Multicarrier Authentication at the Physical Layer

Paul L. Yu and John S. Baras
University of Maryland
College Park, MD 20742
{paulyu, baras}@umd.edu

Brian M. Sadler
Army Research Laboratory
Adelphi, MD 20783
bsadler@arl.army.mil

Abstract

Authentication is the process where claims of identity are verified. Though authentication mechanisms typically exist above the physical layer, physical layer methods have recently been introduced that do not require extra bandwidth. In this paper we propose a multi-carrier extension to the work and consider the stealth and robustness tradeoffs. We conclude by discussing the power-reliability tradeoff and the applicability to cross-layer security.

1 Introduction

Physical layer authentication systems have been shown to be stealthy, robust, and secure [4] in single carrier systems. In this paper we consider extensions in multi carrier systems to improve these properties.

Multi-carrier systems are increasingly prevalent for wideband wireless communications. We are motivated by the single-carrier authentication results to consider how an authentication system can use multiple carriers to improve its stealth and robustness.

By using multiple carriers, the authentication tags can be hidden in both time and frequency. However, using multiple carriers also introduces some additional wrinkles. Frequency-selective fading attenuates the carriers unequally, thus allowing only some of the symbols to be recovered. We give results that indicate that the authentication can be made robust to channel conditions with reasonable parameters. We show that the single carrier PHY authentication ideas can be extended to the multi-carrier case, without sacrificing stealth or robustness.

2 Physical Layer Authentication

In this paper we consider single-antenna transceivers. The sender (Alice) has blocks of symbols that she wishes to transmit to the receiver (Bob). The adversary (Eve) is able to hear what Alice is transmitting and also transmit arbitrary messages to Bob.

Alice transmits messages to Bob in plain view: Eve can also recover the messages. In addition, Alice superimposes tags upon her messages for authentication purposes. Bob authenticates Alice only when he detects the correct tags in his received signal. When a signal contains an authentication tag, we say it is *tagged*. In the next section we describe how the messages and tags are created in a multi-carrier setting.

2.1 Multiple Carrier Signal Models

Suppose that Alice and Bob communicate using $N > 1$ sub-carriers. This is the situation with orthogonal frequency division multiplexing (OFDM). Of the N carriers, N^s are used to transmit messages and N^n are used as null carriers for spectral shaping. Each frame is composed of N^f OFDM symbols; hence there are $N^s N^f$ message symbols per frame. In addition to the message, there are $N^t N^f$ authentication symbols per frame. We allow the authentication to be superimposed on the message symbols only, and hence $N^t \leq N^s$.

The ith message is denoted by $\mathbf{B}_i$. The multi-carrier analogue of the single carrier case is straightforward. Alice and Bob share secret keys k_i which are used to generate the authentication signal. The message and authentication signals are respectively

$$\mathbf{S}_i = f_e(\mathbf{B}_i) \tag{1}$$
$$\mathbf{T}_i = g(\mathbf{B}_i, k_i) \tag{2}$$

where $f_e(\cdot)$ encapsulates any coding and modulation of the message symbols and $g(\cdot)$ generates the authentication tag from the corresponding message and secret key. Both signals are complex matrices of size $N \times N^f$ and satisfy

$$\sum_{m,n} I(S(m,n)) = N^s N^f \tag{3}$$
$$\sum_{m,n} I(T(m,n)) = N^t N^f \tag{4}$$

where $I(\cdot)$ is the indicator function. That is, the message signal has exactly $N^s N^f$ non-zero entries while the tag signal has exactly $N^t N^f$. We allow the tag symbols to be placed randomly across the message carriers (Figure 1). The placement of the tags may vary from frame to frame and is determined by the choice of $g(\cdot)$ (equation (2)). Because the tag is generated using a secret key, it is unknown to the adversary.

The frequency domain signal is formed by superimposing the tag atop the message

$$\mathbf{X}_i = \rho_s \mathbf{S}_i + \rho_t \mathbf{T}_i \tag{5}$$

where ρ_s, ρ_t are scalar terms that determine the signal power as discussed below. We assume that the message and tags are i.i.d. and thus in the following we drop the frame index i.

Assume that the message and tag symbols have unit variance. Therefore the energy of the message and tag are given by their Frobenius norm, respectively

$$||\mathbf{S}||^2 = \text{Trace}(\mathbf{S}^H \mathbf{S}) = N^s N^f \tag{6}$$
$$||\mathbf{T}||^2 = \text{Trace}(\mathbf{T}^H \mathbf{T}) = N^t N^f \tag{7}$$

where $(\cdot)^H$ denotes Hermitian transpose. Further, we assume that the message and tag symbols are uncorrelated, so

$$E[\text{Trace}(\mathbf{S}^H \mathbf{T})] = 0 \tag{8}$$

The scale terms ρ_s and ρ_t are used to enforce the energy constraint

$$||\mathbf{S}||^2 = ||\mathbf{X}||^2 \tag{9}$$
$$= ||\rho_s \mathbf{S} + \rho_t \mathbf{T}||^2 \tag{10}$$
$$= (\rho_s)^2 ||\mathbf{S}||^2 + (\rho_t)^2 ||\mathbf{T}||^2 \tag{11}$$
$$(\rho_t)^2 = \frac{||\mathbf{S}||^2}{||\mathbf{T}||^2}(1 - (\rho_s)^2) \tag{12}$$
$$= \frac{N^s}{N^t}[1 - (\rho_s)^2] \tag{13}$$

Since N^s, N^t are fixed system parameters, specifying ρ_s determines ρ_t and vice versa. Therefore we only refer to $(\rho_s)^2$ since it is simply the percentage of power used to signal the message. The remaining power $1 - (\rho_s)^2$ is divided up amongst the tag symbols and depends on the ratio N^s/N^t.

Assuming perfect synchronization with Alice, Bob makes the signal observation

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{W} \tag{14}$$

where $\mathbf{H}$ is a diagonal matrix of carrier attenuations and $\mathbf{W}$ is AWGN. We assume slow fading so that the channel is held constant over the entire frame of symbols.
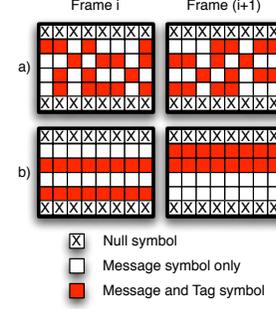
Figure 1. $N^f = 8, N^s = 4, N^t = 2$. **Tags are (a) randomly scattered or (b) on certain carriers.**

In this paper we assume that Bob uses pilot symbol assisted modulation (PSAM) to make the simplified minimum mean square error estimate (LMMSE) [1]. In general the channel estimate may be written

$$\hat{\mathbf{H}} = \mathbf{H} + \eta \tag{15}$$

where η is the channel estimation error.

Using the channel estimate, the receiver estimates the message signal as

$$\hat{X}(k) = \frac{\hat{H}^*(k)}{|\hat{H}(k)|^2} Y(k) \tag{16}$$
$$= X(k) - \frac{\eta(k)X(k)}{\hat{H}(k)} + \frac{W(k)}{\hat{H}(k)} \tag{17}$$

The estimated message is

$$\hat{\mathbf{B}} = f_d(\hat{\mathbf{X}}) \tag{18}$$

where $f_d(\cdot)$ is the decoding function corresponding to the encoder $f_e(\cdot)$ from equation (2).

For example, suppose that $f_e(\cdot)$ applies an error-correction code to the raw data $\mathbf{B}$. The corresponding decoder $f_d(\cdot)$ depends on the choice of code. Cyclic codes such as Reed-Solomon (RS) and Bose-Chaudhuri-Hocquneghem (BCH) can be efficiently decoded using Berlekamp-Massey algorithm [2].

2.2 Message Recovery

We consider the uncoded bit error probability of the symbols. For analysis, we assume that the message and tag symbols are modulated using QAM. For example, when the message and tag symbols are both modulated with 4-QAM, the tag constellation is superimposed on each message symbol to form the constellation shown in Figure 2. In the literature this is called the 4/16 hierarchical QAM constellation.

Note that the constellation has 16 symbols; each of these symbols signal the message symbol (which quadrant) and the tag symbol (which point in the quadrant). That is, the message symbol is fictitious in the sense that it is not actually transmitted.

To calculate the BER for a hierarchical QAM constellations, we must know the distance between the symbols (see Figure 2) as well as the noise power. $2d_1$ is the minimum distance between any two message points, $2d_2$ is the minimum distance between any two tag points within the same quadrant, and $2d'_1$ is the minimum distance between points in adjacent quadrants. We first give the exact BER expressions for unit-energy 4/16 constellations and then apply them to the authentication signals. In general, any number of QAM constellations may be superimposed on each other. The general expressions for the BER of general hierarchical QAM constellations are given in [3].

In AWGN, the BER of the message symbol can be written as [3]

$$p^s = \frac{1}{2}\left(\frac{1}{2}\text{erfc}\frac{d'_1}{\sqrt{N_0}} + \frac{1}{2}\text{erfc}\frac{d'_1 + 2d_2}{\sqrt{N_0}}\right) \quad (19)$$

$$= \frac{1}{4}\left(\Psi(1,0) + \Psi(1,2)\right) \quad (20)$$

where N_0 is the noise power, while the BER of the tag bit is

$$p^t = \frac{1}{2}\left(\text{erfc}\frac{d_2}{\sqrt{N_0}} + \frac{1}{2}\text{erfc}\frac{2d'_1 + d_2}{\sqrt{N_0}} \right.$$
$$\left. - \frac{1}{2}\text{erfc}\frac{2d'_1 + 3d_2}{\sqrt{N_0}}\right) \quad (21)$$

$$= \frac{1}{4}\left(2\Psi(0,1) + \Psi(2,1) + \Psi(2,3)\right) \quad (22)$$

The noise power N_0 is the average noise power for a unit variance channel. For perfect channel information, $1/\gamma$, while for MMSE estimation it is $1/\gamma^{lmmse} > 1/\gamma$. The helper function $\Psi(\cdot)$ [3] depends on the channel distribution, and for the Rayleigh channel with unit energy constellations it is

$$\Psi(a,b) = 1 - \sqrt{\frac{(ad'_1 + bd_2)^2\gamma}{1 + (ad'_1 + bd_2)^2\gamma}} \quad (23)$$

Next we consider three cases, depending on the tag locations.

2.2.1 Case 1: Each message symbol is tagged

For a symbol that contains both message and tag, we have that the message symbol is scaled by ρ_s and the tag symbol is scaled by ρ_t. Since the symbols are each unit variance, the effective SNR is $[(\rho_s)^2 + (\rho_t)^2]/\sigma_w^2$. In order to use Equations (19) and (21), the constellation needs to be unit

energy. Thus we scale

$$\tilde{\rho}_s = \rho_s/\sqrt{(\rho_s)^2 + (\rho_t)^2} \quad (24)$$

$$\tilde{\rho}_t = \rho_t/\sqrt{(\rho_s)^2 + (\rho_t)^2} \quad (25)$$

$$N_0 = \sigma_w^2/[(\rho_s)^2 + (\rho_t)^2] \quad (26)$$

and calculate the following parameters:

$$d_1 = \tilde{\rho}_s\sqrt{2} \quad (27)$$

$$d_2 = \tilde{\rho}_t\sqrt{2} \quad (28)$$

$$d'_1 = d_1 - d_2 \quad (29)$$

We calculate the BER of the message and tag bits by using these values in Equations (19) and (21). respectively.

2.2.2 Case 2: Message symbol only

When a message symbol stands alone without any superimposed tag, it uses the 4-QAM constellation. Note that it is still scaled by the term ρ_s, and thus the effective SNR is $(\rho_s)^2/\sigma_w^2$. Once again we scale in order to make the constellation unit energy:

$$\tilde{\rho}_s = 1 \quad (30)$$

$$\tilde{\rho}_t = 0 \quad (31)$$

$$N_0 = \sigma_w^2/(\rho_s)^2 \quad (32)$$

and calculate the following parameters:

$$d_1 = \tilde{\rho}_s\sqrt{2} \quad (33)$$

$$d_2 = 0 \quad (34)$$

$$d'_1 = d_1 \quad (35)$$

We calculate the BER of the message and tag bits by using these values in Equations (19) and (21). respectively.

2.2.3 Case 3: Some messages are tagged, others are not

Denote by p_1^s the message BER for the tagged case, and p_2^s the message BER for the untagged case. Let p_1^t, p_2^t be similarly defined for the tag BER. Given the fraction of tagged symbol N_t/N_s, the overall message and tag BER of the system is simply

$$p^s = \frac{N_t}{N_s}p_1^s - (1 - \frac{N_t}{N_s})p_2^s \quad (36)$$

$$p^t = \frac{N_t}{N_s}p_1^t - (1 - \frac{N_t}{N_s})p_2^t \quad (37)$$

2.3 Tag Detection

With his estimate of the data $\hat{\mathbf{B}}$, Bob uses $g(\cdot)$ from equation (2) to reconstruct the estimated tag:

$$\hat{\mathbf{T}}_k = g(\hat{\mathbf{B}}, k) \quad (38)$$

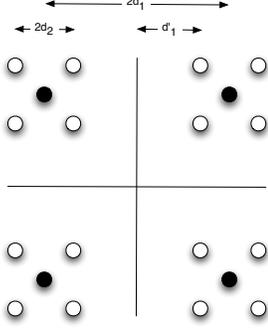Next we develop two cases, depending on whether the correct tag is generated.

Figure 2. 4/16 QAM constellation.

2.3.1 Case 1 - Bob generates the correct tag

Assuming that Bob generates the correct tag ($\hat{\mathbf{T}}_k = \mathbf{T}$), he uses matched filtering to detect it in his observation $\mathbf{Y}$. First, he calculates the residual $\mathbf{R}$ and then correlates it with the tag

$$\mathbf{R} = \frac{1}{\rho_t}\left(\mathbf{Y} - \frac{1}{\rho_s}f_e(\hat{\mathbf{B}})\right) \tag{39}$$

$$\tau_k = \text{tr}(\hat{\mathbf{T}}_k^H \mathbf{R}) \tag{40}$$

Assume that the Bob is synchronized with Alice and estimates the channel without error ($\hat{\mathbf{H}} = \mathbf{H}$). Then τ_k is a sum of $N^t N^f$ Gaussian variables. The resulting Gaussian variable has variance is $\sum_k \sigma^2(k)$, where the kth variance is $\sigma^2(m) = (\sum_m |T(m, n)|^2)/\gamma(m)$ where k is the carrier tone. The mean is simply $N^t N^f$ when the tag is present and we assume that it is 0 when the tag is not present.

Bob decides hypothesis H_δ according to

$$\delta = \left\{ \begin{array}{ll} 0 & \tau_k < \tau^0 \\ 1 & \tau_k \geq \tau^0 \end{array} \right\} \tag{41}$$

where the hypotheses are

$$H_0: \quad \hat{\mathbf{T}}_k \text{ is not present in } \mathbf{R} \tag{42}$$

$$H_1: \quad \hat{\mathbf{T}}_k \text{ is present in } \mathbf{R} \tag{43}$$

Bob calculates the threshold τ^0 as follows:

$$\tau^0(\gamma) = \arg\min_\tau \Phi(\tau/\sum_k c(\hat{\gamma}(k))) \geq 1 - \alpha \tag{44}$$

$$c(\gamma) = \frac{1}{\rho_t}\sqrt{N^t N^f/\gamma} \tag{45}$$

where α is the acceptable false alarm probability of the authentication. The probability of correct authentication given the carrier SNRs $\gamma(1), \ldots, \gamma(N_s)$ and $\hat{\mathbf{T}}_k = \mathbf{T}$ is

$$P^a(\gamma) = 1 - \Phi\left(\frac{\tau^0(\gamma) - N^t N^f}{\sum_k c(\gamma(k))}\right) \tag{46}$$

2.3.2 Case 2 - Bob generates an incorrect tag

When Bob generates the incorrect tag ($\hat{\mathbf{T}}_k = \mathbf{T}$), he will identify it as correct with false alarm probability α. Assuming that Bob has the correct key, it is clear from equation (38) that this occurs when his recovered message contains errors. Therefore, the performance of the authentication is directly tied to the performance of the message; authentication will occur only when the message is correctly received. This is logical because distorted messages should not be authenticated.

Consider the (n, k, t) BCH code. It encodes k message bits into n code bits and is able to recover from up to t errors. Consider the authentication system with parameters $\gamma, (\rho_s)^2, N_t$, and N_s. With LMMSE channel estimation the BER of the message symbols p^s is given by (36).

With bit interleaving, the symbol errors can be assumed independent, and thus the probability that there are at most t errors in n bits is given by

$$P = \sum_{i=0}^{t} \binom{n}{i}(p^s)^i(1 - p^s)^{n-i} \tag{47}$$

Thus the probability that the BCH code (n, k, t) can recover the message without error is P.

We can apply this result to the robustness of the authentication as follows. Given the correct tag, the authentication probability is $(P^a|\hat{\mathbf{T}} = \mathbf{T})$ while the false alarm probability is α. Now given the incorrect tag, the detection probability is simply α. Thus the unconditional authentication probability is

$$P^a = (P^a|\hat{\mathbf{T}} = \mathbf{T}) * P + \alpha * (1 - P) \tag{48}$$

## 3 Properties of the Authentication System

We now discuss the stealth and robustness of the authentication system. We will then qualitatively and quantitatively give heuristics for system design.

In the simulations, we assume $N = 32$ carriers, of which $N^s = 28$ are message carriers and $N^n = 4$ are null carriers. Each frame consists of $N^f = 8$ OFDM symbols, for a total of $8 * 28 = 224$ message symbols (and 32 null symbols).
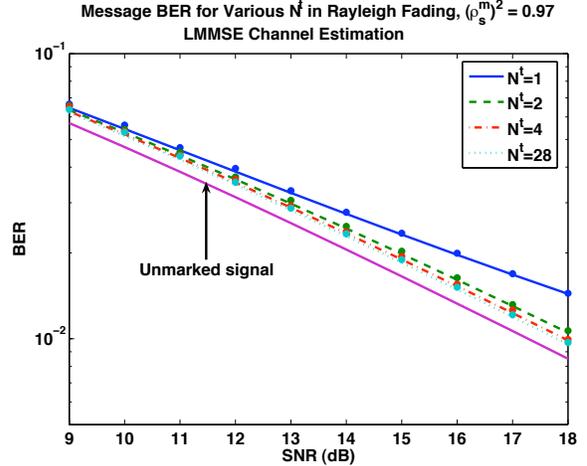
3.1 Stealth

The stealth of the system is measured by the inability of the adversary to distinguish between signals containing authentication information and signals that do not. Many statistics of the observation can be measured and compared against the statistics of the reference signal (the signal that contains messages only, i.e., $\rho_t = 0$).

A straightforward comparison is between the bit error probabilities of the observation with that of the reference
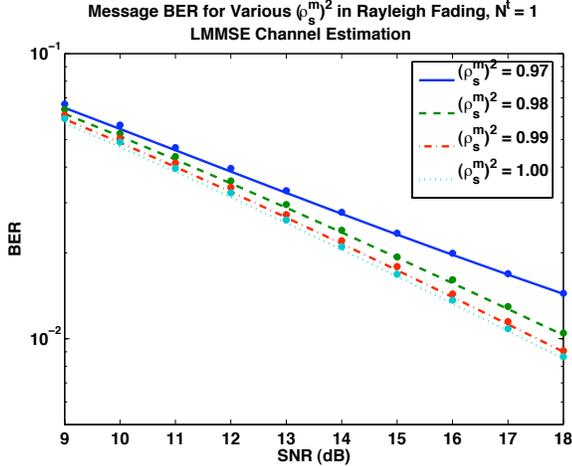
Figure 3. Stealth is improved with more message power (higher ρ_s).

Figure 4. Stealth is improved with more scattered tag placement (higher N^t).

system. We compare the uncoded bit error probabilities. That is, $f_e(\cdot)$ and $f_d(\cdot)$ only modulate and demodulate the symbols, respectively. In our simulation, $f_e(\cdot)$ is a 4-QAM mapper while $f_d(\cdot)$ is the corresponding demapper.

In Figure 3 we compare the BER of the tagged and untagged signals for various power allocations $(\rho_s)^2$. The theoretical BER curves are indicated by the lines; the simulation results are indicated by the hash marks. This figure verifies the validity of equations (36) and (37). Not surprisingly, the more power that is allocated to the message symbols, the lower the message BER.

Now we fix the power allocation $(\rho_s)^2$ to observe the effects of N^t. In Figure 4 we see that decreasing N^t increases the message BER. It is perhaps counter-intuitive to note that decreasing the number of tag symbols actually increases the overall message BER. However, note that by decreasing N^t, the tag power is more concentrated in fewer symbols, thereby increasing the interference to the underlying message symbol. While many tag symbols each with low power may avoid causing errors to the message, a few high powered tag symbols probably will.

3.2 Robustness

The robustness of the system is measured by the ability of the intended receiver (Bob) to authenticate Alice while rejecting signals without the proper tags. Equation (46) gives the probability of authentication under ideal conditions: perfect channel estimation and zero frequency offset.

In Figure 5 the probability of authentication is compared for various message powers. As the message power $(\rho_s)^2$ decreases, there is more power available to signal the authentication tags. The figure confirms the intuition that in-

creasing the tag power increases the authentication probability.

Now we fix the power allocation $(\rho_s)^2$ to observe the effects of N^t. In Figure 6 we see that increasing N^t increases the probability of authentication. As with stealth, this may be counter-intuitive because the tag power is fixed. However, the answer lies in the frequency selectivity of the channel: a tag that utilizes more carriers has more resistance to deep fades.

The above discussion assumed that the authentication tag is always generated without error at the receiver. Let us now consider the tradeoff between the robustness of the authentication and the message rate. In Figure 7 we see that the more powerful the message coding, the better the probability of detection. Of course, this decreases the rate of the message. Note that since all systems have some coding to ensure accurate recovery of the message, the authentication does not impose any stricter requirements on the system.

4 Tradeoffs

The parameters of a multi-carrier authentication system are the power allocation $(\rho_s)^2$ and the fraction of tag symbols N^t. We see from Section 3 that increasing N^t improves both properties simultaneously (Figures 4 and 6). Thus the best strategy is to set $N^t = N^s$.

When the message power is decreased, the stealth of the system increases (Figure 3) while the robustness decreases (Figure 5). Thus there is a fundamental tradeoff between the power of the authentication and its reliability. Note that we constrain the power of the authentication tag, but not the energy. That is, we can extend the length of the tag in time
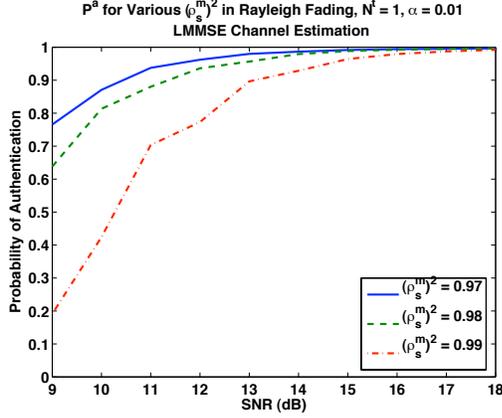
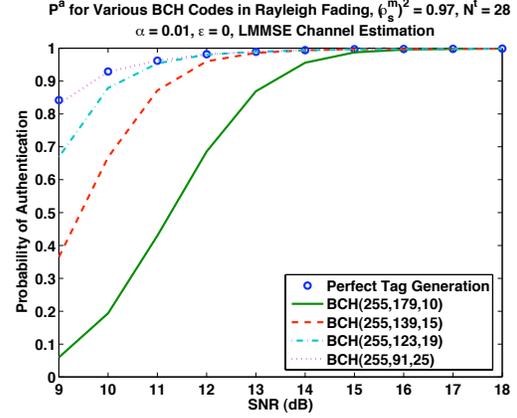**Figure 5. Robustness is improved with less message power (lower ρ_s).**
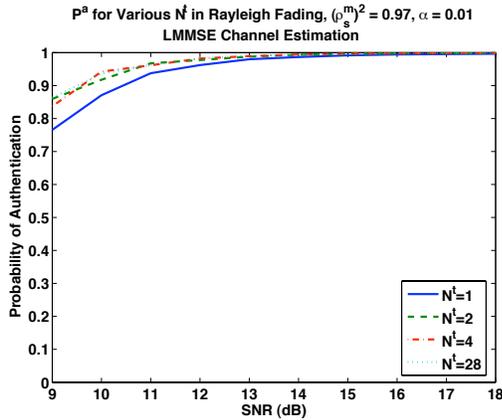

Figure 6. Robustness is improved with more scattered tag placement (higher N^t).

and thus increase the robustness of the detection [4].

The more important property is stealth, because without it the messages cannot be recovered. Therefore the parameters should first satisfy the stealth requirements. Each requirement (e.g. BER below x, probability of authentication above y) maps to a set of values for $(\rho_s)^2$ and N^t. As long as the intersection is non-empty, the requirements are jointly satisfiable.

5   Conclusion

A flexible framework for designing multi-carrier physical layer authentication systems is presented. By constraining the allocation of power between message and authentication tag, the authentication can be made simultaneously stealthy and robust. Rather than concentrating the energy in

Figure 7. Robustness: the authentication probability increases with stronger codes.

a few high powered few carriers, it is better to use many low powered carriers to improve stealth and robustness. This finding indicates the main benefit of multi-carrier authentication systems: improved stealth and robustness with no increase in power.

This work has many interesting potential applications for cross-layer security designs. In conjunction with higher layer mechanisms, this method allows nodes to make low-complexity but high quality authentication decisions. Since it is a physical layer technique, no changes need to be made at the higher layers, nor is any data bandwidth taken to explicitly signal any authentication information. In contrast, typical authentication mechanisms time multiplex authentication tags with data.

References

[1] O. Edfors, M. Sandell, J.-J. van de Beek, S. K. Wilson, and P. O. Borjesson. OFDM channel estimation by singular value decomposition. *IEEE Trans. Commun.*, 46(7):931–939, July 1998.

[2] J. L. Massey. Shift-register synthesis and BCH decoding. *IEEE Trans. Inf. Theory*, 15(1):122–127, Jan. 1969.

[3] P. K. Vitthaladevuni and M.-S. Alouini. A recursive algorithm for the exact ber computation of generalized hierarchical qam constellations. *IEEE Trans. Inf. Theory*, 49(1):297–3073, Jan. 2003.

[4] P. Yu, J. S. Baras, and B. M. Sadler. Physical layer authentication. *IEEE Trans. Inf. Forensics Security*, 3(1):38–51, Mar. 2008.