan. 1972.

[4] C. Fei, D. Kundur, and R. H. Kwong, "Analysis and design of secure watermark-based authentication systems," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 1, pp. 43–55, Mar. 2006.

[5] L. M. Marvel, C. G. Boncelet, Jr., and C. T. Retter, "Spread spectrum image steganography," *IEEE Trans. Image Process.*, vol. 8, no. 8, pp. 1075–1083, Aug. 1999.

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

[7] J. G. Proakis*, Digital Communications*. New York: McGraw-Hill, 2000.

[8] S. H. Supangkat, T. Eric, and A. S. Pamuji, "A public key signature for authentication in telephone," in *Proc. APCCAS*, 2002, pp. 495–498.

[9] J. E. Kleider, S. Gifford, S. Chuprun, and B. Fette, "Radio frequency watermarking for OFDM wireless networks," in *Proc. ICASSP*, Montreal, QC, Canada, 2004, pp. 397–400.

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

[11] L.-F. Wei, "Coded modulation with unequal error protection," *IEEE Trans. Commun.*, vol. 41, no. 10, pp. 1439–1449, Oct. 1993.

[12] P. K. Vitthaladevuni and M.-S. Alouini, "Exact BER computation of generalized hierarchical PSK constellations," *IEEE Trans. Commun.*, vol. 51, no. 12, pp. 2030–2037, Dec. 2003.

[13] M. Morimoto, M. Okada, and S. Komaki, "A hierarchical image transmission system in a fading channel," in *Proc. 4th IEEE Int. Conf. Universal Personal Communications*, Nov. 1995, pp. 769–772.

[14] M. Dong, L. Tong, and B. M. Sadler, "Optimal insertion of pilot symbols for transmissions over time-varying flat fading channels," *IEEE J. Sel. Areas Commun.*, vol. 52, no. 5, pp. 1403–1418, May 2004.

[15] J. E. Kleider, G. Maalouli, S. Gifford, and S. Chuprun, "Preamble and embedded synchronization for RF carrier frequency-hopped OFDM," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 5, pp. 920–931, May 2005.

[16] J. Fridrich and M. Goljan, "Robush hash functions for digital watermarking," in *Proc. Int. Conf. Information Technology: Coding and Computing*, Las Vegas, NV, Mar. 2000, pp. 178–183.

[17] A. Swaminathan, Y. Mao, and M. Wu, "Robust and secure image hashing," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp. 215–230, Jun. 2006.

[18] K. Ramchandran, M. Vetterli, and C. Herley, "Wavelets, subband coding, and best bases," *Proc. IEEE*, vol. 84, no. 4, pp. 541–560, Apr. 1996.

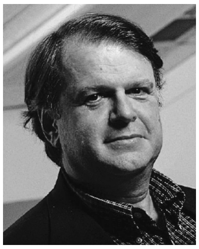
[19] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pp. 379–423, Jul. 1948.

[20] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pp. 623–656, Oct. 1948.

[21] M. Medard, "The effect upon channel capacity in wireless communications of perfect and imperfect knowledge of the channel," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 933–946, May 2000.

Paul L. Yu received the B.Sc. degree in mathematics (Hons.) and the B.Sc. degree in computer engineering from the University of Maryland, College Park (UMCP), in 2002 and 2003, respectively, where he is currently pursuing the Ph.D. degree.

Currently, he is a Graduate Research Assistant in the Department of Electrical and Computer Engineering at UMCP. His research interests include signal processing and security over wireless networks.



John S. Baras (F'84) was born in Piraeus, Greece, on March 13, 1948. He received the B.S. degree in electrical engineering (Hons.) from the National Technical University of Athens, Athens, Greece, in 1970, and the M.S. and Ph.D. degrees in applied mathematics from Harvard University, Cambridge, MA, in 1971 and 1973, respectively.

Since 1973, he has been with the Department of Electrical and Computer Engineering, University of Maryland at College Park, where he is currently Professor, member of the Applied Mathematics and Scientific Computation Program Faculty, and Affiliate Professor in the Department of Computer Science. From 1985 to 1991, he was the Founding Director of the Institute for Systems Research (ISR) (one of the first six National Science Foundation Engineering Research Centers). In 1990, he was appointed to the Lockheed Martin Chair in Systems Engineering. Since 1991, he has been the Director of the Maryland Center for Hybrid Networks (HYNET), which he co-founded. He has held visiting research scholar positions with Stanford, Massachusetts Institute of Technology, Harvard, the Institute National de Reserche en Informatique et en Automatique, the University of California at Berkeley, Linkoping University, and the Royal Institute of Technology, Sweden. His research interests include control, communication, and computing systems. He is a Foreign Member of the Royal Swedish Academy of Engineering Sciences (IVA). He is a member of ACM, SIAM, AMS, AIAA, ATA, and Sigma Xi. He has published many refereed publications, graduated 60 Ph.D. students, and sponsored 40 postdoctoral scholars. He was the editor of the book *Recent Advances in Stochastic Calculus* (Springer, 1990). He holds three patents and has three more patents pending. He has co-founded three small companies. He was the initial principal architect of the ISR M.S. program in systems engineering. More recently, he has been heavily involved in the development of new core courses for systems engineering, addressing the need for a new integrative approach to engineering.

Dr. Baras received the 1980 George S. Axelby Prize of the IEEE Control Systems Society; the 1978, 1983 and 1993 Alan Berman Research Publication Award from NRL; the 1991 and 1994 Outstanding Invention of the Year Award from the University of Maryland; the 1996 Engineering Research Center Award of Excellence for Outstanding Contributions in Advancing Maryland Industry; the 1998 Mancur Olson Research Achievement Award, from the University of Maryland, College Park; the 2002 Best Paper Award at the 23rd Army Science Conference; the 2004 Best Paper Award at the Wireless Security Conference WISE04; and the 2007 IEEE Communications Society Leonard G. Abraham Prize in the Field of Communication Systems. He has served on the IEEE Engineering R&D Committee, the Aerospace Industries Association Advisory Committee on Advanced Sensors, the IEEE Fellow Evaluation Committee, and the IEEE Control Systems Society Board of Governors (1991–1993). He is currently serving on the editorial boards of *Mathematics of Control, Signals and Systems*, *Systems and Control: Foundations and Applications*, *IMA Journal of Mathematical Control and Information*, and *Systems Automation—Research and Applications*.

Brian M. Sadler (F'06) received the B.S. and M.S. degrees from the University of Maryland, College Park, and the Ph.D. degree from the University of Virginia, Charlottesville, all in electrical engineering.

Currently, he is a Senior Research Scientist with the Army Research Laboratory (ARL), Adelphi, MD. He was a Lecturer at the University of Maryland, and has been lecturing at Johns Hopkins University, Baltimore, MD, since 1994 on statistical signal processing and communications. He is an Associate Editor for the IEEE SIGNAL PROCESSING LETTERS and the IEEE TRANSACTIONS ON SIGNAL PROCESSING, and has been a Guest Editor for several journals including the *IEEE Journal on Selected Topics in Signal Processing*, *IEEE Journal on Selected Areas in Communications*, and the *IEEE Signal Processing Magazine*. His research interests include signal processing for mobile wireless and ultra-wideband systems, sensor signal processing and networking, and associated security issues.

Dr. Sadler is a member of the IEEE Signal Processing Society Sensor Array and Multi-channel Technical Committee, and received a Best Paper Award (with R. Kozick) from the Signal Processing Society in 2006.