Preventing Wormhole Attacks Using Physical Layer Authentication

Shalabh Jain and John S. Baras
Institute for Systems Research
University of Maryland, College Park, MD 20742
Email: {shalabh, baras}@umd.edu

***Abstract*—Mobile ad-hoc networks (MANETs) are a key enabler of pervasive computing. Constrained resources in mobile stations make it critical for nodes to be able to cooperate to enhance communication and computation capabilities. However, the wireless and dynamic nature of the links presents easy attack vectors for adversaries. The ability to securely discover and identify neighboring nodes (secure ND) is a fundamental building block for such networks. Even a relatively weak adversarial relay has the capability of distorting the network view and diverting significant amount of traffic. This can cause significant performance degradation. In this paper, we utilize the physical layer authentication scheme introduced by Yu, Baras and Sadler [1] to secure neighborhood discovery against adversarial relays. The proposed method incurs little performance overhead and requires no additional hardware. We provide analytical and simulation based performance evaluation of the security of our scheme.**

I. Introduction

The rapid progress of wireless technology over the past decades has inspired a new paradigm of usage and applications, particularly in the form of sensor and mobile ad-hoc networks. Mobile wireless networks offer the opportunity to form dynamic cooperative structures and topologies to achieve computational tasks, or simply increase communication range. However the dynamic nature of the medium also brings several open problems such as security, efficient routing and power management.

Any cooperative protocol such as routing and collaborative sensing, requires, at the very least, the nodes' one-hop neighborhood information. Performance of the network depends on the quality and robustness of the neighborhood discovery (ND) component. A breakdown of security in ND can be catastrophic for all services. For example, there are several routing techniques, [2], which guarantee security under the assumption of secure ND. Thus there is great interest to secure ND, for example [3], [4], [5].

One particular attack that has attracted significant attention is the wormhole attack. Wormholes are relay attacks with the goal of drawing network traffic by offering low latency (or cost) paths. These can be launched by simple adversaries and have the capability of immense performance degradation. Conventional higher layer authentication can securely provide the identity of the creator. These credentials can however be relayed without violating the cryptographic primitives, rendering the scheme futile against wormholes. This makes wormholes extremely difficult to detect. Several techniques have been proposed for detection of wormholes [5], [6], [7], [8]. Guler et al, [9] provide an excellent overview of wormhole attacks and their countermeasures. Most of these schemes depend on stringent timing constraints or special hardware.

Timing based schemes, such as [5], require tight synchronization and specialized hardware. Other timing based schemes, such as [6], use metrics such as the expected round trip time. These parameters are highly dependent on network topology and congestion. Additionally, authors in [10] formally prove the failure of timing based schemes against fast adversaries. Location based schemes, which are provably secure, have the major disadvantage of requiring specialized hardware. Statistical and graph theoretic models proposed in [7], [8], for wormhole detection do not suffer from special hardware requirements. However, these techniques require central decision making [7] or have high computational complexity [8]. Furthermore, these techniques are unable to pin-point the exact location of the wormhole.

The advantage offered by radio-fingerprinting for preventing wormhole attacks is well acknowledged. There has been considerable effort in this direction [11], [12] and the references therein. However, several authors [13] have raised concern over the scalability of such metrics. These authors also demonstrate feasible impersonation attacks for transient based methods.

Yu et al [1] provide a framework for inserting low power fingerprint-like signals to authenticate the transmitter. We modify this scheme for application to ad-hoc networks. Since the fingerprint used is generated through a deterministic algorithm (as compared to natural imperfections), the security of the signal can be guaranteed by cryptographic primitives. Our scheme requires no additional hardware. The computation and power overhead of our scheme is negligible. Thus our scheme causes very little degradation in network performance. Another important advantage of our scheme is the ability to pin-point the adversarial nodes. Since the proposed scheme is based on physical layer signature, it is independent of network topology and other associated problems such as congestion.

The rest of the paper is organized as follows. In section II we describe the system model and assumptions. In section III we also provide an overview of the mechanism presented in [1] and our modifications. In section IV we analyze the security of the scheme when applied to the ND scenario. In section V we describe the numerical evaluation results.

978-1-4673-0437-5/12/$31.00 ©2012 IEEE

II. System Model

Consider the scenario where N wireless nodes are deployed over a geographic area. The nodes are mobile, thus requiring periodic updates to their one-hop neighbor lists.

A. System Assumptions

We assume the existence of a pairwise key pre-distribution scheme. However, depending on the attack considered, this requirement can be relaxed. For example, for the simple relay attack we highlight, a common secret shared by all the network nodes may be sufficient for wormhole detection. We focus primarily on the physical layer modeling. We assume the existence of higher layer mechanisms for sharing the allocated resources like TDMA or some collision avoidance mechanism. Regarding hardware, we assume the nodes are equipped with omni-directional antennas.

B. Attacker Model

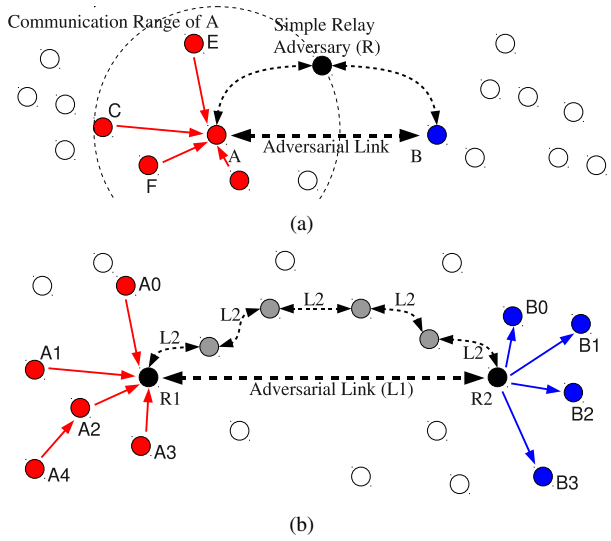


Fig. 1. Wormhole scenario with (a) Single adversary R creating an artificial link between the genuine nodes A and B; (b) Cooperating adversaries R_1 and R_2 creating a link between A_i and B_i using an out of band channel.

We consider the typical wormhole attack scenario, whereby the adversary attempts to draw significant traffic by presenting a low latency or shorter link. A taxonomy of wormholes is described well in [14]. We consider the class of external adversarial relays, with either a single adversary R (1(a)) or multiple adversaries R_1, R_2 (1(b)). Figure 1(a) represents a single relay that extends the communication neighborhood of nodes, thus creating false links. In Figure 1(b), two cooperating relays R_1 and R_2 tunnel packets from one side of the network to the other via an out of band channel, L_1.

Since we consider external relays, we assume that the relays do not have access to any network secrets. We will assume a powerful relay capable of directional transmissions with no power constraints. Though such adversaries seem weak, they are capable of significant performance degradation by selective dropping or mis-routing of data, providing poor QoS or offline data attacks. Because of their simple behavior, such relays are extremely difficult to detect by existing mechanisms at the higher layer.

III. System Description

We utilize the scheme presented in [1] to secure point-to-point links for securing multi-hop communications. Here we briefly present their scheme and notation. For details and performance metrics of the single link system, the reader is encouraged to read [1].

Consider a single-antenna transceiver transmitting narrow-band signals in flat fading channels. The sender wants to transmit a message $\mathbf{b} = \{b_1, \ldots, b_M\}$ to the receiver so that it can be recovered and authenticated. 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 sender wants to transmit an authentication tag $\mathbf{t}$ together with the message $\mathbf{s}$ so the receiver can verify her identity. In general, the tag is a function of the message $\mathbf{s}_i$ and the secret key $\mathbf{k}$, i.e.,

$$\mathbf{t}_i = g(\mathbf{s}_i, \mathbf{k}). \tag{1}$$

The tag is padded (if necessary) to the message length and simultaneously transmitted with the data. Let the transmitted signal be denoted by $\mathbf{x} = \{x_1, \ldots, x_L\}$.

$$\mathbf{x}_i = \rho_s \mathbf{s}_i + \rho_t \mathbf{t}_i \tag{2}$$

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

As with the message signal, assume the tags satisfy $E[t_k] = 0$ and $E|\mathbf{t}|^2 = L$. Also assume that $E[\mathbf{s^H t}] = 0$, so that one can interpret ρ_s^2 and ρ_t^2 as energy allocations to message and tag, respectively. An appropriate $g(\cdot)$ would make the message and tag appear uncorrelated (but not independent). The constraint $\rho_s^2 + \rho_t^2 = 1$ ensures that the transmission power remains unchanged.

A. Channel Model

Assume a Rayleigh block fading (slow fading) channel so that different message blocks experience independent fades. The channel for the i^{th} block is h_i, a circularly symmetric complex Gaussian variable with variance σ_h^2. The receiver observes the block

$$\mathbf{y}_i = h_i \cdot \mathbf{x}_i + \mathbf{w}_i, \tag{3}$$

where $\mathbf{w} = \{w_1, \ldots w_L\}$ and $w_k \sim CN(0, \sigma_w^2), \forall k$, where CN denotes complex-valued normal random variable

B. Receiver Model

Pilot symbols are typically used to aid in channel estimation. For the current setup, pilots are inserted in the middle of the block, however the framework is general enough to consider other cases as well. For the pilot symbols $\mathbf{p}$ and their observations $\mathbf{y_p}$, the MMSE channel estimate is simply

$$\hat{h} = \frac{1}{|\mathbf{p}|^2} \mathbf{p}^H \mathbf{y_p}, \tag{4}$$

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

The receiver uses its channel estimate to estimate the i^{th} message signal

$$\hat{\mathbf{x}}_i = \frac{\hat{h}_i^*}{|\hat{h}_i|^2}\mathbf{y}_i. \tag{5}$$

Let $f_d(\cdot)$ denote the decoding function corresponding to $f_e(\cdot)$. It then uses $f_d(\cdot)$ to recover the message symbols

$$\hat{\mathbf{b}}_i = f_d(\hat{\mathbf{x}}_i) \text{ and } \hat{\mathbf{s}}_i = f_e(\hat{\mathbf{b}}_i). \tag{6}$$

With the secret key, it can generate the estimated tag $\hat{\mathbf{t}}_i$ using equation (1) 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 errors, when $g(\cdot)$ is robust against input errors. For example, robust hash functions in [15] are suitable for this purpose.

$$\hat{\mathbf{t}}_i = g(\hat{\mathbf{s}}_i, \mathbf{k}) \tag{7}$$

$$\mathbf{r}_i = \frac{1}{\rho_t}(\hat{\mathbf{x}}_i - \rho_s f_e(\hat{\mathbf{b}}_i)). \tag{8}$$

The receiver performs a threshold test with hypotheses

$$H_0: \quad \hat{\mathbf{t}}_i \text{ is not present in } \mathbf{r}_i \tag{9}$$

$$H_1: \quad \hat{\mathbf{t}}_i \text{ is present in } \mathbf{r}_i. \tag{10}$$

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

$$\begin{aligned}\tau_i|H_1 &= \mathbf{t}_i^H \mathbf{r}_i \\ &= |\mathbf{t}_i|^2 + \frac{\hat{h}_i^*}{\rho_t|\hat{h}_i|^2}\mathbf{t}_i^H\mathbf{w} = |\mathbf{t}_i|^2 + v_i, \end{aligned} \tag{11}$$

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

$$\tau_i|H_0 = \left(\frac{1-\rho_s}{\rho_t}\right)\mathbf{t}_i^H\mathbf{s}_i + v_i \tag{12}$$

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

Here we deviate from the decision regions of [1]. Since our primary objective in this scenario is to minimize the probability of accepting faulty tags, we choose a smaller region of acceptance. The authenticity δ_i for the i^{th} block is made according to

$$\delta_i = \begin{cases} 1 & \tau_i^L < \tau_i < \tau_i^H \\ 0 & otherwise. \end{cases} \tag{13}$$

The thresholds τ_i^L, τ_i^H of this test can be determined by alpha level tests. The introduction of an upperbound leads to reduced probability of detection and can be compensated for by considering the decision over multiple blocks.

IV. Security Analysis

Our security scheme is based on detection of changes in tag statistics due to the additional noise. We will show that even in the best case scenario, the adversary contributes two sources of additional noise. One is the channel between the adversary and receiver. The other, is an increase in estimation error of channel parameters by the receiver, due to a change in the underlying statistics.

Consider the scenario in Figure 1(a). The genuine nodes A and B follow the strategy described in section II. In the case when the two nodes are not in direct communication range, the adversarial relay R may attempt to relay messages between them to create a shorter path. If successful, the adversary can divert significant traffic from other nodes such as C, D as well.

Assume node B broadcasts a neighborhood discovery request, which is successfully relayed by the adversary to node A. Node A attempts to reply with an authentication signal embedded as described in section II. At the physical layer, the message received at the adversary R would be

$$\begin{aligned}\mathbf{y}_r &= h_r \cdot \mathbf{x}_a + \mathbf{w}_r \\ &= h_r \cdot (\rho_s \mathbf{s}_a + \rho_t \mathbf{t}_a) + \mathbf{w}_r, \end{aligned} \tag{14}$$

where h_r is the channel between node A and the adversary R and $\mathbf{w}_r$ is the additive noise.

Though we are highlighting the security with respect to Figure 1(a), the formulation above holds identically for the scenario in Figure 1(b). Since traffic between R_1 and R_2 is tunneled without modification, the pair of nodes appears as a single sink and source. From a strictly practical point of view, the signal for transmission between R_1 and R_2 will have to be reasonably quantized. Tags with sufficiently low power may suffer severe distortion or might be completely lost by quantization. Thus the analysis presented is slightly optimistic.

The relay can either decode the signal and retransmit a noise free version or amplify the received signal for transmission. To perform the former, the adversary should be able to decode the signal and the tag, and recreate the original signal. Even if we assume a powerful adversary that is able to successfully estimate the channel ($\hat{h}_r$) and the signal ($\hat{s}_a$) without errors, it cannot generate the tag without the key. To estimate the tag, following equation (7),

$$\begin{aligned}\tilde{\mathbf{y}}_r &= \frac{\hat{h}_r^*}{|\hat{h}_r|^2}\mathbf{y}_r \\ \tilde{\mathbf{t}}_r &= \frac{1}{\rho_t}(\tilde{\mathbf{y}}_r - \rho_s \mathbf{s}_a) \\ &= \mathbf{t}_a + \frac{\hat{h}_r^*}{|\hat{h}_r|^2} \cdot \frac{1}{\rho_t}\mathbf{w}_r = \mathbf{t}_a + \hat{\mathbf{w}}_r, \end{aligned} \tag{15}$$

where $\hat{\mathbf{w}}_r \sim CN\left(0, \frac{\sigma_w^2}{\rho_t^2|\hat{h}_r|^2}\mathbf{I}\right)$. We can define the tag-to-noise ratio as follows

$$\gamma_t = \frac{\rho_t^2|\hat{h}_r|^2}{\sigma_w^2} = \rho_t^2\gamma_r \ , \ \bar{\gamma}_t = \frac{\rho_t^2\sigma_h^2}{\sigma_w^2}. \tag{16}$$

In order to maintain signal quality and noise characteristics, and limit bandwidth leakage, for any practical system we

choose ρ_t^2 to be sufficiently small. This would make it difficult to estimate the tag reliably.

As an example, if we consider the tag to be modulated by a simple scheme as a BPSK signal, then average probability of error is

$$P_e = \frac{1}{2}\left(1 - \sqrt{\frac{\bar{\gamma}_t}{\bar{\gamma}_t + 1}}\right) \approx \frac{1}{2}(1 - \rho_t),$$

which is close to random guessing. Thus the best strategy for the adversary to follow is amplify-and-forward. Suppose the adversary amplifies the signal by a factor A, then

$$\mathbf{x}_r = A\frac{\hat{h}_r^*}{|\hat{h}_r|^2}\mathbf{y}_r = A(\mathbf{x}_a + \tilde{\mathbf{w}}_r), \tag{17}$$

where $\tilde{\mathbf{w}}_r \sim CN\left(0, \frac{\sigma_w^2}{|h_r|^2}\mathbf{I}\right)$. The signal received at B may be expressed as

$$\begin{aligned} \mathbf{y}_b &= A \cdot h_b(\mathbf{x}_a + \tilde{\mathbf{w}}_r) + \mathbf{w}_b & (18)\\ &= A \cdot h_b\mathbf{x}_a + (A \cdot h_b\tilde{\mathbf{w}}_r + \mathbf{w}_b). & (19)\end{aligned}$$

Clearly the noise characteristics are deviant from typical Gaussian noise due to the product of Gaussian type terms present. The receiver will continue to process the data as described earlier. However, this will lead to sub-optimal results. Consider the MMSE estimation of the channel response using the K pilot symbols.

$$\begin{aligned} \tilde{\mathbf{y}}_b^p &= \frac{\mathbf{p}^H\mathbf{y}_b^p}{|\mathbf{p}|^2} & (20)\\ &= Ah_b\left(1 + \frac{\rho_t\mathbf{p}^H t_a^p}{|\mathbf{p}|^2} + \frac{\mathbf{p}^H\tilde{\mathbf{w}}_r}{|\mathbf{p}|^2}\right) + \frac{\mathbf{p}^H\mathbf{w}_b}{|\mathbf{p}|^2} & (21)\\ &= Ah_b(1 + w_t + w_r^p) + w_b^p, & (22)\end{aligned}$$

where t_a^p is the component of the tag along the signal. $w_b^p \sim CN\left(0, \frac{\sigma_w^2}{K}\right)$, and conditioned on h_r, $w_r^p \sim CN\left(0, \frac{\sigma_w^2}{K|h_r|^2}\right)$. In our system, we design the tag such that there is no component over the pilot symbols. Thus $w_t = 0$. The MMSE estimate of h_b is given by

$$\hat{h}_b = \alpha(Ah_b(1 + w_r^p) + w_b^p)\ ,\ \alpha = \frac{\sigma_h^2}{\sigma_h^2 + \sigma_w^2/K}. \tag{23}$$

For the pilot length and SNR to be sufficiently large, we can approximate $\alpha \approx 1$ and claim $|\hat{h}_b|^2 \approx A^2|h_b|^2$. We proceed with the signal estimation and tag detection as follows

$$\begin{aligned} \tilde{\mathbf{y}}_b &= \frac{\hat{h}_b^*\mathbf{y}_b}{|\hat{h}_b|^2}\\ &= \frac{1}{A|h_b|^2}(Ah_b(1 + w_r^p) + w_b^p)^*(Ah_b(\mathbf{x}_a + \tilde{\mathbf{w}}_r) + \mathbf{w}_b)\\ &= (1 + w_r^p)^*(\mathbf{x}_a + \tilde{\mathbf{w}}_r) + \frac{w_b^{p*}\mathbf{w}_b}{A^2|h_b|^2}\\ &\quad + \frac{w_b^{p*}}{Ah_b}(\mathbf{x}_a + \tilde{\mathbf{w}}_r) + \frac{1}{Ah_b}(1 + w_r^p)\mathbf{w}_b. & (24)\end{aligned}$$

Assuming perfect decoding of the signal ($\hat{s}_a$), we can obtain the residue and test statistic as

$$\mathbf{r}_b = \frac{\tilde{\mathbf{y}}_b - \rho_s\hat{s}_b}{\rho_t}\ ,\ \tau = \mathbf{t}_a^H\mathbf{r}_b. \tag{25}$$

We would like to consider the additional noise in this statistic, compared to the absence of the adversary,

$$\begin{aligned} \tilde{\tau} &= \tau - (|\mathbf{t}_a|^2 + \mathbf{t}_a^H\tilde{\mathbf{w}}_b)\\ &= \frac{1}{\rho_t}\left(w_r^{p*} + \frac{w_b^{p*}}{Ah_b}\right)\mathbf{t}_a^H(\mathbf{x}_a + \tilde{\mathbf{w}}_r)\\ &\quad + \frac{1}{\rho_t}\frac{1}{Ah_b}\left(\frac{1}{Ah_b}w_b^{p*} + (w_r^{p*})\right)\mathbf{t}_a^H\mathbf{w}_b & (26)\\ &= W_1 + W_2. & (27)\end{aligned}$$

The product of independent normal densities is a modified Bessel function of the second kind. We use W_2 to encapsulate all such terms in equation (26). To simplify analysis, we can ignore W_2 and improve a better-case (less noise) result. W_1 is complex Gaussian random variable with 0 mean and variance.

$$\sigma_{W_1}^2 = \frac{\sigma_w^2}{K}L^2\left(1 + \frac{\rho_s^2}{\rho_t^2}\beta^2\right)\left(\frac{1}{A^2|h_b|^2} + \frac{1}{|h_r|^2}\right).$$

The value $\beta \in [0, 1]$ depends on the choice of $g(.)$ relating the tag to the message. It can thus be considered as a design parameter for selection of the tag generation scheme. We can thus observe an m fold increase in the variance of the detection statistic where

$$m = \frac{L}{K}(\rho_t^2 + \beta\rho_s^2)\left(1 + \frac{1}{A^2}\right) + 1.$$

Clearly, it is possible to reduce the additional error term to a negligible value by choosing a sufficiently large amplification factor. However, this can be easily detected by simple energy sensing methods. If we consider E to be the energy detected on the channel, we can claim adversarial behavior if $E > E_0$, where E_0 denotes the energy threshold. Even by choosing a conservative threshold, we can guarantee the range of A to be small enough to cause a noticeable degradation in the test statistic.

A. Multiple blocks

Since our scheme relies on the deviation of the noise variance, a single observation may not be sufficient to make a decision about adversarial behavior of a neighbor. Thus we extend the decision over several blocks. Most MANETs require nodes to perform a periodic neighbor update for tracking changes. In this case, our scheme would require a minimum number of HELLO messages, N_{auth}, that is to be observed before declaring a neighbor as adversarial. Alternatively, in the absence of such periodic updates, or to speed up the process of detection of adversaries, we may piggyback the authentication tag periodically on data packets. Since the power overhead and computational requirements of our scheme are negligible, there is no loss of performance.

Consider the observation of N_{auth} tagged packets. Let $N_{corr} \leq N_{auth}$ be the number of packets received with a valid tag. We make the decision of adversarial behavior as

$$\begin{aligned} N_{corr} \geq N_0 &: \quad \text{Authentic}\\ N_{corr} < N_0 &: \quad \text{Adversarial Behavior.} & (28)\end{aligned}$$

Clearly, the performance of the detector is a function of the threshold N_0. If we consider α_m to be the maximum acceptable probability of missed detection, we may select N_0 based on an alpha level test. Consider p_{good}, and p_{adv} to be the probability of detecting the presence of the tag in the absence and presence of an adversary respectively. Thus N_{auth} will be a Binomial random variable with success probability p_{good}, and p_{adv} depending on the presence or absence of the adversary. We may determine N_0 as

$$N_0 = \arg\min_j \left(1 - f(N_{auth}, j, p_{adv})\right) \leq \alpha_m, \qquad (29)$$

where $f(N, j, p)$ denotes the binomial cumulative distribution function. As will be highlighted in section V, there exists a fundamental trade-off between the number of messages observed and the robustness of the decision.

V. Simulation Results

Since our scheme is based at the physical layer of a point-to-point link, it is independent of the network topology. Thus it suffices to verify our results for a single transmitter receiver pair in the presence of a single adversary. We verify our scheme with MATLAB simulations. To enable comparison of statistics, we have used parameters similar to [1]. In our simulations, the data symbols are i.i.d equiprobable binary symbols. The message is coded with a rate 1/2 code for error protection. The data and the tag are BPSK modulated. We use the Harr (Daubechies 2) wavelet decomposition to embed the tag to minimize bandwidth expansion. The resultant signal is modulated with a root raised cosine pulse shape (with rolloff factor 0.5). We consider two different environments with coherence time $L = 256$ and $L = 512$. The number of pilots are either $K = 8$ or $K = 16$, based on the coherence time. Figure 2 shows the bit error rate in the estimation of

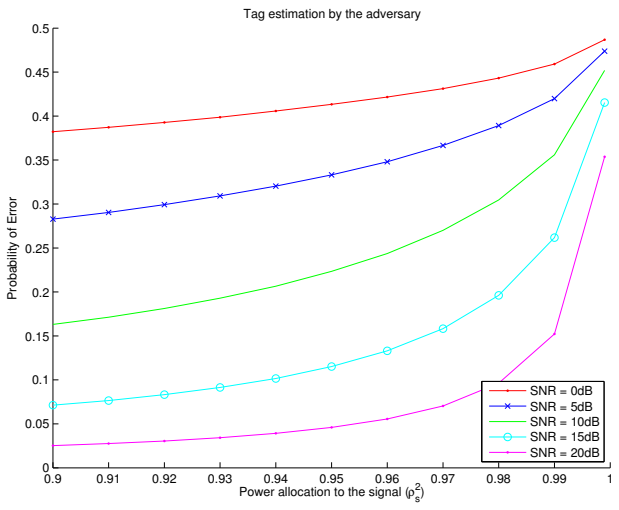


Fig. 2. Probability of error in estimation of tag by the adversary

the tag signal by the adversary for $L = 512$. Due to limited resources, it would be reasonable to consider the sensor or

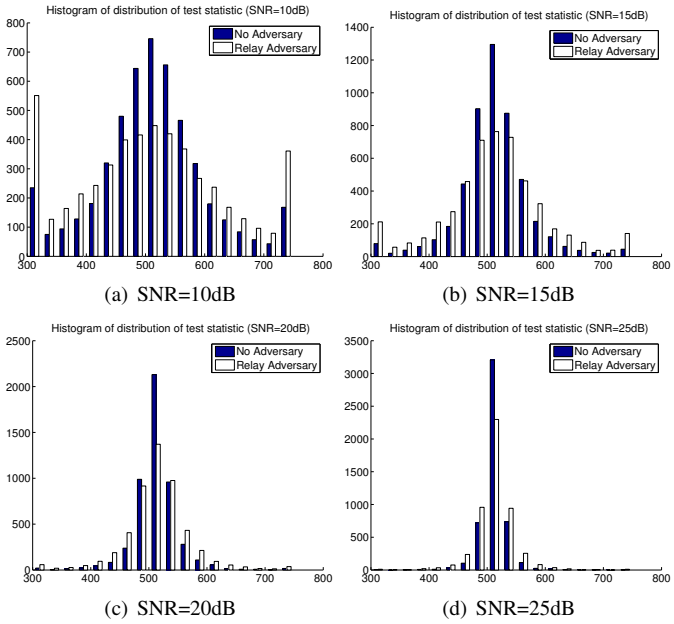
TABLE I
PROBABILITY OF DETECTION OF TAG FOR $L = 512$, $\rho_s^2 = 0.99$, ACCEPTANCE RANGE = $\pm 3\sigma$

SNR	$A = 1$		$A = 3$	
	No Adv	Adv	No Adv	Adv
10dB	0.69	0.47	0.69	0.47
15dB	0.69	0.48	0.69	0.49
20dB	0.69	0.5	0.7	0.5
25dB	0.7	0.5	0.69	0.5

TABLE II
PROBABILITY OF DETECTION OF TAG FOR $L = 256$, $\rho_s^2 = 0.98$, ACCEPTANCE RANGE = $\pm 2.5\sigma$

SNR	$A = 1$		$A = 3$	
	No Adv	Adv	No Adv	Adv
10dB	0.79	0.56	0.79	0.56
15dB	0.78	0.57	0.78	0.57
20dB	0.79	0.57	0.78	0.57
25dB	0.79	0.57	0.78	0.57

ad-hoc networks to operate in the low SNR regime. Clearly, for $\rho_s^2 > 0.98$, the error in the estimated tag is too high for re-transmission. As will be evident from the rest of this section, the performance of the authentication credentials is reasonably good for $\rho_s^2 > 0.98$. Figures 3 and 4, show the histogram

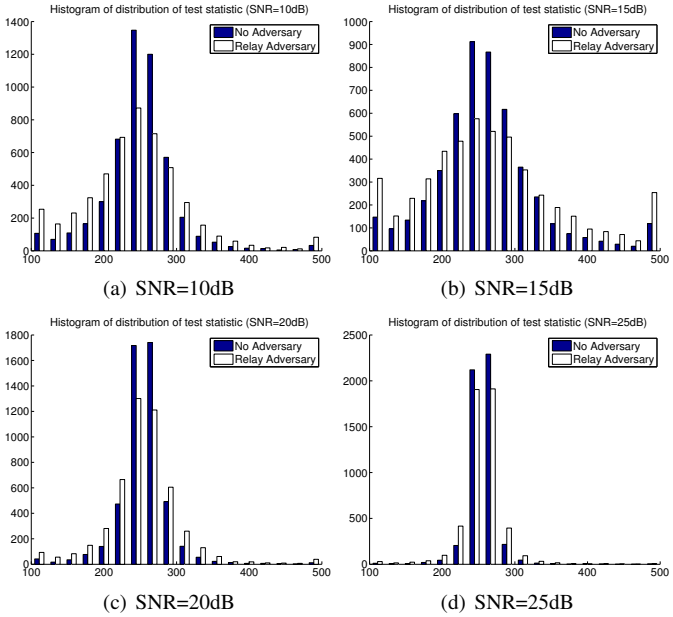


(a) SNR=10dB (b) SNR=15dB

(c) SNR=20dB (d) SNR=25dB

Fig. 3. Distribution of the auth tag for $L = 512$, $\rho_s^2 = 0.99$, adv ampl $A = 3$

of the tag statistic for both the non-adversarial and adversarial case. The exact values for the probability of detection of tag by considering $\tau_i^L = L - t\sigma_{v_i}$ and $\tau_i^H = L + t\sigma_{v_i}$ are highlighted in Table I and II. We choose the parameter $t = 2.5$ or $t = 3$ which maximizes the gap between probability of acceptance of an adversary's message vs a non-adversary's message. It can be seen from Table I, II that the difference in noise statistics



(a) SNR=10dB (b) SNR=15dB

(c) SNR=20dB (d) SNR=25dB

Fig. 4. Distribution of the auth tag for $L = 512$, $\rho_s^2 = 0.98$, adv ampl $A = 1$

is not large enough to make a reliable decision based upon a single observation.

Let us fix the alpha level $\alpha_m = 0.01$, i.e. 1% probability of missing adversarial behavior. By considering statistics from Table II, we can calculate the smallest value of N_{auth} to ensure the probability of false alarm is less than 5%. We see that for $N_{auth} \geq 80$, setting $N_0 \sim 0.65 N_{auth}$ yields an acceptable tradeoff.

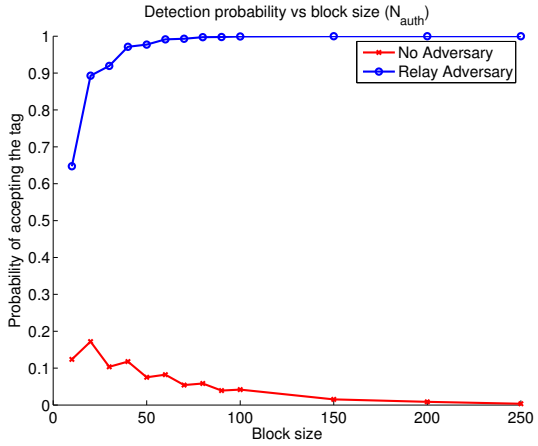


Fig. 5. Probability of error in estimation of tag by the adversary $N_0 = 65$

Figure 5 shows the variation of the probability of detection of the adversary decay with increase in the number of observation blocks.

VI. Conclusion

We developed a robust mechanism to identify wormhole attacks based on physical layer authentication. Considering the decision to be spanning several blocks, our scheme could robustly identify the adversarial behavior. The primary advantage of our scheme is the low power overhead, which is critical for mobile networks.

Acknowledgment

This material is based upon work partially supported by the Defense Advanced Research Projects Agency (DARPA) through contract award number 013641-001, MURI grant award W911-NF-0710287 from the Army Research Office, MURI grant award 015356-001 from the AFOSR and grant award CNS1018346 from the National Science Foundation (NSF).

Any opinions, findings and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of any of the funding agencies mentioned.

References

[1] P. Yu, J. Baras, and B. Sadler, "Physical-layer authentication," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 38–51, Mar. 2008.

[2] I. Khalil, S. Bagchi, C. N. Rotaru, and N. B. Shroff, "UnMask: Utilizing neighbor monitoring for attack mitigation in multihop wireless sensor networks," *Ad Hoc Networks*, vol. 8, pp. 148–164, Mar. 2010.

[3] R. Shokri, M. Poturalski, G. Ravot, P. Papadimitratos, and J.-P. Hubaux, "A practical secure neighbor verification protocol for wireless sensor networks," in *Proc. of the 2nd ACM Conference on wireless network security*, Mar. 2009, pp. 193–200.

[4] T. Hayajneh, P. Krishnamurthy, and D. Tipper, "SECUND: A protocol for secure neighborhood creation in wireless ad hoc networks," in *Proc. of 2009 International Conference on Collaborative Computing*, Nov. 2009, pp. 1–10.

[5] Y.-C. Hu, A. Perrig, and D. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *Proc. 2003 IEEE INFOCOM*, vol. 3, 2003, pp. 1976–1986.

[6] P. V. Tran, L. X. Hung, Y.-K. Lee, S. Lee, and H. Lee, "TTM: An efficient mechanism to detect wormhole attacks in wireless ad-hoc networks," in *Proc. 2007 Consumer Communications and Networking Conference*, Jan. 2007, pp. 593–598.

[7] S. Zheng, T. Jiang, J. Baras, A. Sonalker, D. Sterne, R. Gopaul, and R. Hardy, "Intrusion detection of in-band wormholes in MANETs using advanced statistical methods," in *Proc. 2008 IEEE MILCOM*, Nov. 2008, DOI: 10.1109/MILCOM.2008.4753177.

[8] R. Maheshwari, J. Gao, and S. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in *Proc 2007 IEEE INFOCOM*, May 2007, pp. 107–115.

[9] I. Guler, M. Meghdadi, and S. Ozdemir, "A survey of wormhole-based attacks and their countermeasures in wireless sensor networks," *IETE Technical Review*, vol. 28, no. 2, pp. 89–102, 2011.

[10] M. Poturalski, P. Papadimitratos, and J.-P. Hubaux, "Secure neighbor discovery in wireless networks: formal investigation of possibility," in *Proc. of the ACM symposium on information, computer and communications security*, 2008, pp. 189–200.

[11] N. T. Nguyen, G. Zheng, Z. Han, and R. Zheng, "Device fingerprinting to enhance wireless security using nonparametric Bayesian method," in *Proc. 2011 IEEE INFOCOM*, April 2011, pp. 1404–1412.

[12] A. Candore, O. Kocabas, and F. Koushanfar, "Robust stable radiometric fingerprinting for wireless devices," in *Proc. IEEE Workshop on Hardware-Oriented Security and Trust*, July 2009, pp. 43–49.

[13] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on physical-layer identification," in *Proc. of the 3rd ACM conference on wireless network security*, 2010, pp. 89–98.

[14] I. Khalil, S. Bagachi, and N. B. Shroff, "LITEWORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks," in *Proc. 2005 Conf. on Dependable Systems and Networks*, pp. 612–621.

[15] J. Fridrich and M. Goljan, "Robust hash functions for digital watermarking," in *Proc. International Conference on Information Technology: Coding and Computing*, Mar. 2000, pp. 178–183.