Power Allocation Tradeoffs in Multicarrier Authentication Systems

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

Abstract

Physical layer authentication techniques exploit signal characteristics to 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 on each carrier.

1. 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 such an authentication system.

2. 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 1) observe what Alice is transmitting and 2) transmit arbitrary messages to Bob.

Alice transmits messages to Bob in plain view: Eve can also recover the messages. In addition, Alice superimposes authentication signals, called **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.

2.1. Signal Model

Suppose that Alice and Bob communicate using $N > 1$ 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 therefore we do not use time indices. Denote the transmitted signal by the matrix $\mathbf{X}$ with complex entries $\{X(m,n)\}$. We constrain the energy as given by its Frobenius norm

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

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

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

$$\mathbf{X} = \rho^s\mathbf{S} + \rho^t\mathbf{T} \quad (3)$$

where ρ^s, ρ^t are diagonal scaling matrices used to allocate power between the message and tag. $\mathbf{S}$ and $\mathbf{T}$ are matrices with dimension $N \times N^f$. The non-zero entries of the matrices have mean 0 and variance σ_x^2. The message $\mathbf{S}$ has NN^f non-zero entries while the tag $\mathbf{T}$ has N^tN^f. We refer to N^t as the **spread** of the tag.

The scaling matrices ρ^s and ρ^t are chosen to satisfy the energy constraint of equation (2). We refer to ρ as the baseline power allocation, which is simply the allocation when no authentication is transmitted. That is, when $\rho^t = 0$ the corresponding matrix is $\rho = \rho^s$.

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

$$\mathbf{S} = f_e(\mathbf{B}) \quad (4)$$

$$\mathbf{T} = g(\mathbf{B}, k) \quad (5)$$

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

$$\mathbf{B} = f_d(f_e(\mathbf{B})) \quad (6)$$

for all possible inputs $\mathbf{B}$ of $f_e(\cdot)$.

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 $g(\mathbf{X},k) = g(\mathbf{Y},k)$.

2.2. Channel Model and Estimation

We assume a block fading multipath channel [4]. The channel is modeled as a delay line with equally spaced taps and has frequency response $\mathbf{H}$. The frequency response per carrier has unit expected variance.

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

$$\hat{X}(k) = \rho^{-1} \frac{\hat{H}^*(k)}{|\hat{H}(k)|^2} Y(k) \quad (7)$$

The estimated message is

$$\hat{\mathbf{B}} = f_d(\hat{\mathbf{X}}) \quad (8)$$

where $f_d(\cdot)$ is the decoding function corresponding to the encoder $f_e(\cdot)$ from equation (4).

2.3. Tag Detection

With his estimate of the data $\hat{\mathbf{B}}$, Bob uses $g(\cdot)$ from equation (5) to construct the estimated tag:

$$\hat{\mathbf{T}} = g(\hat{\mathbf{B}},k) \quad (9)$$

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.

$$\mathbf{R} = \mathbf{Y} - \hat{\mathbf{H}}\rho^s f_e(\hat{\mathbf{B}}) \quad (10)$$

$$\tau = \Re(\mathrm{tr}((\rho^t \hat{\mathbf{H}}\hat{\mathbf{T}})^H \mathbf{R})) \quad (11)$$

The decision of authenticity δ is made according to the threshold test

$$\delta = \begin{cases} \hat{\mathbf{T}} \text{ is not present in } \mathbf{R} & \tau < \tau^0 \\ \hat{\mathbf{T}} \text{ not present in } \mathbf{R} & \tau \geq \tau^0 \end{cases} \quad (12)$$

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]The concept of *easy* and *hard* calculations can be characterized by their feasibility [3]. Hard calculations are infeasible to compute given constraints on computational resources, while easy calculations are feasible to compute under the same constraints.

3. 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 [5]. When no authentication tag is transmitted, the optimal power allocation is given by

$$P_k = (\nu - N_k)^+ \quad (13)$$

$$1 = P = \sum_k (\nu - N_k)^+ \quad (14)$$

where $P_k = \rho(k,k)^2$, $P = |\rho|^2$ and $N_k = \sigma_w^2/|H(k,k)|^2$. The operation $(\cdot)^+$ is defined as $(x)^+ \triangleq \max(x,0)$. We assume that ρ is given and that the allocations ρ^s, ρ^t satisfy

$$\rho_k^2 = (\rho_k^s)^2 + \frac{E|\mathbf{T}_k|^2}{E|\mathbf{S}_k|^2}(\rho_k^t)^2 \quad (15)$$

where $(\cdot)_k$ denotes the k^{th} row of a matrix. That is, 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.

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 the percentage of power used for the message and tag.

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 $P^s = |\rho^s|^2, P^t = |\rho^t|^2$.

3.1. Strategies

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

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.

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

$$P_k^t = (\nu_t - N_k)^+ \quad (16)$$

$$P^t = \sum_k (\nu_t - N_k)^+ \quad (17)$$

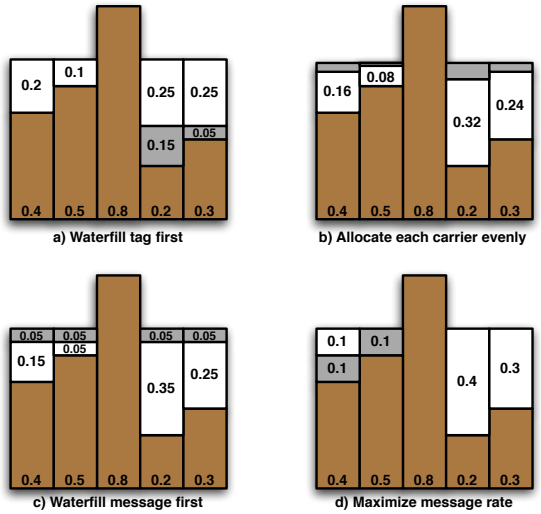

Figure 1. Power allocation strategies. Base bars represent noise power on the carriers, white bars represent message power, and lightly shaded bars represent tag power. Power allocation is 80% message and 20% tag ($P^s = 0.8, P^t = 0.2$).

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

$$\begin{aligned} P_k^s &= (\nu_s - N_k - P_k^t)^+ && (18)\\ P^s &= \sum_k (\nu_s - N_k - P_k^t)^+ && (19)\end{aligned}$$

This strategy is shown in Figure 1a. In this case, the message always occupies at least as many carriers as the tag.

3.1.2. 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 (13) and (14). Then, using the message and tag power allocations (P^s, P^t, respectively) we calculate the message and tag powers per carrier

$$\begin{aligned} P_k^s &= P^s P_k && (20)\\ P_k^t &= P^t P_k && (21)\end{aligned}$$

This strategy is shown in Figure 1b. 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.

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

$$\begin{aligned} P_k^s &= (\nu_s - N_k)^+ && (22)\\ P^s &= \sum_k (\nu_s - N_k)^+ && (23)\end{aligned}$$

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

$$\begin{aligned} P_k^t &= (\nu_t - N_k - P_k^s)^+ && (24)\\ P^t &= \sum_k (\nu_t - N_k - P_k^s)^+ && (25)\end{aligned}$$

This strategy is shown in Figure 1c. In this case, the tag always occupies at least as many carriers as the message.

3.1.4. Maximization of Message Rate. Consider the message capacity of the k^{th} carrier. In a AWGN channel with the water-filling allocation (13), the message capacity is

$$C_k^s = \begin{cases} \frac{1}{2}\log\left(\frac{\nu}{N_k + P_k^t}\right) & P_k^s > 0 \\ 0 & \text{otherwise} \end{cases} \quad (26)$$

where we assume that the tag has a normal distribution.

Suppose we wish to allocate power across carriers such that the message rate is maximized. From (26) 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

$$\max_{\mathbf{P^t}} \sum_k C_k^s \quad (27)$$

with the constraints

$$\begin{aligned} \sum_k P_k^t &= P^t = 1 - ||\rho^s||^2 && (28)\\ P_k^t &\geq 0, \forall k && (29)\\ P_k^t &\leq P_k, \forall k && (30)\end{aligned}$$

We use the Lagrange method to solve the problem and find that the optimal strategy places the tag power in the carriers with the highest noise levels. 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 $k \leq K$

Table 1. Simulation parameters for the multi-carrier, perfect CSI case

Channel Model	Rayleigh block fading
Noise Model	AWGN
# Carriers	32 (4 taps)
Modulation	BPSK: SNR $\leq$ 7dB 4-QAM: SNR $>$ 7 dB 16-QAM: SNR $>$ 12 dB 64-QAM: SNR $>$ 17 dB
Channel Estimate Method	Known
Frame Length	4 OFDM symbols
# Monte Carlo Samples	2^{14}

- $P^t_{(t_k)} = \min\left(\left(T - \sum_{l<k} P^t_{(t_l)}\right)^+, \nu - N_{(t_k)}\right)$
- k = k+1

This strategy is shown in Figure 1d. 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.

4. Metric Evaluation

We perform a Monte Carlo simulation to evaluate the robustness, stealth, and security of the authentication system. The simulation parameters are given in Table 1.

4.1. 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 total tag power as well as the effect of various power allocation strategies.

Figure 2 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.

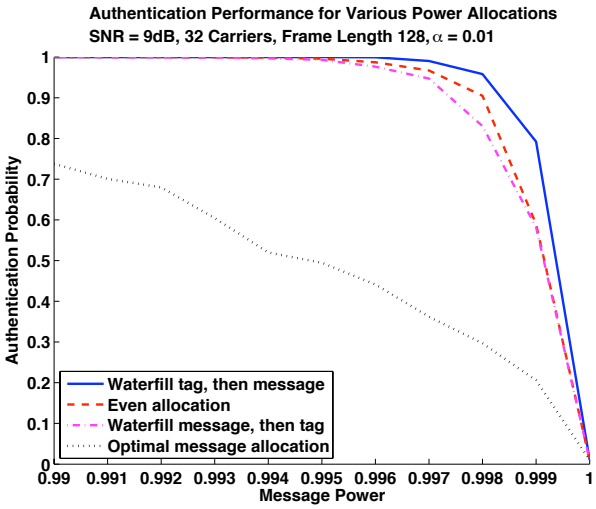

Figure 2. Robustness for various strategies. Average SNR = 9 dB. False alarm probability $\alpha = 0.01$.

4.2. Stealth

The stealth of the authentication system can be measured by its message 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 that increases as the total tag power increases.

4.3. Security

The equivocation [6] 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 con-

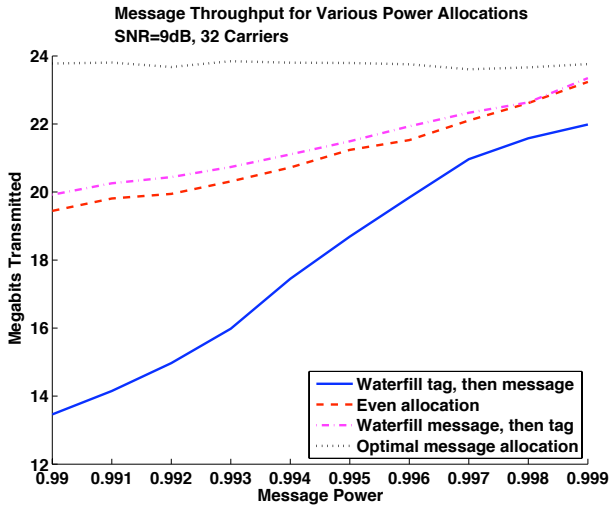

Figure 3. Throughput for various strategies. Average SNR = 9 dB.

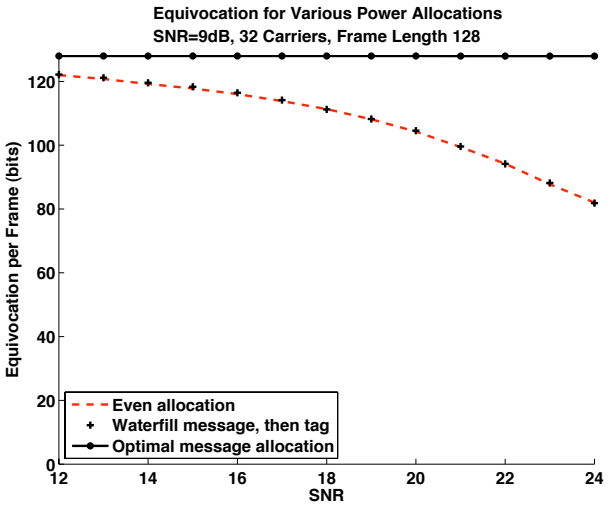

Figure 4. Tag equivocation for various strategies. 128 tag bits. Average SNR = 9 dB.

tain (between 0 and M). The probability of observing n errors in a length M tag with bit error probability p^t is

$$Pr(p^t, n, M) = (p^t)^n (1-p^t)^{M-n} \tag{31}$$

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

$$\begin{aligned} H(\mathbf{T}|p^t) &= \sum_{T \in \mathcal{T}} Pr(\mathbf{T}=T|p^t) \frac{1}{Pr(\mathbf{T}=T|p^t)} \qquad (32) \\ &= \sum_{n=0}^{M} \binom{M}{n} Pr(p^t, n, M) \log_2 \frac{1}{Pr(p^t, n, M)} \end{aligned}$$

where $Pr(\cdot,\cdot,\cdot)$ is defined above in equation (31).

We compare the equivocation for the policies as shown in Figure 4. 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.

5. Conclusion

We have extended the physical layer authentication framework to multicarrier systems and have shown how to stealthily authenticate while maintaining high levels of security and robustness. When channel state information is 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 to 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] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 2001.

[4] J. G. Proakis, *Digital Communications*. McGraw-Hill, 2000.

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

[6] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.