POWER ALLOCATION TRADEOFFS IN MULTICARRIER AUTHENTICATION SYSTEMS

P. L. Yu*, J. S. Baras
University of Maryland
College Park, MD 20742

B. M. Sadler
Army Research Laboratory
Adelphi, MD 20783

***Abstract*—Physical layer authentication techniques exploit signal characteristics to uniquely identify radios. We describe how multicarrier systems may use such techniques to stealthily authenticate while maintaining high levels of security and robustness. We show that with channel state information (CSI) at the transmitter and receiver, multicarrier authentication systems can further improve performance by carefully allocating the authentication power each carrier.**

I. Introduction

Physical layer authentication systems have been shown to be stealthy, robust, and secure [1] in single carrier systems. In this paper we consider extensions to multicarrier systems to improve these properties [2]. In particular, we show that with channel state information at the transmitter and receiver, multicarrier authentication systems can further improve performance by carefully allocating the authentication power over each carrier.

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

II. System Framework

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 a) observe what Alice is transmitting and b) transmit arbitrary messages to Bob.

Alice transmits messages to Bob in plain view: Eve can also recover the messages. In addition, Alice superimposes tags with messages for authentication. Bob authenticates Alice only when he detects the correct tags in the received signal. In the next section we describe how the messages and tags are created in a multi-carrier setting.

A note on notation: Bold face indicates matrices (e.g. $\mathbf{A}$). Upper case indicates signals in the frequency domain (e.g. $\mathbf{H}$). Lower case indicates in the time domain (e.g. $\mathbf{h}$).

A. Signal Model

Suppose that Alice and Bob communicate using multiple carriers. In general, some carriers will be nulled out for spectral shaping purposes, but this does not have a significant impact on the authentication framework. Therefore we ignore the null carriers and assume that there are $N > 1$ message carriers.

The signals are transmitted in frames represented by size $N \times N^f$ matrices where N^f is the frame length. We assume the signals are i.i.d. and do not use time indices. Denote the transmitted signal by the matrix $\mathbf{X}$ with complex entries $\{X(m,n)\}$ that have variance σ_x^2. We constrain the energy as given by its Frobenius norm

$$|\mathbf{X}|^2 = \text{Trace}(\mathbf{X}^H\mathbf{X}) \quad (1)$$

$$E|\mathbf{X}|^2 = NN^f\sigma_x^2 \quad (2)$$

First we consider **untagged** signals which are message-only (no tags). The transmitted signal is

$$\mathbf{X} = \rho\mathbf{S} \quad (3)$$

where ρ is a $N \times N$ diagonal scaling matrix and $\mathbf{S}$ is a $N \times N^f$ message matrix satisfying

$$E[S(m,n)] = 0 \quad (4)$$

$$E[|S(m,n)|^2] = \sigma_x^2 \quad (5)$$

$$\sum_{m,n} I(S(m,n)) = NN^f \quad (6)$$

where $I(\cdot)$ is the indicator function. That is, the message symbols have zero mean and variance σ_x^2, and they occupy each of the NN^f symbol positions in the frame. The term ρ is used to allocate power among the carriers such that equations (2) and (3) are satisfied.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 DEC 2008	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Power Allocation Tradeoffs In Multicarrier Authentication Systems	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **University of Maryland College Park, MD 20742**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM002187. Proceedings of the Army Science Conference (26th) Held in Orlando, Florida on 1-4 December 2008, The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**8**	

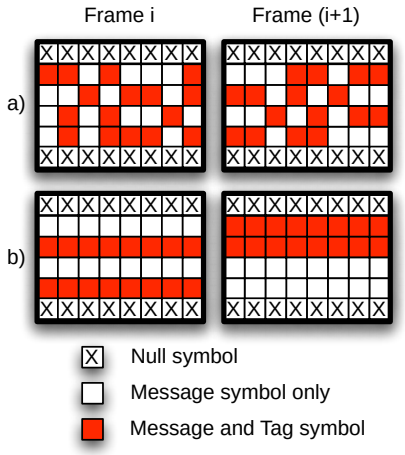

Fig. 1. Example tag placements with $N = 4, N^f = 8$ and tag spread $N^t = 2$. a) tag on specific carriers only, b) general tag placement.

The **tagged** signals are formed by superimposing the authentication tag $\mathbf{T}$ with the message $\mathbf{S}$:

$$\mathbf{X} = \rho^s \mathbf{S} + \rho^t \mathbf{T} \tag{7}$$

where ρ^s, ρ^t are scaling matrices and $\mathbf{T}$ satisfies

$$E[T(m,n)] = 0 \tag{8}$$

$$E[|T(m,n)|^2] = \begin{cases} 0 & T(m,n) \text{ is absent} \\ \sigma_x^2 & T(m,n) \text{ is present} \end{cases} \tag{9}$$

$$\sum_{m,n} I(T(m,n)) = N^t N^f \tag{10}$$

Note that the tag symbols occupy $N^t N^f$ out of a possible $N N^f$ symbol positions with $0 \le N^t \le N$. When present, each tag symbol has zero mean and variance σ_x^2. In general N^t is not restricted to be a natural number, but doing so admits the natural interpretation of N^t as the number of carriers that are used to signal the authentication (Figure 1b). In general, N^t specifies the **spread** of the tag across the symbols; a large N^t indicates that the tag is very spread out over many symbols while a small N^t indicates that the tag is concentrated over only a few symbols. Figure 1a is an example of how the tags are not confined to specific carriers.

Denote the k^{th} row of a matrix by $(\cdot)_k$. For diagonal matrices such as ρ we slightly abuse the notation to write $\rho_k = \rho(k,k)$. The terms ρ^s, ρ^t are chosen to normalize the energy of tagged and untagged signals:

$$E|\rho \mathbf{S}_k|^2 = E|\rho_k^s \mathbf{S}_k + \rho_k^t \mathbf{T}_k|^2 \tag{11}$$

where

We assume that the message and tag are uncorrelated

$$E[\text{Trace}(\mathbf{S}^H \mathbf{T})] = 0 \tag{12}$$

so that the power constraint becomes

$$\rho_k^2 = (\rho_k^s)^2 + \frac{E|\mathbf{T}_k|^2}{E|\mathbf{S}_k|^2}(\rho_k^t)^2 \tag{13}$$

Since N^s, N^t are fixed system parameters, specifying ρ^s determines ρ^t and vice versa. Note that $|\rho^s|^2$ (resp. $|\rho^t|^2$) is simply the overall percentage of power allocated to the message (resp. tag) symbols. The untagged signal is a special case of the tagged signal where $\rho^s = \rho$ and $\rho^t = \mathbf{0}$. We thus use the more general formulation of equation (7) to represent both tagged and untagged signals.

Alice wants to send the message $\mathbf{B}$ to Bob. They also share a secret key $k \in \mathcal{K}$, where $|\mathcal{K}| = K$, that is used to generate the authentication tag from the message. The signals and tags are generated as follows

$$\mathbf{S} = f_e(\mathbf{B}) \tag{14}$$

$$\mathbf{T} = g(\mathbf{B}, k) \tag{15}$$

The encoding function $f_e(\cdot)$ encapsulates any coding, modulation, or pulse shaping that may be used. The corresponding decoding function $f_d(\cdot)$ is used at the receiver and satisfies

$$\mathbf{B} = f_d(f_e(\mathbf{B})) \tag{16}$$

for all possible inputs $\mathbf{B}$ of $f_e(\cdot)$. 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-Hocqueneghem (BCH) can be efficiently decoded using Berlekamp-Massey algorithm [3].

The tag generating function $g(\cdot)$ is assumed to be one-way, i.e., it is easy[1] to calculate $\mathbf{T}$ given $\mathbf{B}$ and k, but hard to find k given $\mathbf{T}$ and $\mathbf{B}$. Further, it is collision resistant so that it is hard to find $\mathbf{X} \neq \mathbf{Y}$ such that $g(\mathbf{X}, k) = g(\mathbf{Y}, k)$.

The transmitted (time domain) signal $\mathbf{x}$ is obtained by taking the IDFT of $\mathbf{X}$

$$\mathbf{x} = \text{IDFT}[\mathbf{X}] \tag{17}$$

$$= \mathbf{F}^H \mathbf{X} \tag{18}$$

where $\mathbf{F}$ is the unitary $N \times N$ FFT matrix with entries

$$F(m,n) = \frac{1}{\sqrt{N}} \exp(-j2\pi mn/N) \tag{19}$$

and $0 \le m, n \le N-1$.

B. Channel Model and Estimation

We assume a block fading multipath channel: $\vec{\mathbf{h}}$ is a length L column vector that is constant over a frame of symbols. The channel is modeled as a delay line with equally spaced taps

$$\vec{h}(m) = \sum_{l=0}^{L-1} \alpha(l) \delta(m-l) \tag{20}$$

[1]The concept of *easy* and *hard* calculations can be characterized by their feasibility. Hard calculations are infeasible to compute given constraints on computational resources, while easy calculations are feasible to compute under the same constraints.

where $\alpha(\cdot)$ are i.i.d. complex zero-mean Gaussian random variables with variance N/L. The frequency response of the channel is

$$\mathbf{H} = \text{diag}(\mathbf{F}\vec{\mathbf{h}}) \quad (21)$$

where $\vec{\mathbf{h}}$ is zero-padded to N, the length of the FFT. The operator $\text{diag}(\vec{\mathbf{x}})$ returns the diagonal matrix with (vector) $\vec{\mathbf{x}}$ on the main diagonal. Note that the frequency response per carrier has unit expected variance ($\sigma_h^2 = 1$).

Suppose that Alice and Bob have channel state information (CSI), i.e., prior to transmission Alice knows $\mathbf{H}$ and for each observed block Bob has $\hat{\mathbf{H}} = \mathbf{H}$. Using the channel estimate, the receiver estimates the message signal as

$$\hat{X}(k) = \frac{\hat{H}^*(k)}{|\hat{H}(k)|^2} Y(k) \quad (22)$$

$$= X(k) + \frac{W(k)}{\hat{H}(k)} \quad (23)$$

The estimated message is

$$\hat{\mathbf{B}} = f_d(\hat{\mathbf{X}}) \quad (24)$$

where $f_d(\cdot)$ is the decoding function corresponding to the encoder $f_e(\cdot)$ from equation (15).

C. Tag Detection

With his estimate of the data $\hat{\mathbf{B}}$, Bob uses $g(\cdot)$ from equation (15) to reconstruct the estimated tag:

$$\hat{\mathbf{T}} = g(\hat{\mathbf{B}}, k) \quad (25)$$

Bob uses matched filtering to detect it in his observation $\mathbf{Y}$. He calculates the residual $\mathbf{R}$ by removing the message and then correlates it with the estimated tag to obtain the test statistic τ.

$$\mathbf{R} = \mathbf{Y} - \hat{\mathbf{H}}\rho^s f_e(\hat{\mathbf{B}}) \quad (26)$$

$$\tau = \Re(\text{tr}((\rho^t \hat{\mathbf{H}}\hat{\mathbf{T}})^H \mathbf{R})) \quad (27)$$

The receiver performs a hypothesis test with hypotheses

$$H_0: \quad \hat{\mathbf{T}} \text{ is not present in } \mathbf{R} \quad (28)$$

$$H_1: \quad \hat{\mathbf{T}} \text{ is present in } \mathbf{R} \quad (29)$$

The decision of authenticity δ is made according to

$$\delta = \begin{cases} 0 & \tau < \tau^0 \\ 1 & \tau \geq \tau^0 \end{cases} \quad (30)$$

The threshold τ^0 of this test is determined for a false alarm probability α according to the distribution of $(\tau|H_0)$. As in the single carrier case, the authentication is low-complexity because the required tag generation and correlation are simple operations.

1) False Alarm Probability: In order to limit the false alarm probability α, we calculate the threshold τ^0 such that $P(\tau > \tau^0|H_0) \leq \alpha$. There are two main cases where a false alarm can occur: when the observation contains no tag at all or when the observation contains an incorrect tag.

We assume that the message is recovered without error because that is when authentication is useful. That is, $\hat{\mathbf{B}} = \mathbf{B}$. Consider the structure of the residual $\mathbf{R}$

$$\mathbf{R} = \mathbf{HX} + \mathbf{W} - \rho^s \mathbf{HS} \quad (31)$$

$$= \mathbf{H}(\mathbf{X} - \rho^s \mathbf{S}) + \mathbf{W} \quad (32)$$

where σ_w^2 is the noise variance.

Case 1: the transmitted signal does not contain any tag (i.e., $\mathbf{X} = \rho\mathbf{S}$). Then

$$\tau|H_0 = \Re(\text{tr}((\rho^t \mathbf{H}\hat{\mathbf{T}})^H \mathbf{R})) \quad (33)$$

$$= \Re\left(\text{tr}((\rho^t \mathbf{H}\hat{\mathbf{T}})^H ((\rho - \rho^s)\mathbf{HS} + \mathbf{W}))\right) \quad (34)$$

$$= \Re\left(\text{tr}(\rho^t(\rho - \rho^s)(\mathbf{H}^H\mathbf{H})\hat{\mathbf{T}}^H\mathbf{S})\right) + v \quad (35)$$

where v is a real Gaussian variable with zero mean and variance $\sigma_v^2 = |\rho^t|^2|\mathbf{H}|^2|\hat{\mathbf{T}}|^2\sigma_w^2$.

Consider the term $\Re(\text{tr}(\hat{\mathbf{T}}^H\mathbf{S}))$. It is a sum of N^tN^f i.i.d. variables and is well approximated by a Gaussian distribution when N^tN^f is large (central limit theorem). The mean is zero (12) and the variance depends on the symbol constellations. For example, if the message and tag are composed of QPSK symbols, the variance of $\Re(\text{tr}(\hat{\mathbf{T}}^H\mathbf{S}))$ is $\sigma_{ts}^2 = N^tN^f * \frac{1}{4}(1+1+0+0) = \frac{N^tN^f}{2}$. Thus the test statistic τ is Gaussian with zero mean and variance

$$\sigma_\tau^2 = |\rho^t|^2|\rho - \rho^s|^2|\hat{\mathbf{H}}|^4\sigma_{ts}^2 + \sigma_v^2 \quad (36)$$

Case 2: the transmitted signal contains a tag different from estimated tag (i.e., $\mathbf{T} \neq \hat{\mathbf{T}}$). Then

$$\tau|H_0 = \Re(\text{tr}((\rho^t \mathbf{H}\hat{\mathbf{T}})^H \mathbf{R})) \quad (37)$$

$$= \Re(\text{tr}((\rho^t \mathbf{H}\hat{\mathbf{T}})^H (\rho^t \mathbf{HT} + \mathbf{W})) \quad (38)$$

$$= \Re(\text{tr}((\rho^t)^2(\mathbf{H}^H\mathbf{H})\hat{\mathbf{T}}^H\mathbf{T})) + v \quad (39)$$

where v is defined as in case 1.

Consider the term $\Re(\text{tr}(\hat{\mathbf{T}}^H\mathbf{T}))$. It is a sum of N^tN^f i.i.d. variables and is well approximated by a Gaussian distribution when N^tN^f is large (central limit theorem). The mean is zero (12) and the variance depends on the symbol constellations. For example, if the tag is composed of QPSK symbols, the variance of $\Re(\text{tr}(\hat{\mathbf{T}}^H\mathbf{S}))$ is $\sigma_{ts}^2 = N^tN^f * \frac{1}{4}(1+1+0+0) = \frac{N^tN^f}{2}$. Thus the test statistic τ is Gaussian with zero mean and variance

$$\sigma_\tau^2 = |\rho^t|^4|\mathbf{H}|^4\sigma_{ts}^2 + \sigma_v^2 \quad (40)$$

Without priors that indicate which case is applicable, the threshold is calculated based on the worst case distribution from either case 1 or 2. Since both are zero mean Gaussian distributions, the worst case has the larger variance σ_τ^2 from equations (36) and (40).

$$\tau^0 = \arg\min_\tau \Phi(\tau/\sigma_\tau) \geq 1 - \alpha \tag{41}$$

where $\Phi(\cdot)$ is the standard Gaussian cumulative distribution function.

2) Detection Probability: When Bob generates the correct tag ($\hat{\mathbf{T}} = \mathbf{T}$), the test statistic is

$$\begin{aligned} \tau|H_1 &= \Re(\mathrm{tr}((\rho^t \mathbf{H}\hat{\mathbf{T}})^H \mathbf{R})) && (42)\\ &= \Re(\mathrm{tr}((\rho^t)^2 (\mathbf{H}^H\mathbf{H})\mathbf{T}^H\mathbf{T})) + v && (43)\\ &= |\rho^t \mathbf{H}\mathbf{T}|^2 + v && (44) \end{aligned}$$

The probability of detection is

$$P^a(\gamma) = 1 - \Phi\left(\frac{\tau^0 - |\rho^t \mathbf{H}\mathbf{T}|^2}{\sigma_v}\right) \tag{45}$$

III. Power Allocation Strategies

Since that Alice and Bob have channel state information, the Alice can vary the power loading across carriers to improve the rate of the message or tag. It is well known that the water-filling power allocation maximizes the message rate for parallel Gaussian channels [4]. When no authentication tag is transmitted, the optimal power allocation is given by

$$\begin{aligned} P_k &= (\nu - N_k)^+ && (46)\\ 1 = P &= \sum_k (\nu - N_k)^+ && (47) \end{aligned}$$

where $P_k = \rho(k,k)^2$, $P = |\rho|^2$ and $N_k = \sigma_w^2/|H(k,k)|^2$. We assume that ρ is given and that the allocations ρ^s, ρ^t satisfy equation (13), i.e., the total power per carrier for tagged and untagged signals is equal. We require this for stealth purposes: if the power spectrum of the signal is different it is easy for the adversary to detect the anomaly.

For brevity in the sequel, we denote the per-carrier powers by $P_k^s = \rho^s(k,k)^2, P_k^t = \rho^t(k,k)^2$ and the total power constraints by $P^s = |\rho^s|^2, P^t = |\rho^t|^2$.

In the authentication system, we transmit message and tags simultaneously, so the question becomes how to best allocate the power between message and tag on a per-carrier basis given P^s and P^t (the percentage of power used for the message and tag).

A. Strategies

The water-filling allocation given above maximizes the message rate of the system when no tag is transmitted. We consider four power allocation strategies that are easy to implement (Figure 2). Their relative merits are discussed in the next section.

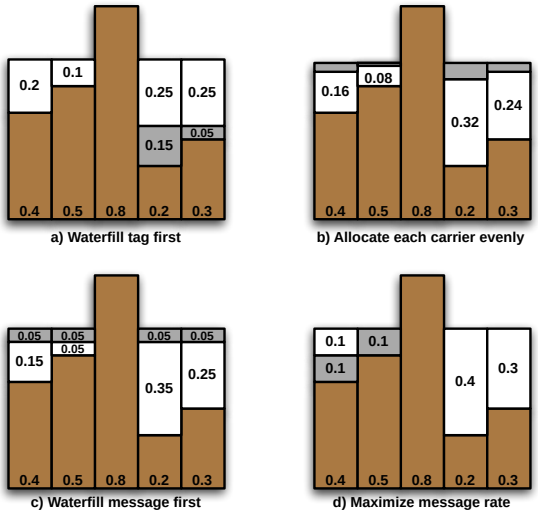

Fig. 2. Power allocation strategies. Base bars represent noise power on the carriers, white bars represent message power, and lightly shaded bars represent tag power. Power allocation is 80% message and 20% tag ($P^s = 0.8, P^t = 0.2$).

By design, each of the power allocation strategies yields the same signal power per carrier as the untagged signal. This is done for stealth purposes: an abnormal power spectrum can be easily detected and flagged as anomalous by adversaries.

1) Waterfill Tag, then Message: First, allocate the tag powers P_k^t by water-filling with the power budget P^t.

$$\begin{aligned} P_k^t &= (\nu_t - N_k)^+ && (48)\\ P^t &= \sum_k (\nu_t - N_k)^+ && (49) \end{aligned}$$

Then, treating the tag power as noise, allocate the message powers P_k^s by water-filling with the power budget P^s.

$$\begin{aligned} P_k^s &= (\nu_s - N_k - P_k^t)^+ && (50)\\ P^s &= \sum_k (\nu_s - N_k - P_k^t)^+ && (51) \end{aligned}$$

This strategy is shown in Figure 2a. In this case, the message always occupies at least as many carriers as the tag.

2) Evenly allocate: First we determine the signal powers P_k that will used on each carrier using the total power budget P by using equations (46) and (47). Then, using the message and tag power allocations (P^s, P^t, respectively) we calculate the message and tag powers per carrier

$$\begin{aligned} P_k^s &= P^s P_k && (52)\\ P_k^t &= P^t P_k && (53) \end{aligned}$$

This strategy is shown in Figure 2b. The proportion of message to tag power is identical for each carrier with non-zero signal power. In this case, the message always occupies the same carriers as the tag.

3) Waterfill Message, then Tag: First, allocate the message powers P_k^s with the power budget P^s.

$$\begin{aligned} P_k^s &= (\nu_s - N_k)^+ && (54)\\ P^s &= \sum_k (\nu_s - N_k)^+ && (55)\end{aligned}$$

Then, treating the message power as noise, allocate the tag powers P_k^t with the power budget P^t.

$$\begin{aligned} P_k^t &= (\nu_t - N_k - P_k^s)^+ && (56)\\ P^t &= \sum_k (\nu_t - N_k - P_k^s)^+ && (57)\end{aligned}$$

This strategy is shown in Figure 2c. In this case, the tag always occupies at least as many carriers as the message.

4) Maximization of Message Rate: Consider the message capacity of the k^{th} carrier. With the message and tag allocations P_k^s and P_k^t, it is

$$C_k^s = \frac{1}{2}\log\left(1 + \frac{P_k^s}{N_k + P_k^t}\right) \quad (58)$$

Note that the tag acts as additional noise to the message. With the water-filling allocation (46), we may simplify this equation to

$$C_k^s = \begin{cases} \frac{1}{2}\log\left(\frac{\nu}{N_k + P_k^t}\right) & P_k^s > 0 \\ 0 & \text{otherwise} \end{cases} \quad (59)$$

Suppose we wish to allocate power across carriers such that the message rate is maximized. From (59) is clear that carriers with zero message power have no contribution to the capacity. Thus we remove the carriers with $P_k^s = 0$ from consideration, and for brevity write $\sum_k$ to mean $\sum_{k|P_k^s>0}$.

The constrained optimization problem is

$$\max_{\mathbf{P^t}} \sum_k C_k^s \quad (60)$$

with the constraints

$$\begin{aligned} \sum_k P_k^t &= P^t = 1 - ||\rho^s||^2 && (61)\\ P_k^t &\geq 0, \forall k && (62)\\ P_k^t &\leq P_k, \forall k && (63)\end{aligned}$$

We use the Lagrange method to solve the problem. The objective function is

$$\begin{aligned} J(\mathbf{P^t}) &= \sum_k C_k^s \\ &\quad +\lambda(P^t - \sum_k P_k^t) \\ &\quad +\sum_k \mu_k^- P_k^t \\ &\quad +\sum_k \mu_k^+(\nu - (N_k + P_k^t)) \quad (64)\end{aligned}$$

Since the cost function is concave and each constraint is linear, the KKT conditions are necessary and sufficient to solve the problem. The KKT conditions are

$$\begin{aligned} \frac{\partial J(\mathbf{P^t})}{\partial P_k^t} &= 0, \forall k && (65)\\ \lambda(P^t - \sum_k P_k^t) &= 0, \lambda \geq 0 && (66)\\ \mu_k^- P_k^t &= 0, \mu_k^- \geq 0, \forall k && (67)\\ \mu_k^+(\nu - (N_k + P_k^t)) &= 0, \mu_k^+ \geq 0, \forall k && (68)\end{aligned}$$

Setting the derivative to zero (65), we have

$$-\frac{1}{2}\frac{1}{N_k + P_k^t} + \mu_k^- - \mu_k^+ = \lambda \quad (69)$$

Case 1: $P_k^t = 0$. Then $\mu_k^- > 0, \mu_k^+ = 0$

$$-\frac{1}{2}\frac{1}{N_k} + \mu_k^- = \lambda \quad (70)$$

Case 2: $0 < P_k^t < \nu - N_k$. Then $\mu_k^- = 0, \mu_k^+ = 0$

$$-\frac{1}{2}\frac{1}{N_k + P_k^t} = \lambda \quad (71)$$

Case 3: $P_k^t = \nu - N_k$. Then $\mu_k^- = 0, \mu_k^+ > 0$

$$-\frac{1}{2}\frac{1}{\nu} - \mu_k^+ = \lambda \quad (72)$$

Ambiguities remain since there are multiple power allocations that will satisfy the above equations. To proceed further we use the following lemma. This lemma indicates that to maximize the total capacity of two independent channels, it is better to add any interference in the noisier of two channels.

Lemma 1: For $\Delta > 0$,

$$\begin{aligned} &\frac{1}{2}\left[\log\left(\frac{\nu}{N_1 + \Delta}\right) + \log\left(\frac{\nu}{N_2}\right)\right] \\ &> \frac{1}{2}\left[\log\left(\frac{\nu}{N_1}\right) + \log\left(\frac{\nu}{N_2 + \Delta}\right)\right]\end{aligned}$$

TABLE I
SIMULATION PARAMETERS FOR THE MULTI-CARRIER, PERFECT CSI CASE

Channel Model	Rayleigh block fading
Noise Model	AWGN
# Carriers	32 (4 taps)
Channel State Information?	Yes
Modulation	BPSK: SNR $\leq$ 7dB 4-QAM: SNR $>$ 7 dB 16-QAM: SNR $>$ 12 dB 64-QAM: SNR $>$ 17 dB
Channel Estimate Method	Known
# Pilot Symbols	1 OFDM symbol per frame
Frame Length	4 OFDM symbols
False Alarm Probability	10^{-7}
# Monte Carlo Samples	2^{14}

if and only if $N_1 > N_2$.

Together with the KKT conditions, it is clear that the optimal strategy places the tag power in the carriers with the highest noise levels. The sum power of the tags are distributed in cases 2 and 3. With the lemma, only a single carrier can satisfy case 2. The other carriers are either dedicated to message or tag. It is easy to check that the following algorithm yields an optimal solution (it may not be unique):

1) Define (descending) order statistics $t_1, \ldots, t_K$ such that $N_{(t_1)} \geq N_{(t_2)} \geq \cdots \geq N_{(t_K)}$
2) Initialize $k = \arg[\min_l(\nu - N_{(t_l)}) > 0]$.
3) While $k \leq K$
   - $P^t_{(t_k)} = \min\left(\left(T - \sum_{l<k} P^t_{(t_l)}\right)^+, \nu - N_{(t_k)}\right)$
   - k = k+1

This strategy is shown in Figure 2d. The algorithm greedily places the tag power in the carriers with the highest noise until there is not enough power to entirely occupy any of the remaining carriers. At that point, the remaining tag power is placed in the next noisiest carrier. Note that in this strategy, at most one carrier is used to signal both message and tag.

IV. METRIC EVALUATION

We perform a Monte Carlo simulation with the parameters in Table I.

A. Stealth

The stealth of the authentication system can be measured by its message throughput and by its BER. We consider each in turn.

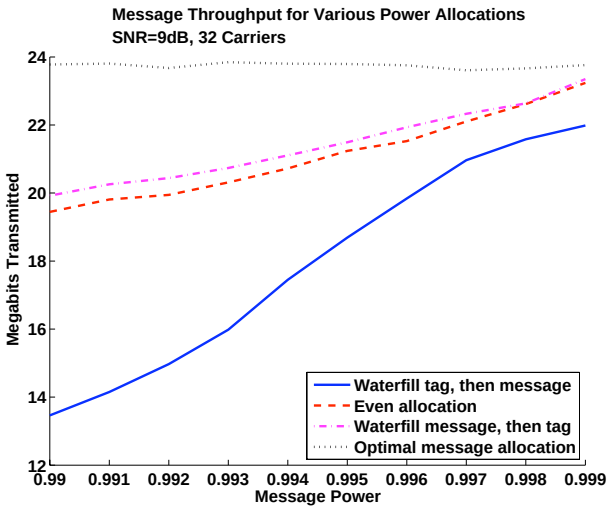

Fig. 3. Throughput for various strategies. Frame length = 32 symbols. Average SNR = 9 dB.

Throughput

The message throughput for various policies is shown in Figure 3. The throughput using strategy 4 (the optimal message allocation) is consistently high when the message power is high (P^s close to $P = 1$). The other strategies are more noticeably affected by the decrease in message power. However, the throughputs are not affected in the same way.

Strategies 2 and 3 offer reasonably high throughputs when the message power is high. There is little difference between the two, though Strategy 2 is marginally better.

Finally, strategy 1 has the lowest throughput of the four power allocation strategies. By signaling the tag over the highest SNR carriers, the effective message is lowered, thus having a substantial impact on throughput when P^s is not very close to $P = 1$.

Message BER

When the authentication tag is present, power is necessarily allocated away from the message, and hence the message BER increases. The impact of the authentication tag varies depending on the power allocation strategy.

Figure 4 shows the increase in BER for various strategies. The BER is the least affected when the message power is near 1. Of the strategies, the optimal message allocation has the best stealth: the BER is the least impacted for all message powers.

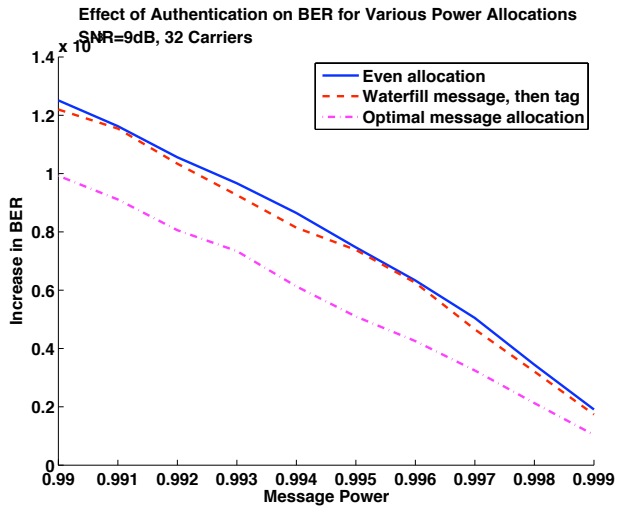

Fig. 4. Stealth for various strategies. Frame length = 32 symbols. Average SNR = 9 dB.

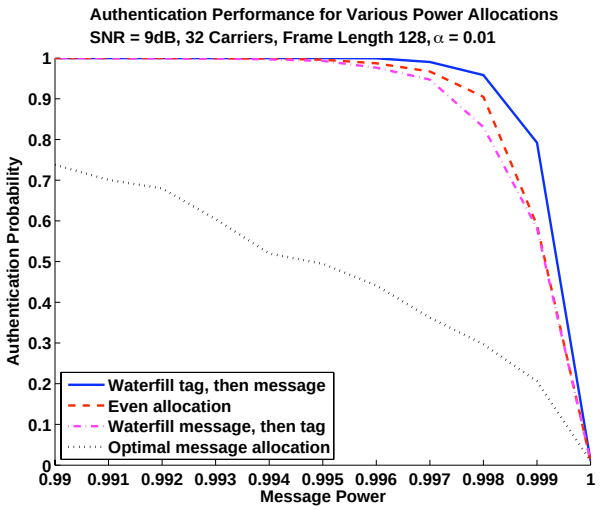

Fig. 5. Robustness for various strategies. Frame length = 32 symbols. Average SNR = 9 dB. False alarm probability $\alpha = 0.01$.

B. Robustness

The robustness of the authentication system is given by its probability of authentication for a given false alarm probability. We compare the effect of frame lengths as well as the effect of various power allocation strategies.

Figure 5 shows that the choice of policy can greatly impact the robustness of the authentication system. The best performing strategy is to allocate water-fill the tag first before water-filling the message. Strategies 1-3 have approximately equal performance, but strategy 4 performs much worse.

Since strategy 4 places the tag at the lowest SNR carriers, the tag detection does not receive much benefit from any frequency diversity. The tags are placed in the highest noise regions by design in order to maximize the message throughput, and as a result the authentication performance suffers.

C. Security

The stealth of the authentication system is given by the tag equivocation of the unaware or adversarial receiver. When the tag is observed through a noisy channel, it leads to positive key equivocation. Suppose that the authentication tag is composed of M bits. For example, with $N_t = 32$ and $N^f = 4$ there are 128 symbols. With binary signaling there are $M = 256$ bits.

The equivocation of the authentication tag depends on the bit error rate that it is observed with. Suppose that the authentication tag $\mathbf{T}$ is composed of M bits and is observed with i.i.d. bit errors with probability p^t. We can calculate the tag equivocation $H(\mathbf{T}|p^t)$ by iterating through the number of bit errors the tags can contain (between 0 and M). The probability of observing n errors in a length M tag with bit error probability p^t is

$$Pr(p^t, n, M) = (p^t)^n (1 - p^t)^{M-n} \tag{73}$$

Since tags with the same number of i.i.d. bit errors have the same probability of occurring (and there are $\binom{M}{n}$ length M tags with n errors), the tag equivocation is

$$H(\mathbf{T}|p^t) = \sum_{T \in \mathcal{T}} Pr(\mathbf{T} = T|p^t) \frac{1}{Pr(\mathbf{T} = T|p^t)} \tag{74}$$

$$= \sum_{n=0}^{M} \binom{M}{n} Pr(p^t, n, M) \log_2 \frac{1}{Pr(p^t, n, M)} \tag{75}$$

where $Pr(\cdot, \cdot, \cdot)$ is defined above in equation (73).

We compare the equivocation for the policies as shown in Figure 6. Clearly the power allocation that maximizes message capacity also maximizes the tag equivocation among the policies. However, from the previous section we see that this allocation also performs the worst in terms of authentication robustness. The remaining two policies result in very similar equivocation, demonstrating that proportionally allocating power between message and authentication is a reasonable strategy with little tradeoff. As before, higher SNR situations reduce the tag equivocation.

V. Conclusion

We have extended the physical layer authentication framework [1] to multicarrier systems and have shown how to stealthily authenticate while maintaining high levels of security and robustness. When channel state information is

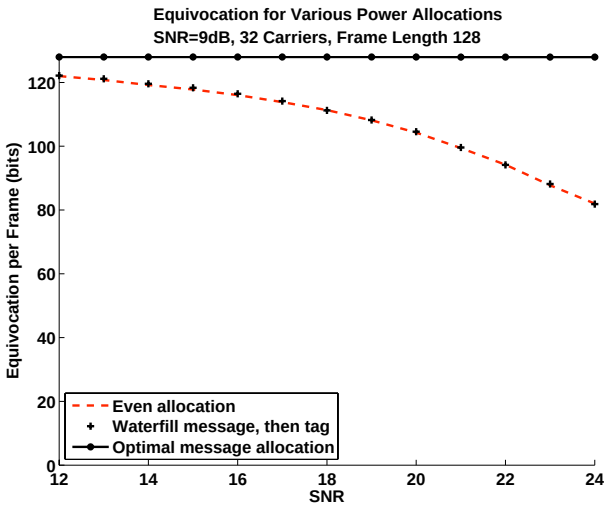

Fig. 6. Tag equivocation for various strategies. Frame length = 32 symbols. Average SNR = 9 dB. False alarm probability $\alpha = 0.01$.

known to the transmitter, we demonstrated that the allocation of the tag power plays a very important role in terms of maintaining stealth and robustness. While it is possible to place tag energy so maximize the message throughput, it is unusable for authentication. Allocating power between message and tag at a constant ratio per carrier is shown to have good overall performance while requiring little additional computation.

REFERENCES

[1] P. Yu, J. S. Baras, and B. M. Sadler, "Physical Layer Authentication," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 38–51, Mar. 2008.

[2] ——, "Multi-Carrier Authentication at the Physical Layer," in *IEEE Workshop on Security, Privacy and Authentication in Wireless Networks*, Newport Beach, CA, Jun. 2008, pp. 1–6.

[3] J. L. Massey, "Shift-Register Synthesis and BCH Decoding," *IEEE Trans. Inf. Theory*, vol. 15, no. 1, pp. 122–127, Jan. 1969.

[4] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley & Sons, 1991.