Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 564503, 12 pages
http://dx.doi.org/10.1155/2013/564503

Research Article

Reconfigurable Antenna Assisted Intrusion Detection in Wireless Networks

Prathaban Mookiah,[1] John M. Walsh,[1] Rachel Greenstadt,[2] and Kapil R. Dandekar[1]

[1] *Department of Electrical and Computer Engineering, Drexel University, Philadelphia, PA 19104, USA*
[2] *Department of Computer Science, Drexel University, Philadelphia, PA 19104, USA*

Correspondence should be addressed to Kapil R. Dandekar; dandekar@coe.drexel.edu

Received 7 June 2013; Accepted 20 August 2013

Academic Editor: Korkut Yegin

Intrusion detection is a challenging problem in wireless networks due to the broadcast nature of the wireless medium. Physical layer information is increasingly used to protect these vulnerable networks. Meanwhile, reconfigurable antennas are gradually finding their way into wireless devices due to their ability to improve data throughput. In this paper, the capabilities of reconfigurable antennas are used to devise an intrusion detection scheme that operates at the physical layer. The detection problem is posed as a GLRT problem that operates on the channels corresponding to the different modes of a reconfigurable antenna. The performance of the scheme is quantified through field measurements taken in an indoor environment at the 802.11 frequency band. Based on the measured data, we study the achievable performance and the effect of the different control parameters on the performance of the intrusion detection scheme. The effect of pattern correlation between the different modes on the scheme's performance is also analyzed, based on which general guidelines on how to design the different antenna modes are provided. The results show that the proposed scheme can add an additional layer of security that can significantly alleviate many vulnerabilities and threats in current fixed wireless networks.

1. Introduction

Attacks on wireless networks have become increasingly sophisticated with the increasing pervasiveness of these networks. It is challenging to detect and counteract intrusions in wireless networks due to the inherent broadcast nature of the medium. Among many known security risks, man-in-the-middle attacks and spoofing attacks [1] pose a significant intrusion threat to wireless networks since such attacks allow intruders to hijack a connection already established by a legitimate user. Though advanced wireless intrusion protection and detection systems have been developed and deployed to mitigate such threats, it has been repeatedly demonstrated that each method has its point of failure and no single method guarantees protection against all attacks [2, 3].

Such a hostile landscape requires multiple levels of defense for network protection. This requirement has gradually led to a more cross-layer approach to wireless security in recent times where security mechanisms are being deployed at different layers of the network. Particularly channel information available at the physical layer is being increasingly used to provide an additional degree of protection against intruders. Schemes that employ channel based security techniques can be categorized into encryption and authentication schemes. The former uses the wireless channel as a source for encryption key generation [4–9], while the latter utilizes a metric derived from the channel information as an identifier for authentication [10–16].

Intrusion detection has traditionally been categorized into misuse detection or anomaly detection techniques. While the former uses patterns characteristic of known attacks to detect known intrusions, the latter relies on detecting deviations from the established behavior patterns in the system [17]. In many usage scenarios, where the physical link remains unchanged over a session, the wireless channel response corresponding to the link can be considered to represent the established behavior pattern for that link. Any changes that violate this pattern abruptly beyond a certain

limit can be then checked for adversarial behavior. In this paper, we follow this approach where the channel is monitored for any abrupt changes in its statistics through repeated applications of the generalized likelihood ratio test (GLRT) [18]. The scheme is based on the idea that the statistics of the link corresponding to an intruder who is physically located at a different location will be different from that of the legitimate user and when the intruder tries to inject packets over the same connection, it will trigger an abrupt change in the GLR value.

Additionally we utilize a pattern reconfigurable antenna to improve the performance of the intrusion detection scheme. The ability of pattern reconfigurable antennas to enhance system throughput has been well demonstrated [19]. By picking antenna modes that are decorrelated in their radiation patterns, decorrelated channel realizations can be obtained to enhance system performance. Hence channels corresponding to different modes of the antenna can be expected to have different statistics, a property which is exploited to the benefit of the proposed detection scheme. However, the use of reconfigurable antennas (pattern diversity) should be differentiated from schemes that use multiple antennas (spatial diversity) with perfect decorrelation between the elements [11, 14, 16]. We relax any assumptions about channel correlation between the different diversity branches and specifically quantify the effect of correlation on detection performance. Moreover, a reconfigurable antenna provides a more practically viable solution to generate multiple channel realizations than spatially separated multiple antenna elements due to cost and space constraints.

In many public open networks (e.g., coffee shops) higher level authentication solutions are usually not implemented. Freely available software tools such as Firesheep can be used to simply execute session hijacking attacks when users visit insecure websites in such networks [20]. A wireless access point equipped with reconfigurable antennas that can implement the proposed method can be used to provide a layer of security that can significantly alleviate such security threats in these networks. In networks with higher level security mechanisms for encryption, authentication, and integrity, the proposed scheme can complement those mechanisms while they continue to play their part in securing the wireless link.

The rest of the paper is organized as follows. The intrusion detection problem and the threat model are described in Section 2. The detection scheme is described and the GLRT for intrusion detection is developed in Section 3. The channel measurement procedure is described in Section 4. We justify our assumption regarding the probability distribution of the channels in Section 5. The performance of the scheme is analyzed and the results are presented in Section 6. Some practical considerations are discussed in Section 7 before we conclude this paper in Section 8.

2. Problem Definition and Threat Model

The problem that is addressed in this paper is one of detecting an intruder who has gained access into the system by means of hijacking a connection already established by a legitimate user. The problem scenario consists of three players:

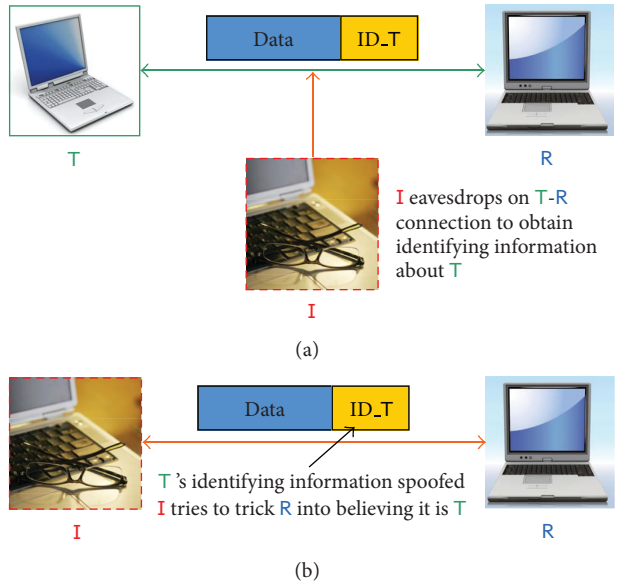

Figure 1: Illustration of the problem. (a) T eavesdrops on a data transfer session between R and T to obtain sensitive information about T's identity. (b) After obtaining the information, I tries to masquerade as T to R.

the receiver R, transmitter T, and an intruder I. Transmitter T and receiver R have established a connection and are in the process of exchanging information as shown in Figure 1(a). Intruder I eavesdrops into this connection and waits till he gathers sufficient information to spoof T. A surprisingly large number of vulnerabilities exist in modern wireless access technologies that allow I to obtain this information with relative ease. Once this information is obtained, I launches a spoofing attack by posing as T to R as shown in Figure 1(b).

To gain a practical perspective of the problem, R can be thought of as a wireless access point through which T is connected to the organizational network. I can be an adversarial entity whose objective is to gain entry into the organizational network, hijack T's connection with R, or launch a man-in-the-middle attack on the connection between T and R among other possibilities. The objective of the security scheme is to detect this change in the real transmitter at R in order to initiate counter measures.

To achieve his goal, I can be equipped with a powerful transceiver capable of passively monitoring and capturing all traffic between T and R and sufficient computational resources to analyze the traffic to exploit the vulnerabilities in relatively quick time. I can be an external adversary attempting to launch an attack on the network from outside the organization's premises or an internal entity who is interested in launching an attack on T. In both cases, we note that I cannot be physically colocated with T which forms the basis of our method for intrusion detection.

It should be noted that I's motive is to compromise T's identity in the network and therefore it is imperative for I that T first initiates and establishes a connection with R. Therefore, it is assumed that I will not resort to jamming attacks to prevent T from establishing a successful connection with R.

Additionally, we assume that only R is equipped with a reconfigurable antenna with M modes since it is more likely that an access point is equipped with such an antenna than a user terminal due to cost and space constraints. Therefore, we also assume T and R to be equipped with standard omnidirectional antennas.

As stated earlier, the proposed solution exploits the fact that T and I have to be located in two different physical locations which would be manifested by two different channel distributions sensed by R. Due to the multipath structure of the environment, I cannot methodically manipulate the channel between itself and R in such a way as to imitate the channel between T and R. This is because it does not and cannot know the channel between T and R. Introducing reconfigurable antennas to the solution adds multiple channel distributions corresponding to each mode used in the antenna. This makes the problem of closely matching the channel corresponding to T even more challenging for I which results in enhanced protection. However, it should be noted that our scheme does not attempt to localize T or I. Instead, channel information pertaining to the different antenna modes is used to detect I if it compromises the existing link between T and R.

3. Description of Scheme

With the notable exception of mobile networks, many current and emerging wireless data networks are associated with stationary terminals at both ends of the link. Temporal variations in channels related to such networks arise mainly due to movements of people and objects in the vicinity of the terminals as well as small localized movement of the terminals within a very small area [21–23]. A typical example for such a scenario would be a user seated at a bench in a public place accessing the network from a laptop connected to an access point in the vicinity. This work addresses intrusion problems that pertain to such wireless network usage scenarios and does not address large-scale terminal mobility.

The amplitude of the estimated complex channel coefficient, corresponding to a single frequency carrier g, is denoted by h. The probability distribution of h follows a Ricean or Rayleigh distribution. We choose the latter distribution with parameter σ to describe h for reasons that will be discussed in Section 5:

$$p_\sigma(h) = \frac{h}{\sigma^2} e^{-h^2/2\sigma^2}. \tag{1}$$

During the connection establishment process, $\sigma = \sigma_0$ corresponding to T is estimated through a sequence of training packets. At some time instant when I succeeds in spoofing T, it will hijack this connection. However, since I is at a physically different location, $\sigma = \sigma_1$, corresponding to this link, will be different from σ_0 and will be unknown.

Let h_i ($i \in \mathbb{Z}$, $i > 0$) be a sequence of observed i.i.d. channel estimates from the incoming packets after the initial training stage and $\mathbf{h} = [h_j, \ldots, h_k]$. i can be taken to denote the packet or time index. $N = k - j + 1$ is the *block size*. If we denote $\sigma(\mathbf{h})$ as the σ value of the Rayleigh distribution from which the elements of $\mathbf{h}$ originated, the intrusion detection problem can be now formulated as a hypothesis testing problem as follows:

$$\begin{aligned} \mathsf{H}_0 &: \sigma(\mathbf{h}) = \sigma_0, \\ \mathsf{H}_1 &: \sigma(\mathbf{h}) \neq \sigma_0. \end{aligned} \tag{2}$$

We employ a Neyman-Pearson detector which decides H_1 if the likelihood ratio exceeds a threshold:

$$L(\mathbf{h}) = \log\left(\frac{p_{\sigma_1}(\mathbf{h}; \mathsf{H}_1)}{p_{\sigma_0}(\mathbf{h}; \mathsf{H}_0)}\right) > \gamma. \tag{3}$$

However, σ_1 is not known in our case. In this case, it is well known that the GLRT which replaces σ_1 with its maximum likelihood estimate (MLE) is asymptotically the uniformly most powerful among all tests [18]. Hence, we resort to the GLRT that uses the MLE of σ_1 denoted by $\widehat{\sigma}_1$. Estimation is done over the elements in block $\mathbf{h}$. The MLE for σ_1^2 is given by [24]

$$\widehat{\sigma}_1^2 = \frac{1}{2N} \sum_{i=j}^{k} h_i^2. \tag{4}$$

Substituting (4) into (3) and simplifying yields:

$$L(\mathbf{h}) = \left(\frac{2N\sigma_0^2}{\lambda}\right)^N e^{(\lambda/2\sigma_0^2 - N)}, \tag{5}$$

where $\lambda = \sum_{i=j}^{k} h_i^2$.

The use of multiple antenna modes will result in M different channel realizations at each time instant. The environment "seen" by the different modes of the antennas will be different due to the differences in their radiation patterns and therefore the distribution for each of these M channel realizations will be characterized by different σ's. Assuming that the channel realizations yielded by the different antenna modes are independent, we can now write

$$L(\mathbf{h}) = \log\left(\prod_{m=1}^{M} \frac{p_{\sigma_{1m}}(\mathbf{h}_m; \mathsf{H}_1)}{p_{\sigma_{0m}}(\mathbf{h}_m; \mathsf{H}_0)}\right) > \gamma, \tag{6}$$

where σ_{0m} and σ_{1m} are the distributions' parameters for mode m under the null and alternate hypothesis, respectively, $\mathbf{h}_m$ represents the channel vector for mode m. The decision function and is simplified to:

$$L(\mathbf{h}) = \sum_{m=1}^{M} \left[\left(\frac{2N\sigma_{0m}^2}{\lambda_m}\right)^N e^{(\lambda/2\sigma_{0m}^2 - N)}\right], \tag{7}$$

where $\lambda_m = \sum_{i=j}^{k} h_{im}^2$ and h_{im} denotes the channel realization at time instant i for the mth antenna mode.

The control parameters that can be used to tune the performance of this scheme are listed in Table 1.

A graphical depiction of these parameters are shown with respect to a sample evolution of $L(\mathbf{h})$ in Figure 2.

Table 1: Control parameters.

Parameter	Description
N	Block size. Number of most recent consecutive channel estimates used in the test including the estimate corresponding to the packet under test.
N_T	Number of training packets used to estimate σ_0 during connection initialization.
γ	Threshold. It can be set based on the values of $L(\mathbf{h})$ observed during the training phase.
N_D	Detection delay. Maximum number of packets from I within which it should be detected. If detection does not happen by this time, it is considered a missed detection.
N_F	Number of packets from T before I takes over. Though this is not a controllable parameter in real time, it has a critical effect on the false alarm rate.
M	Number of antenna modes.

3.1. Steps of the Detection Scheme

(1) During the outset of the session, R estimates σ_0 through training. The number of packets used for training is denoted by N_T.

(2) R also computes $L(\mathbf{h})$ for $j = i - N + 1$ and $k = i$ based on these channel estimates at each instant i $(N \leq i \leq N_T)$.

(3) Actual transmissions begin from T and R continues to compute $L(\mathbf{h})$ for each packet transmission. I is assumed to hijack this connection and starts transmitting to R after N_F transmissions from T.

(4) Based on these computed $L(\mathbf{h})$ during the training phase, a threshold γ is picked such that an alarm is raised whenever $L(\mathbf{h}) > \gamma$.

(5) In the event of an alarm, a higher layer reauthentication procedure can be evoked to reverify the identity of the transmitter.

3.2. Threshold Selection. The value of γ will be chosen based on the values observed for $L(\mathbf{h})$ during the training period. If the maximum value of $L(\mathbf{h})$ observed during training is $L_M(\mathbf{h})$, we can express γ as $KL_M(\mathbf{h})$ where K is the scaling factor that needs to be controlled in order to achieve the desired detection and false alarm rates. In our scheme, selection of K is performed in an adaptive manner. We start with $K = 1$ and gradually increase its value till an acceptable false alarm rate is achieved.

The connection can be vulnerable to an attack during this threshold selection phase as well. Therefore, higher layer authentication protocols (e.g., 802.11i) should be evoked to verify false alarms during this adaptation process to ensure security until the target value of K is reached though this may cause some processing overhead due to frequent reauthentication. Optionally, depending on the level of threat to which the network is exposed to, this reauthentication process can be relaxed during this adaptive threshold determination phase for more efficient operation and all alarms may be treated as false alarms.

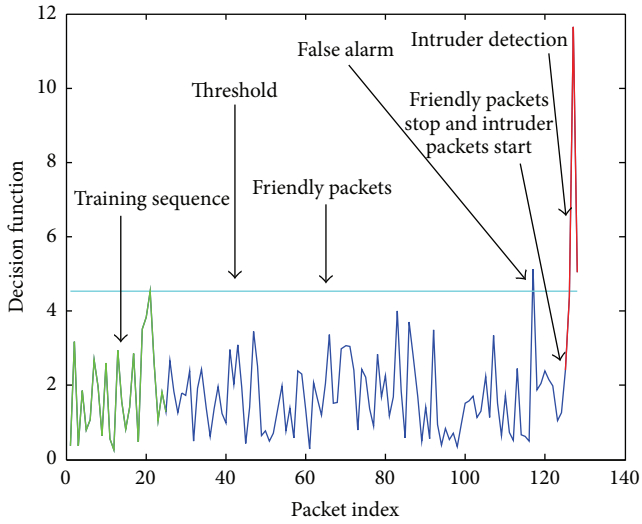

Figure 2: Sample evolution of the GLRT. $N_T = 25$, $N_F = 100$, $N = 5$, and $M = 1$. Threshold in this case is chosen to be the maximum of $L(\mathbf{h})$ observed during training.

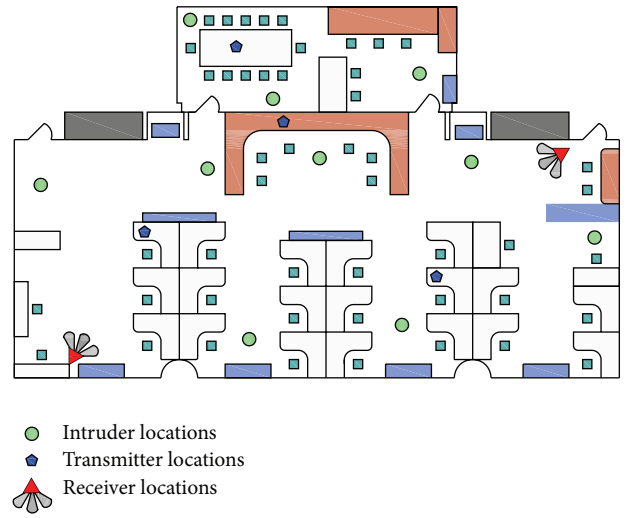

Figure 3: Layout of measurement environment. Test locations of R, T, and I are indicated as shown in the figure.

4. Channel Measurements

Channel measurements were performed on Drexel University campus using a four-port vector network analyzer. The measurement environment and node locations are shown in Figure 3. The environment is a large laboratory which is 20 m long, 8 m wide, and 4 m high with plaster walls. The room has several cubicles partitioned using metallic walls and laboratory equipment and furniture distributed throughout the room.

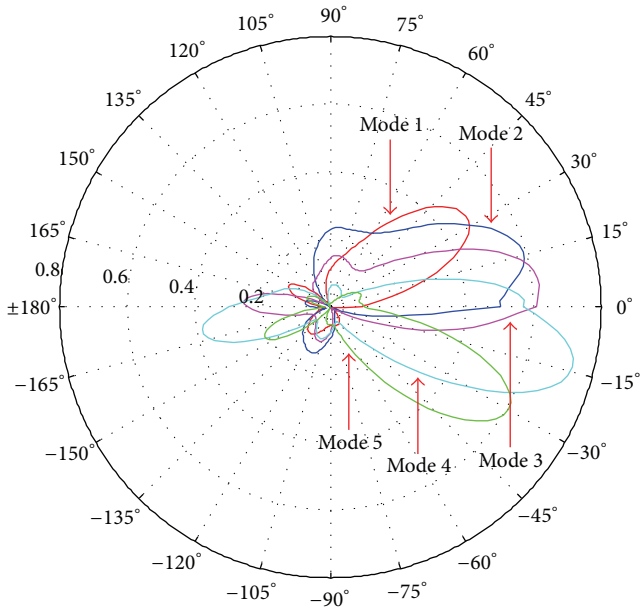

FIGURE 4: Radiation patterns corresponding to the 5 different antenna modes in the elevation plane. The elevation plane corresponds to the measurement environment plane shown in Figure 3. All patterns are vertically polarized.

The measurements were performed with R equipped with a reconfigurable leaky wave antenna (LWA) [25]. The radiation patterns corresponding to the five modes used in the study are shown in Figure 4. T and I were equipped with standard monopoles. Measurements were performed at 2.484 GHz which corresponds to the center frequency of channel 14 of the 802.11 band. Two R, four T, and ten I locations were chosen which yielded a total of eight R – T links each with then corresponding R – I links. For each (R, T, I) combination, 1000 time snapshots were recorded for the R – T and R – I links for the 5 different antenna modes. Measurements were performed during different hours of the day over several days during which there was low to moderate movement in the environment.

5. Why Rayleigh Distribution?

It has been assumed that the channel amplitudes follow a Rayleigh distribution instead of the more general Ricean distribution for the purposes of this study. In order to justify this assumption, the empirical distribution functions obtained for each link from the measured data was compared to a Rayleigh or Ricean distribution whose parameters were estimated from the measurements. The similarity between the empirical distribution (p_e) and standard distribution (p_p) for each link is quantified through two metrics: the total variation distance between the distributions and the Kullback-Leibler (KL) divergence.

The total support S is defined as

$$\min\left(S_e, S_p\right) \leq S \leq \max\left(S_e, S_p\right), \tag{8}$$

where S_e and S_p are the supports of the empirical and standard distributions, respectively. S is discretized into T evenly spaced discrete points. The total variation distance between the two distributions is defined as

$$e = \frac{1}{2}\sum_{t=1}^{T}\left|p_e\left(h_t\right) - p_p\left(h_t\right)\right|, \tag{9}$$

where $p_e(h_t)$ and $p_p(h_t)$ denote the values of the distributions evaluated at the tth discrete point in S. The KL divergence between p_e and p_p is defined as

$$D_{\mathrm{KL}}\left(p_e \parallel p_p\right) = \sum_{t=1}^{T} p_e\left(h_t\right)\log_2\frac{p_e\left(h_t\right)}{p_p\left(h_t\right)}. \tag{10}$$

Table 2 lists the trends in the observed values over all the measured links for the difference between the empirical distribution and the two standard distributions.

As can be observed, though the channel distributions are not "purely" Rayleigh nor Ricean, which is to be expected, they resemble these distributions sufficiently enough which provides us with the ability to develop an analytical framework for the problem. Moreover, as the values indicate, on average, due to the combination of line-of-sight (LOS) and nonline-of-sight (NLOS) links, modeling the channel as Rayleigh does not lead to a large error compared to modeling it as Ricean in the system, though the observed distributions marginally resemble the Ricean distribution more than the Rayleigh. Nevertheless, Rayleigh distribution was picked over Ricean for three reasons. Closed form MLE estimates do not exist for the parameters that characterize Ricean distributions and it requires recursive methods that are computationally intense [26]. The second reason is that when small values of N are used in the scheme, the recursive scheme does not achieve convergence resulting in very poor estimates that will have a significantly negative effect on the scheme's performance. Finally, a simpler form of GLRT function cannot be formulated due to the Bessel functions that characterize Ricean distributions which will lead to higher computational complexity. Based on these observations and reasons, the channel was modeled as Rayleigh distributed.

6. Analysis and Results

The performance of the intrusion detection scheme was studied in terms of the probability of missed detection (β) and false alarm rates (α) as a function of the different control parameters listed in Section 3. α and β characteristics presented in this section were computed from the measured channels as follows.

(1) For each (R, T, I) combination, a detection threshold γ was obtained through the first N_{T} training samples.

(2) For the N_F subsequent samples from T, the number of instances where $L(\mathbf{h})$ exceeds γ was recorded. A false alarm was recorded when the number of instances was greater than one.

(3) The friendly samples were followed by samples from I. A detection was recorded if $L(\mathbf{h})$ exceeds γ within

Table 2: Difference between empirical and parametric distributions.

Distribution	Mean of e	Standard deviation of e	Mean KL divergence
Rayleigh	0.059	0.014	1.56
Ricean	0.036	0.014	0.32

the first N_{I} transmissions from I. If not, a miss was recorded.

(4) This process was repeated for 100 trials with different subsets of friendly and adversary samples and the average α and β were computed.

(5) The overall α and β were computed as the average obtained over all possible (R, T, I) combinations.

Unless specifically otherwise stated, the presented results also reflect the average over the different antenna combinations possible for a given M; that is, for a given α, the presented missed detection probabilities are averages obtained over the $\binom{5}{M}$ possible combinations for a given M.

6.1. Single Antenna Mode (M=1). Figure 5 shows the average detection error tradeoff (DET) curves for a single antenna mode for different values of block size N. The nonlinear scaling of the axes in a DET curve is designed to yield a straight line when $L(\mathbf{h})$ from the system follows a normal distribution [27]. The diagonal line defined by $\beta = -\alpha$ represents completely random performance and curves that lie on the quadrant left of this line represent positive levels of performance.

It can be observed that the performance improves with block size. This is due to two reasons. A larger block size gives a better estimate for σ_1 and hence when the intruder starts injecting packets, the difference between σ_0 and σ_1 becomes more clear which in turn results in $L(\mathbf{h})$ growing above the threshold rapidly. Moreover, when N is large, the increased contribution from channels corresponding to I in $L(\mathbf{h})$ after the intrusion will result in a rapid increase in its value as well.

Moreover, the values of N used in the computation of $L(\mathbf{h})$ are not sufficiently large enough to yield a Gaussian behavior and therefore the DET curves do not exhibit a linear trend. While such a Gaussian behavior is preferred since it allows us to resort to standard normal distributions to set the threshold γ, it will not be possible to employ a sufficiently large N to yield this behavior since a meaningful minimum detection delay N_D is determined by the block size.

However, with just a single antenna mode, the achievable detection rates are unacceptably low at low α regions. In cases where σ_1 and σ_0 are not well separated, the level of increase in $L(\mathbf{h})$ after intrusion will not be sufficient enough to match the γ that is required to maintain a low α which in turn leads to poor detection rates. To gain insights into this, we define the maximum percentage difference between σ's among the different antenna modes as

$$P = \max_{m=1,\ldots,M} \frac{|\sigma_{1m} - \sigma_{0m}|}{\sigma_{0m}} \times 100\%. \quad (11)$$

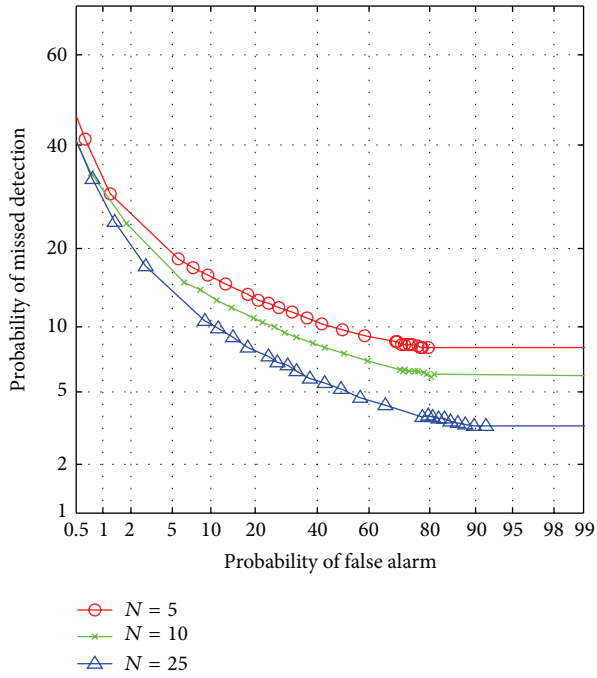

Figure 5: Average DET curves for a single antenna ($M = 1$) mode for different values of N. N_D is equal to N for each curve. $N_{\mathrm{T}} = 25$. For a given α, β decreases with the block size. However, at low α levels, the corresponding β levels remain unacceptably high for a single antenna mode even at relatively large block sizes.

Table 3: Statistics pertaining to P from measured links.

	$M = 1$	$M = 2$	$M = 3$	$M = 4$	$M = 5$
Mean (P)	75.5	95.8	105.6	111.7	116.1
Median	76.2	86.6	88.9	90.4	91.5
Pr ($P \leq 100$)	0.93	0.89	0.86	0.84	0.82

Figure 6 shows the CDF of P for different values of M. Table 3 lists some of the quantities extracted from these CDFs. When a single antenna mode is employed, the mean maximum percentage difference is 75.5% and the probability of this percentage difference being greater than 100% is as low as 0.07. This observation clearly elucidates the challenge with designing a GLRT based detection scheme using a single antenna. Though the links can be differentiated in terms of σ, the amount of separation in σ_0 and σ_1 may not be sufficient in any given scenario for the GLRT to yield acceptable performance levels with a single antenna mode.

Figure 7 shows the variation of probability of detection as a function of detection delay in terms of number of packets. Understandably, detection rate improves with the allowable detection delay. However, it should be noted that timely detection of the intruder is very critical and therefore N_D cannot be increased to arbitrarily large values to achieve the required detection rates. Again, it can also be observed that the performance improves with block size. However, to be effective, higher values of N require that the detection delay to be at least as long as the block size so that the block will contain samples entirely from the intruder. The effect of

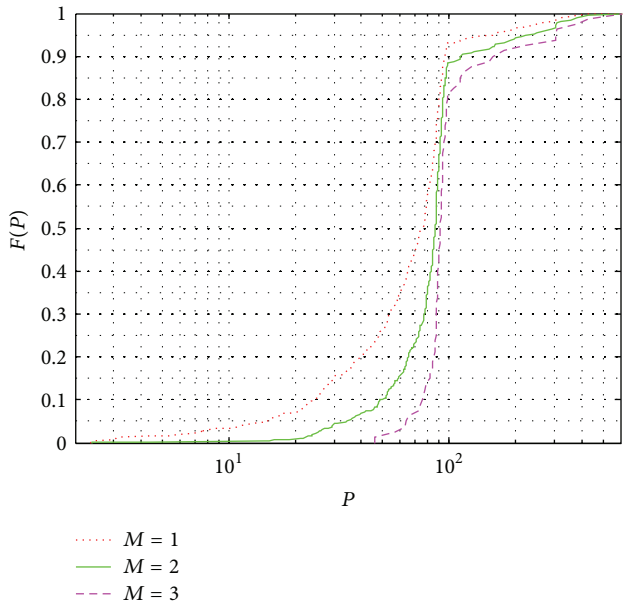

Figure 6: CDF of P for different values of M. The support and mean shifts toward higher values with increasing M.

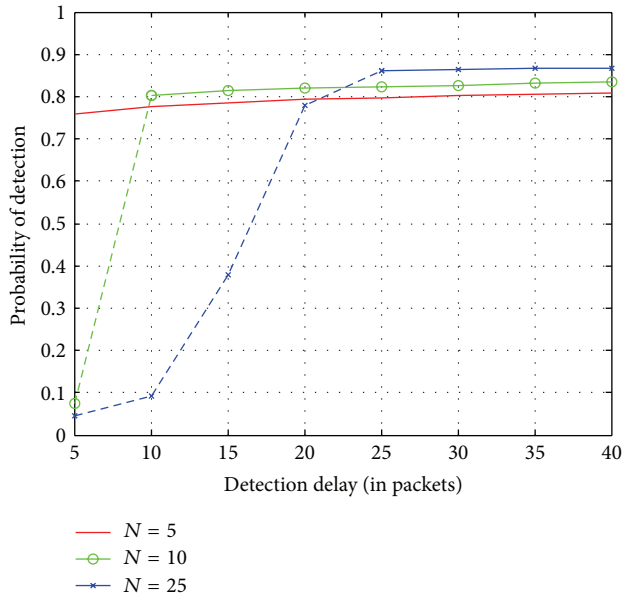

Figure 7: Variation of detection probability with N_D for a single antenna ($M = 1$) mode at $\alpha = 0.05$. $N_T = 25$. N_D is equal to N for each curve. The dashed segments correspond to points where $N_D < N$. Longer delays result in only marginal improvements in detection. Larger N improves performance, but the minimum required detection delay is longer for larger N's.

N being less than the detection delay can be observed by the dotted lines in Figure 7 where the detection performance is significantly deteriorated.

The false alarm rate, as a function of the number of friendly transmissions from T before I takes over, is shown in Figure 8. As one would expect, the chances of raising a false

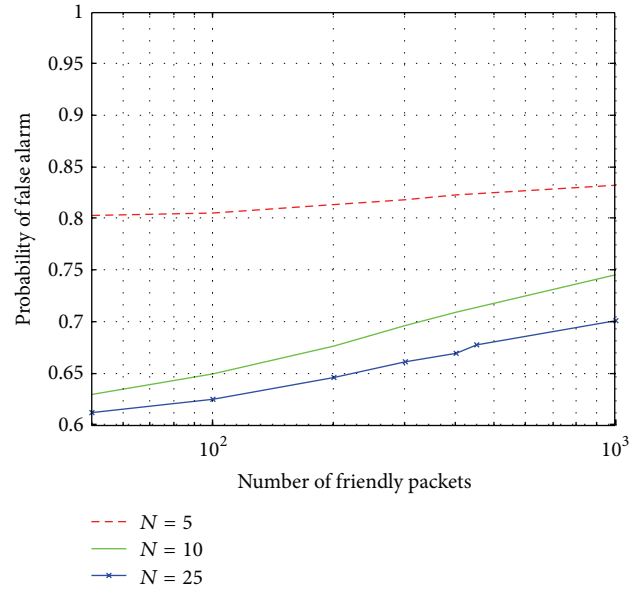

Figure 8: Variation of α with N_F for a single antenna ($M = 1$) mode at $\beta = 0.05$. $N_T = 25$. N_D is equal to N for each curve. Longer number of transmissions from T increases the probability of false alarms. Larger N improves performance due to better σ_0 estimates.

alarm rises with more friendly packets. A larger N results in a better estimate for σ_0 during the training phase. Additionally, it will yield a value for $\sigma(\mathbf{h})$ that is closer to the true σ_0 as well. Thus, the probability of $L(\mathbf{h})$ to exceed γ picked based on the estimated σ_0 will be lower and hence α improves with N.

To summarize the preceding trends, higher N lowers α while improving detection rates. Though a longer detection delay can help detection rates, in practice it is undesirable to have such long delays. However, due to the marginal difference between the σ values for the T − R and T − I links, it is challenging to obtain acceptable detection rates while keeping the false alarm rates very low when using a single mode antenna system. Hence, we resort to multimode antenna systems.

6.2. Multiple Antenna Modes. We begin our analysis of the multiple antenna mode case with Figure 9 which shows the DET curves achievable through the combination of channel information corresponding to multiple antenna modes. For each incoming packet, $L(\mathbf{h})$ is computed as in (7) based on the channel information corresponding to the chosen M configurations from which subsequent detection rates and false alarm rates are computed. It can be clearly seen that the detection rate significantly improves with the number of modes for a given α. Referring again to Figure 6 and Table 3, it can be observed that the maximum percentage difference between σ's among the different antenna modes increases with M. This is by virtue of the fact that different antenna modes will exhibit different σ values and hence the probability that the difference between σ_0 and σ_1 is very small for all the modes will be lower. Thus, modes that exhibit a larger difference in σ will contribute more to the GLRT

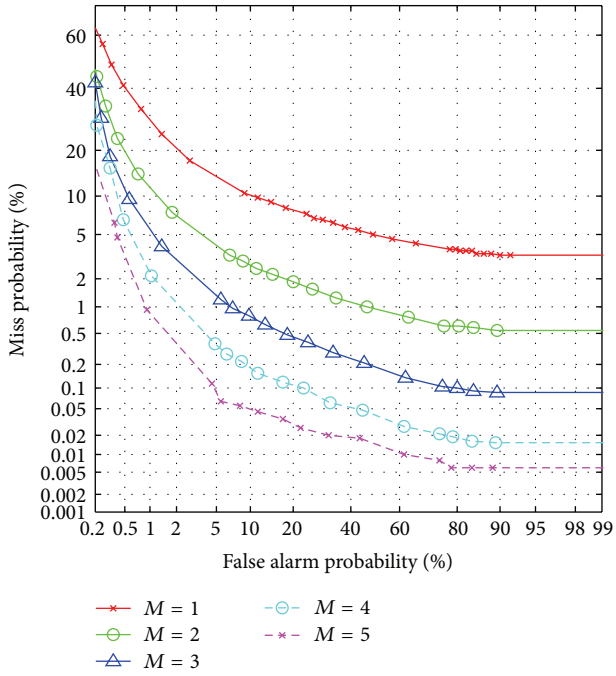

FIGURE 9: Average DET curves for a multiple antenna modes for $N = N_D = 10$. $N_T = 25$. For a given α, β decreases with increasing number of antenna modes. Acceptable levels of β can be achieved at low α levels by using multiple antenna modes.

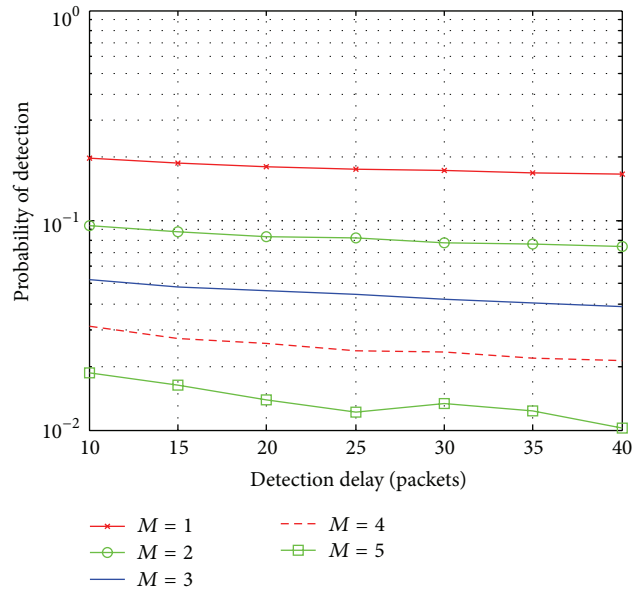

FIGURE 10: Variation of detection probability with N_D for multiple antenna modes at $\alpha = 0.05$. $N = N_D = 10$. $N_T = 25$. As observed in Figure 7, longer delays result in only marginal improvements in detection. More antenna modes however results in better detection rates without requiring longer detection delays.

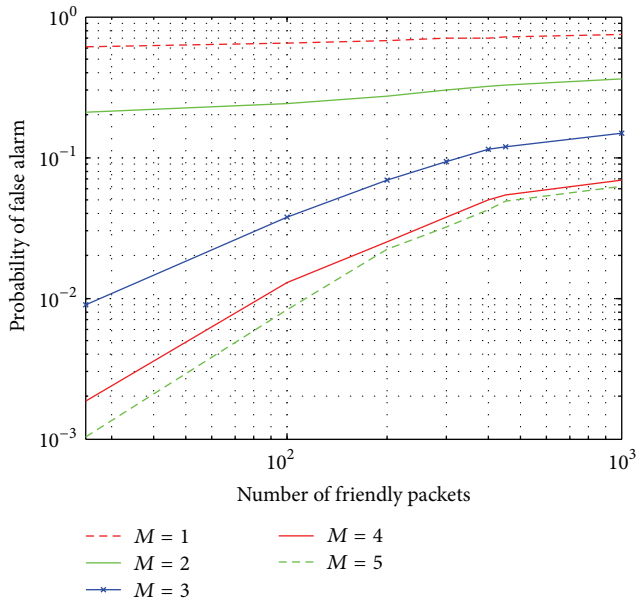

FIGURE 11: Variation of α with N_F for multiple antenna modes at $\beta = 0.05$. $N_T = 25$. N_D is equal to N for each curve. α decreases with M.

resulting in better performance. Increasing M increases the probability of finding modes that exhibit a larger difference in σ's and hence performance significantly improves with M. Again, due to the lower value of N, a non-Gaussian trend is observed in the observed DET curves.

Figure 10 shows the achievable detection rates as function of detection delay for the different M values. Comparing this with Figure 7, it can be seen that the level of improvement achievable in detection rates is quite high with M than N. For example, increasing N from 10 to 25 results in a mere 5% improvement in detection when a single mode is used. Moreover, this improvement comes at the cost of a longer detection delay. By introducing an additional mode, β can be lowered from around 20% to 9% while keeping N and N_D at 10.

Figure 11 shows α as a function of the number of friendly packets. As described in step (2) in Section 6, α is defined as the probability that there will be at least one packet that exceeds the threshold γ during the friendly transmissions. Improvements in α is also observed with increasing M. Naturally false alarms increase with increasing friendly packets regardless of M. For relatively smaller values of N and a single antenna mode, when certain samples in $\mathbf{h}$ come from the tail region of the underlying Rayleigh distribution, the resulting estimate of $\hat{\sigma}_1$ can significantly diverge from σ_0 resulting in excursions of $L(\mathbf{h})$ above the threshold γ. However, when multiple antenna modes are employed, the probability that the channels corresponding to most of the modes belong to the tail region at any given instant is reduced. Therefore, at every time instant, the "well-behaved" modes help dampen the hikes in $\hat{\sigma}_1$ due to the "stray" modes and therefore help keep the excursions of $\hat{\sigma}_1$ above γ low and hence reduce the probability of false alarm.

We conclude this section by providing a list of key statistical measures for α and β that were observed for various values of K in 100 trials. These measures are shown in Table 4. It can be observed that the standard deviation is

Table 4: Key statistical measures for α and β observed during 100 trials ($M = 5$, $N = 25$, $N_T = 25$, and $N_D = 1$).

K	α/β	Std. Dev.	Mean	Min	P_{25}	P_{50}	P_{90}	P_{99}	Max
1.00	α	0.00009	0.00005	0.00000	0.00000	0.00000	0.00020	0.00020	0.00020
	β	0.00000	1.00000	1.00000	1.00000	1.00000	1.00000	1.00000	1.00000
1.05	α	0.00010	0.00007	0.00000	0.00000	0.00000	0.00020	0.00020	0.00020
	β	0.01350	0.83669	0.80566	0.82646	0.83809	0.85381	0.85977	0.85977
1.10	α	0.00009	0.00006	0.00000	0.00000	0.00000	0.00020	0.00020	0.00020
	β	0.01593	0.73663	0.70234	0.72422	0.73994	0.75811	0.77676	0.78477
1.20	α	0.00010	0.00009	0.00000	0.00000	0.00000	0.00020	0.00020	0.00020
	β	0.01861	0.61567	0.57227	0.60215	0.61689	0.63965	0.64688	0.64863
1.40	α	0.00010	0.00014	0.00000	0.00000	0.00020	0.00020	0.00039	0.00039
	β	0.01630	0.44315	0.40430	0.43369	0.44453	0.46113	0.48057	0.48418
1.60	α	0.00010	0.00021	0.00000	0.00020	0.00020	0.00039	0.00039	0.00039
	β	0.01592	0.31338	0.27715	0.30293	0.30986	0.33535	0.35586	0.35820
1.80	α	0.00014	0.00026	0.00000	0.00020	0.00020	0.00039	0.00059	0.00059
	β	0.01575	0.22166	0.19629	0.21064	0.21768	0.24863	0.26113	0.26367
2.00	α	0.00015	0.00029	0.00000	0.00020	0.00020	0.00049	0.00059	0.00059
	β	0.01459	0.15741	0.13613	0.14590	0.15273	0.18145	0.19688	0.19707
2.25	α	0.00019	0.00037	0.00000	0.00020	0.00039	0.00059	0.00078	0.00078
	β	0.01265	0.10750	0.09004	0.09893	0.10361	0.12842	0.14385	0.14570
2.50	α	0.00024	0.00051	0.00020	0.00039	0.00059	0.00078	0.00098	0.00098
	β	0.00867	0.07441	0.06211	0.06992	0.07266	0.07998	0.10449	0.10488

Table 5: Pattern correlation coefficients between different modes of the LWA.

	Mode 1	Mode 2	Mode 3	Mode 4	Mode 5
Mode 1	1	0.73	0.42	0.10	0.06
Mode 2	0.73	1	0.82	0.27	0.07
Mode 3	0.42	0.82	1	0.55	0.11
Mode 4	0.10	0.27	0.55	1	0.56
Mode 5	0.06	0.07	0.11	0.56	1

limited to 1.5% for false alarm rates and to less than 1% for missed detection rates. The data shows that, for a given set of parameters, false alarm rates and missed detection rates are stable across multiple trials.

6.3. Which Modes to Choose? From the previous results it is clear that introducing multiple antenna modes improves the system's overall performance. However, these results do not provide insights into how to pick the mode combinations and most importantly if there is any benefit in increasing the number of modes beyond a certain level. Some insights into this problem can be found by analyzing Figure 12 and Table 5. Table 5 lists the spatial pattern correlation that exists between the radiation patterns corresponding to the different antenna modes used in the study. The best, worst, and average detection rates achieved by different individual mode combinations for $M = 2$ and $M = 3$ are shown in the figure. For $M = 2$, it is evident that the detection rate is a function of the antenna correlation coefficient. The best performance is achieved by the mode combination (5, 1) which also has the lowest correlation between patterns.

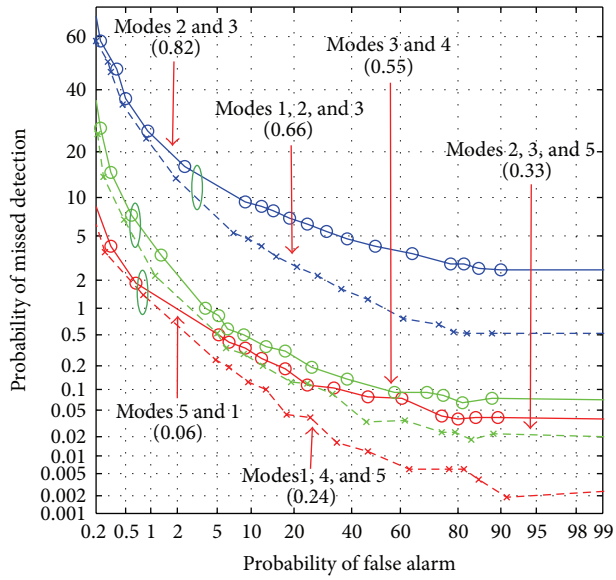

Figure 12: Average DET curves for different antenna mode combinations. $N = N_D = 10$. $N_T = 25$. Detection rates have a direct correlation with the correlation coefficient between the patterns of the employed antenna modes. For a given M, lower correlation coefficient between the antenna patterns results in better detection for a given α.

The combination with the highest correlation of 0.82 achieves the worst performance. Similarly, for $M = 3$, detection rates exhibit the same trend with respect to the average correlation between the different pair of modes within the combinations. Moreover, it can be seen that the performance achieved by

the best combination for $M = 3$ outperforms the $M = 5$ case as well.

The preceding behavior can attributed to the well-known phenomenon of decorrelated antenna patterns resulting in decorrelated channel realizations [28]. The information provided by more decorrelated channel realizations serves to improve the "quality" of $L(\mathbf{h})$ and hence enables the scheme to distinguish between T and I more accurately.

Based on these trends, two guidelines are suggested for picking the different antenna modes. Antenna modes should be picked such that the pattern correlation coefficient between the different modes should be kept as low as possible. Many reconfigurable antenna architectures exist that can generate patterns with a very low correlation coefficient between their modes [19, 29]. The second is that adding new modes will improve detection rates as long as the newly introduced mode does not diminish the average correlation coefficient among the modes. This can be seen by observing the different circled pairs of DET curves in Figure 12, where adding a new mode improves detection when the addition of the mode lowers the average correlation coefficient among the modes.

6.4. Effect of Training. The quality of training will have a significant effect on the performance of the scheme as the estimated σ_0 forms the basis for the likelihood ratio based on which it operates. Figure 13 shows the effect of the amount of training on the DET curves. As evidenced by the figure, longer training leads to better performance at the lower α regions as expected. But interestingly more training has a negative effect on system performance at the larger α regions. Recall that the threshold γ is computed as $KL_M(\mathbf{h})$ where $L_M(\mathbf{h})$ is the maximum of $L(\mathbf{h})$ observed during training. Longer training on average leads to marginally larger values for $L_M(\mathbf{h})$. At high α regions, $K \approx 1$ and hence the threshold γ is more sensitive to $L_M(\mathbf{h})$. Therefore, for a given α, keeping all other parameters constant while increasing only N_T results in an increased estimate of the threshold γ, which in turn deteriorates detection. Although the estimate of σ_0 does improve with N_T, the increase in $L_M(\mathbf{h})$ overweighs its benefit in the high α region leading to performance degradation. Nevertheless, meaningful utilization of this scheme will involve operating in the low false alarm region and therefore longer training will be still preferred.

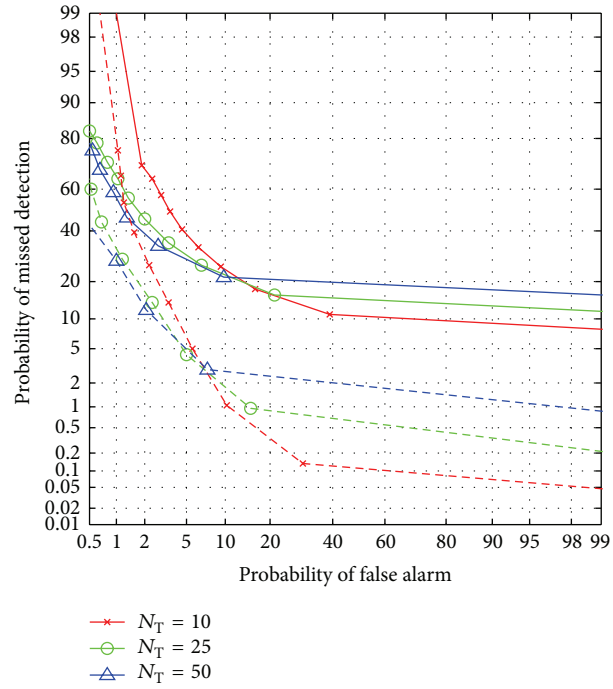

FIGURE 13: Average DET curves for $M = 1$ and $M = 5$ for different number of training samples. $N = N_D = 10$. Solid lines indicate $M = 1$ and dotted lines indicate $M = 5$. Longer training results in better detection at lower α regions. But the gains achieved from more training cannot match the gains achieved by employing more number of antenna modes.

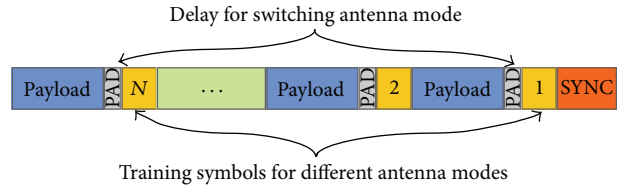

FIGURE 14: Extended transmit frame that can be used to obtain channel estimates for multiple antenna modes using a single packet transmission.

7. Practical Considerations

Some key practical issues need to be considered in order to make this scheme work in practice. The most critical issue is the problem of obtaining channel estimates over all the antenna modes on a packet-by-packet basis. Figure 14 shows the possible candidate for a frame structure at the physical layer that can be used to achieve this operation. An extended payload is interspersed with the necessary training symbols for each mode along with padded intervals to allow for switching the antenna to a new mode and resynchronization. High-speed switches with switching speeds in the order of picoseconds currently exist that can allow the antenna to switch modes at a rate compatible with current high data rate applications.

As noted previously, this scheme is proposed to complement existing higher level security protocols. Therefore, such protocols should continue to play their role in protecting the wireless link. An adaptive approach can be pursued when the GLRT triggers an alarm at the physical layer. When an alarm is raised by the physical layer scheme, the system can reconfigure the GLRT to operate in a point on the DET curve that prioritizes low missed detection over false alarms. Subsequent alarms should be handled by the upper layer authentication protocols such as 802.11i till it is ensured that the perceived threat does not exist after which point the GLRT can prioritize over false alarms again. Moreover, successfully adapting the alarm threshold will also rely on these reauthentication protocols.

Channel statistics may also gradually change with time which can lead to arbitrarily high false alarm rates. Periodic retraining can be implemented to keep the system performance within acceptable levels. Therefore, this scheme can benefit from more comprehensive training algorithms that continually update σ_0 based on packets that pass the intrusion detection test at the physical as well as upper layers.

8. Conclusion

An intrusion detection scheme that utilizes physical layer information based on a reconfigurable antenna was proposed. The intrusion detection problem was setup as a generalized likelihood ratio test under the assumption of Rayleigh fading channels for different antenna modes. The assumption was justified based on channel measurements gathered in an indoor environment using a network analyzer. The measurements were then used to study the performance of the scheme as a function of several control parameters available to the user. It was observed that large block sizes lower false alarm rates while yielding high detection rates as well. By utilizing multiple modes in a reconfigurable antenna concurrently in the likelihood function, it was shown that the detection rates can be improved and false alarm rates can be decreased while keeping the block size low. The pattern correlation coefficient that exists between the radiation patterns of the different antenna modes was shown to have a direct correlation with the resulting detection performance, with lower pattern correlation resulting in better performance. In networks with very limited or nonexistent security such as public WiFi spots, the proposed scheme can add a layer of security that can provide improved levels of protection against intrusion. In more secure networks operating in hostile environments, this scheme in conjunction with existing higher layer based security mechanisms can provide a much needed extra layer of security.

Future work to make the scheme more robust includes smart training algorithms that continuously train the system and keep the system up-to-date as well as algorithms that adaptively tweak the different control parameters to keep the system operating at the required performance level.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant no. 1028608.

References

[1] R. K. Nichols and P. C. Lekkas, *Wireless Security: Models, Threats, and Solutions*, McGraw-Hill, New York, NY, USA, 2001.

[2] W. A. Arbaugh, N. Shankar, Y. C. J. Wan, and K. Zhang, "Your 802.11 wireless network has no clothes," *IEEE Wireless Communications*, vol. 9, no. 6, pp. 44–51, 2002.

[3] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: the insecurity of 802.11," in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MobiCom '01)*, pp. 180–188, Rome, Italy, July 2001.

[4] A. Kitaura and H. Sasaoka, "A scheme of private key agreement based on the channel characteristics in OFDM land mobile radio," *Electronics and Communications in Japan, Part III*, vol. 88, no. 9, pp. 1–10, 2005.

[5] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, 2010.

[6] S. Yasukawa, H. Iwai, and H. Sasaoka, "Adaptive key generation in secret key agreement scheme based on the channel characteristics in OFDM," in *Proceedings of the International Symposium on Information Theory and its Applications (ISITA '08)*, Auckland, New Zealand, December 2008.

[7] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proceedings of the 15th Annual ACM International Conference on Mobile Computing and Networking (MobiCom '09)*, pp. 321–332, Beijing, China, September 2009.

[8] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, pp. 401–410, Alexandria, VA, USA, November 2007.

[9] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Transactions on Communications*, vol. 43, no. 1, pp. 3–6, 1995.

[10] M. Demirbas and Y. Song, "An RSSI-based scheme for sybil attack detection in wireless sensor networks," in *Proceedings of the International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM '06)*, pp. 564–568, Buffalo-Niagara Falls, NY, USA, June 2006.

[11] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2571–2579, 2008.

[12] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: using the physical layer for wireless authentication," in *Proceedings of the IEEE International Conference on Communications (ICC '07)*, pp. 4646–4651, Glasgow, UK, June 2007.

[13] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *Proceedings of the 5th ACM Workshop on Wireless Security (WiSE '06)*, pp. 43–52, Los Angeles, Calif, USA, September 2006.

[14] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "MIMO-assisted channel-based authentication in wireless networks," in *Proceedings of the 42nd Annual Conference on Information Sciences and Systems (CISS '08)*, pp. 642–646, Princeton, NJ, USA, March 2008.

[15] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in *Proceedings of the 13th Annual ACM International Conference on Mobile Computing and Networking (MobiCom '07)*, pp. 111–122, Montreal, Canada, September 2007.

[16] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-selective Rayleigh channels," *IEEE Transactions on Wireless Communications*, vol. 8, no. 12, pp. 5948–5956, 2009.

[17] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *Proceedings of the 6th annual international*

conference on Mobile computing and networking (MobiCom 00), pp. 275–283, 2000.

[18] S. M. Kay, *Detection Theory*, vol. 2 of *Fundamentals of Statistical Signal Processing*, Prentice Hall, New York, NY, USA, 1998.

[19] D. Piazza, P. Mookiah, M. D'Amico, and K. R. Dandekar, "Experimental analysis of pattern and polarization reconfigurable circular patch antennas for MIMO systems," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 5, pp. 2352–2362, 2010.

[20] E. Butler, "Firesheep 2011," http://codebutler.com/firesheep.

[21] C. Oestges, D. Vanhoenacker-Janvier, and B. Clerckx, "Channel characterization of indoor wireless personal area networks," *IEEE Transactions on Antennas and Propagation*, vol. 54, no. 11, pp. 3143–33150, 2006.

[22] P. Pagani and P. Pajusco, "Characterization and modeling of temporal variations on an ultrawideband radio link," *IEEE Transactions on Antennas and Propagation*, vol. 54, no. 11, pp. 3198–33206, 2006.

[23] J. Medbo, J.-E. Berg, and F. Harrysson, "Temporal radio channel variations with stationary terminal," in *Proceedings of the IEEE 60th Vehicular Technology Conference, Wireless Technologies for Global Security (VTC '04)*, vol. 1, pp. 91–95, Los Angeles, Calif, USA, September 2004.

[24] J. Sijbers, A. J. Den Dekker, E. Raman, and D. Van Dyck, "Parameter estimation from magnitude MR Images," *International Journal of Imaging Systems and Technology*, vol. 10, no. 2, pp. 109–114, 1999.

[25] D. Piazza, M. D'Amico, and K. R. Dandekar, "Performance improvement of a wideband MIMO system by using two-port RLWA," *IEEE Antennas and Wireless Propagation Letters*, vol. 8, pp. 830–834, 2009.

[26] J. Sijbers, A. J. Den Dekker, P. Scheunders, and D. Van Dyck, "Maximum-likelihood estimation of rician distribution parameters," *IEEE Transactions on Medical Imaging*, vol. 17, no. 3, pp. 357–361, 1998.

[27] A. Martin, G. Doddington, T. Kamm, M. Ordowski, and M. Przybocki, "The DET curve in assessment of detection task performance," in *Proceedings of the 5th European Conference on Speech Communication and Technology (Eurospeech '97)*, vol. 4, pp. 1895–1898, Rhodes, Greece, 1997.

[28] A. Forenza and R. W. Heath Jr., "Benefit of pattern diversity via two-element array of circular patch antennas in indoor clustered MIMO channels," *IEEE Transactions on Communications*, vol. 54, no. 5, pp. 943–954, 2006.

[29] J. Kountouriotis, D. Piazza, K. R. Dandekar, M. D'Amico, and C. Guardiani, "Performance analysis of a reconfigurable antenna system for MIMO communications," in *Proceedings of the 5th European Conference on Antennas and Propagation (EUCAP '11)*, pp. 543–547, Rome, Italy, April 2011.