Multi-Carrier RF Authentication

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

The Institute for Systems Research

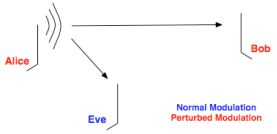
University of Maryland 18 56

Abstract

Prior to joining a network, devices must be authenticated. Typical solutions to the authentication problem involve high complexity (e.g. cryptography), high overhead (e.g. Kerberos), or require physical identification (e.g. smart cards). All of these authentication protocols occur in the open, and are subject to attack by adversaries who wish to disrupt the authentication, modify the messages, or impersonate some of the parties.

We propose a class of authentication systems that use properties of the physical layer to provide a system that is stealthy against detection, robust against noise, and secure against attack. The information necessary for authentication is contained in a tag which is hidden by the receiver noise, path loss, shading, multipath fading, etc. present at the receiver. It is only with the secret shared key that the receiver can detect and validate the authentication.

Scenario



Bob (Rx) wants to authentication Alice (Tx) while Eve (Tx/Rx) attempts to disrupt. Alice sends a perturbed signal to Bob to signal the authentication.

- Can Eve detect that the signal is intentionally perturbed (not just noise)?
- What information does Eve gain about her observation?

Signal Models

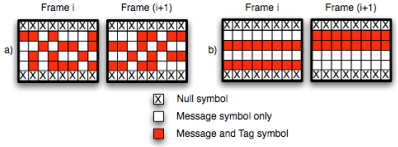
Alice transmits $\tilde{x}(t)$

Bob observes $y(t) = \int_{-\infty}^{\infty} h(t,\tau)\tilde{x}(t-\tau)d\tau + n(t) + v(t)$

Rather than time-multiplexing, Alice superimposes the authentication tags

$$\mathbf{x} = \mathbf{s} \text{ (reference signal)}$$
$$\tilde{\mathbf{x}} = \rho_s \mathbf{s} + \rho_t \mathbf{t} \text{ (tagged signal)} \quad 0 \le \rho_s, \rho_t \le 1$$

In general the signal is multi-carrier. The tags may be placed on only the message symbols.



Properties

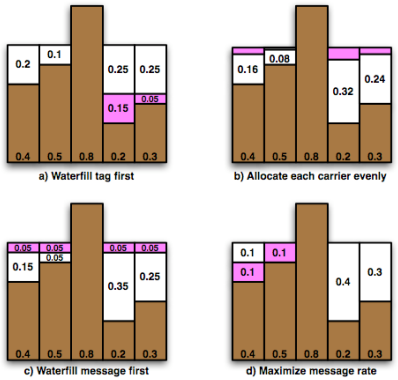
Stealth: with high probability,
- Bob receives data without decrease in performance
- Eve cannot detect presence of authentication

Robustness: with high probability,
- Bob can reliably authenticate Alice in the midst of noise and interference

Security: with high probability,
- Eve cannot modify Alice's messages or impersonate her

Power Allocation

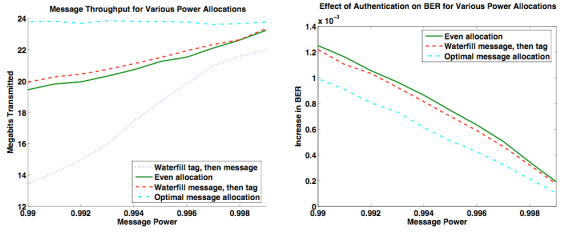
Allocation of power between data and authentication affects the properties. Strategies for tag allocation use the waterfilling solution



Shown: 80% data power, 20% tag power

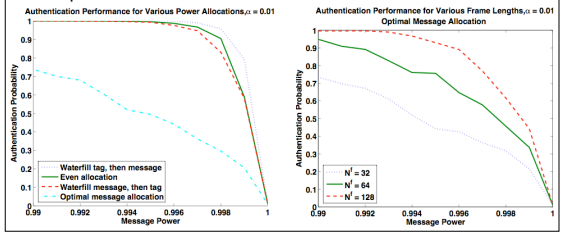
Stealth

Power allocation strategy should be carefully chosen:



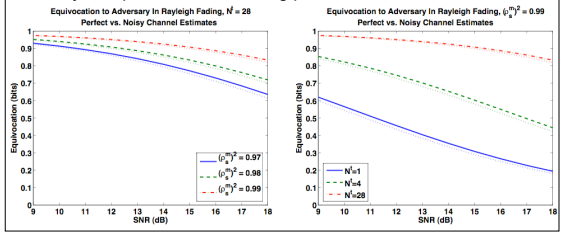
Robustness

Optimal strategy for message rate performs worst, but frame length can improve robustness.



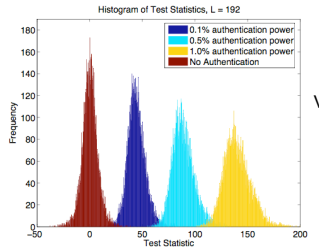
Security

Security is improved with lower tag power over more carriers



Experiment Setup

GNU Radio: Free toolkit to build and deploy software radios
- 64 megasample/sec 12-bit A/D converters
- 128 MS/s 14-bit D/A converters
- USB 2.0
- Universal Software Radio Peripheral



Validate theoretical results
- Single, multi-carrier
- Possibility of small perturbations