Hindawi Publishing Corporation
International Journal of Antennas and Propagation
Volume 2012, Article ID 545783, 11 pages
doi:10.1155/2012/545783

Research Article

A Reconfigurable Antenna-Based Solution for Stationary Device Authentication in Wireless Networks

Prathaban Mookiah and Kapil R. Dandekar

Department of Electrical and Computer Engineering, Drexel University, Philadelphia, PA 19104, USA

Correspondence should be addressed to Kapil R. Dandekar, dandekar@ece.drexel.edu

Received 17 October 2011; Accepted 10 January 2012

Academic Editor: Karim Y. Kabalan

Applying channel information for user authentication is gaining attention in the area of wireless network security. Similarly, reconfigurable antennas capable of generating multiple decorrelated channel realizations have become increasingly popular in wireless systems. In this paper we propose and evaluate a channel-based authentication scheme that applies the capabilities of a pattern reconfigurable antenna for improved performance in user authentication. Field measurements of the channel frequency response employing such an antenna were performed to quantify the performance of the proposed scheme. Based on these measurements, we show the effect of correlation that exists between the different modes on the authentication performance. Furthermore, the performance gain that can be achieved by the scheme is studied as a function of the number of antenna modes. Offline mode analysis is performed to give a loose upper bound on performance while online mode analysis results are presented to quantify achievable authentication performance in realtime. A general guideline on how to choose the different elements of the decision metric in order to realize better performance for physical layer-based authentication schemes based on any diversity scheme is also developed.

1. Introduction

Large-scale proliferation of wireless technology coupled with the increasingly hostile information security landscape, is of serious concern. The fundamental broadcast nature of wireless data transmission aggravates the situation since unlike wired networks it introduces multiple avenues for attack and penetration into a network. Currently known security risks include denial of service attacks, man-in-the-middle attacks, MAC address spoofing attacks, client-to-client attacks, network injection and brute force attacks against access point passwords [1]. These risks will continue to increase in number and sophistication as wireless networks start to carry increasingly more sensitive information.

While several established protection mechanisms such as cryptography-based techniques and wireless intrusion prevention systems exist, each method has its own weaknesses and is susceptible to failure under different circumstances [2–4]. The resulting uncertainties have led to a significant paradigm shift in the design and implementation of wireless security in recent times, where an increasingly cross-layer approach is being pursued to protect wireless networks [5–10]. One such avenue for security has been to use the physical layer information to protect against intruders and attackers. The idea of using physical layer information to enhance security has been approached under two broad categories. The first category of work focuses on cryptography-based techniques that utilizes physical layer information to generate and share keys [11–14]. In the second approach, some form of the physical layer information associated with a device, such as channel frequency response or RSSI, is used as an identifier to differentiate between different devices and thus provide a mechanism for authentication [15–21].

In parallel to these developments, significant progress has been made in the design of reconfigurable antennas resulting in numerous designs that are reconfigurable in frequency, pattern, polarization, or a combination of these parameters [22]. For many new and emerging high data rate applications, pattern reconfigurable antennas are of special interest due to their ability to generate highly uncorrelated radiation patterns which can produce uncorrelated channel realizations in a multipath rich wireless medium for a given frequency [23]. Such antennas have gained widespread attention due to their ability to improve throughput and are gradually finding their way into commercial wireless systems. We contend that the uncorrelated nature of the channel realizations due to such an antenna also holds great potential to enhance physical layer based security schemes.

Previous work that explored the idea of physical layer information based authentication are based on the use of conventional antennas [16–20]. The main purpose of this paper is to demonstrate how the capabilities of reconfigurable antennas to generate decorrelated channels can be used to enhance physical layer information-based device authentication schemes for wireless systems. However, it should be noted that the proposed security scheme is not meant to be a replacement for existing higher layer security algorithms. Instead it leverages the capabilities of reconfigurable antennas to provide an additional layer of security for wireless systems. Moreover this paper also develops a general guideline on how to choose the different elements of the decision metric in order to realize better performance for physical layer-based authentication schemes based on any diversity scheme.

The paper is organized as follows: we start with an overview of the security problem we are trying to solve in Section 2. The underlying wireless channel model is described in Section 3. An identification metric to be used in our authentication scheme and the associated identity test is introduced next in Section 4. Section 5 describes our channel measurement methodology and the reconfigurable antenna used for this study. The correlation that exists in the measured channels is analyzed in Section 6 which will serve to explain the results of our analysis that is discussed in Section 7. We will discuss practical systems issues in Section 8 before concluding our paper.

2. The Problem of Device Authentication

The problem that is being addressed in this paper is one of establishing the identity of a stationary transmitting device in a wireless network. Spoofing attacks in network security encompasses a wide range of attacks that are based on one entity deceiving another to accept the attacking entity's identity to be something else. Many variants of this attack rely on the attacker monitoring the packet flow between the victims to obtain some sensitive information that identifies one or both of the victims. Information obtained thus serves as the launching pad for more sophisticated attacks. Due to the unbounded nature of the medium employed, such information can be obtained easily in a wireless network making them especially vulnerable to such attacks. Hence an additional mechanism for protection at the physical layer that can thwart such attacks can significantly enhance the security of a wireless network.

The proposed authentication scheme is based on the basic idea that the channel between the legitimate transmitter and receiver is difficult to replicate by a malicious entity. Different modes in a reconfigurable antenna present different views of this channel, and thus emulating all the channels seen by the different modes becomes a more difficult proposition for the intruder. Therefore associating a stationary device with a unique channel-based identifier or fingerprint could yield a robust authentication mechanism. It should be emphasized that this identifier utilizes the raw complex channel information rather than any abstracted power-based metrics such as RSSI. This allows the scheme to be more robust to attacks that try to circumvent it through simple power control. Moreover it should be noted that we do not attempt to localize the stationary transmitting device; rather, our goal is to find an unique identifier for each stationary transmitting device in the network based on its location. A data packet that generates the proper location fingerprint at the receiver can be then trusted to be arriving from the legitimate user and vice versa.

The problem scenario consists of three different players: a receiver (R), a transmitter (T), and an intruder (I). In practice R could correspond to a wireless access point while T and I correspond to two users trying to connect to R. In practice it is more likely that a wireless access point would be equipped with a comprehensive reconfigurable antenna system due to space and cost constraints. Therefore we assume that a reconfigurable antenna with N different configurations is employed only at R with T and I equipped with conventional omnidirectional antennas.

The problem evolves as shown in Figure 1. T and R initiate a connection at the outset of the session and are in the process of exchanging information Figure 1(a). At this stage, R measures and stores the channel between itself and T for N different antenna modes. I starts monitoring this exchange during this session until it obtains the identifying information corresponding to T Figure 1(b). After obtaining this information, I tries to pose as T to mislead R, Figure 1(c). The goal now is to enable R to distinguish between T and I at the physical layer based on the stored channel information. R makes this distinction by comparing the estimated channels for the N antenna modes for the incoming packet with the most recent copy stored in memory Figure 1(d). Based on the outcome of this test, R makes a decision on whether the packet arrived from T or not. It is assumed that R performs this comparison periodically and holds the most recent copy of the channel information that passes the test in its memory for the next comparison.

3. Channel Model

Unlike mobile phone-based services, a multitude of current and emerging wireless data services involve stationary terminals at both ends of the link. The terminal locations are usually fixed or movements are localized to a very small area near the seated user for the duration of a session. Temporal variations in such channels, termed as *nomadic mobility channels*, mostly arise due to movements of people and objects in the vicinity of the terminals. In this paper we limit our focus to such channels since they represent a common usage scenario for current high data

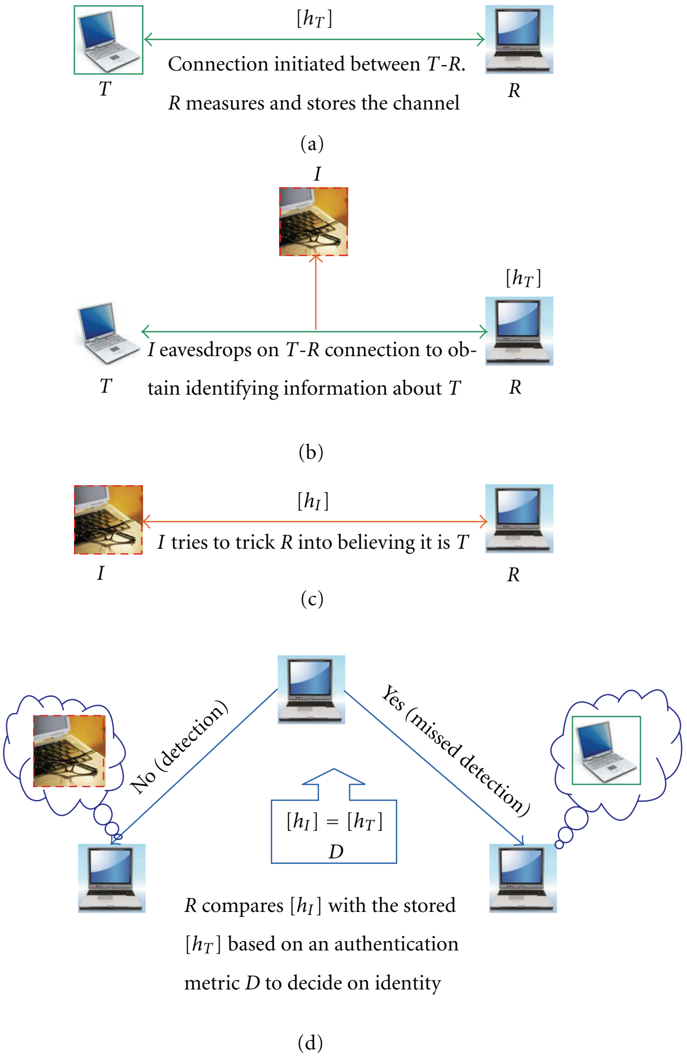

$[h_T]$
Connection initiated between T-R.
R measures and stores the channel
T
R
(a)
I
$[h_T]$
I eavesdrops on T-R connection to obtain identifying information about T
T
R
(b)
$[h_I]$
I tries to trick R into believing it is T
I
R
(c)
No (detection)
Yes (missed detection)
$[h_I] = [h_T]$
D
R compares $[h_I]$ with the stored $[h_T]$ based on an authentication metric D to decide on identity
(d)

Figure 1: Different stages (a)–(d) during the evolution of the authentication problem during a data transfer session between R and T.

rate applications. Challenges posed by large-scale terminal mobility is left for future study.

For a fixed link, the directional channel impulse response for an environment with L clusters and K rays per cluster is given by:

$$h\left(\phi^R,\phi^T\right)=\frac{1}{\sqrt{LK}}\sum_{l=0}^{L-1}\sum_{k=0}^{K-1}\beta_{kl}\delta\left(\phi^T-\phi_{kl}^T\right)\delta\left(\phi^R-\phi_{kl}^R\right), \quad (1)$$

where ϕ^T and ϕ^R are the transmit and receive angles, β_{kl} is the complex ray gain of the kth ray in the lth cluster, and ϕ_{kl}^T and ϕ_{kl}^R are their corresponding angles of departure and arrival. The narrowband channel impulse response corresponding to this cluster model is given by:

$$h=\iint_{-\pi}^{\pi}G_R\left(\phi^R\right)h\left(\phi^R,\phi^T\right)G_T\left(\phi^T\right)d\phi^T d\phi^R, \quad (2)$$

where $G_R(\phi^T)$ and $G_R(\phi^T)$ are the antenna gain patterns at the transmitter and receiver, respectively. If we assume an omnidirectional radiation pattern at the transmitter, substituting (1) in (2) simplifies to

$$h=\frac{1}{\sqrt{LK}}\sum_{l=0}^{L-1}\sum_{k=0}^{K-1}\beta_{kl}G_R\left(\phi_{kl}^R\right). \quad (3)$$

For a sufficiently narrowband channel, we can assume flat fading, and h will be given by a single complex number with $|h|$ distributed according to a Rayleigh or Ricean distribution. (3) quantifies the dependence of h on the antenna configuration at the receiver. For the kth receiver antenna configuration $G_k(\phi^R)$, we denote the corresponding channel by h_k.

Previous measurement campaigns on nomadic mobility channels have shown that for stationary terminals, the temporal channel variations are imparted primarily due to shadowing and scattering by the moving scatterers in the vicinity of the link [24–26]. Figure 2 shows the temporal variation in the measured frequency response corresponding to a single link for a single-antenna mode (Section 5). The entire

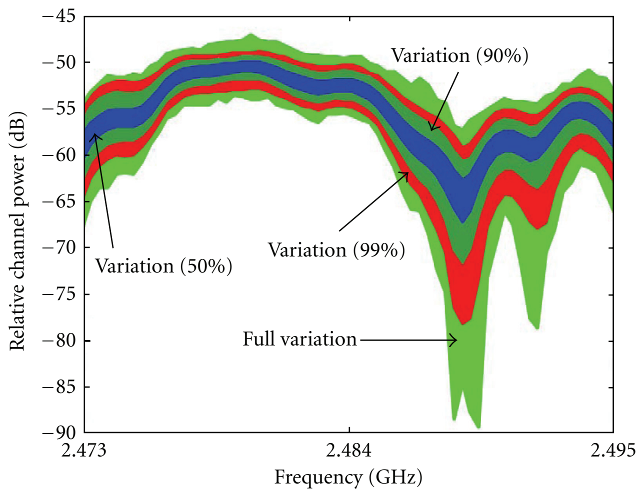


FIGURE 2: Temporal variation in channel frequency response for a single link with a single-antenna configuration over a period of 6 hours.

shaded region constitutes the total power variation in the channel over a period of approximately 6 hours during regular working hours when there was considerable human movement between the two ends of the link. The results follow similar trends that have been reported in earlier measurements where most of the variations are confined to narrow regions [24]. Consistent with the models proposed in the earlier works, we therefore model the channel as follows:

$$\hat{h}_k = X h_k + \epsilon + n, \tag{4}$$

where X denotes the shadowing imposed on the time invariant component h_k, ϵ is the additional small scale fading component induced by the scatterers, and n denotes receiver noise. ϵ and n can be modeled as a complex Gaussian process with 0 means and variances σ_ϵ^2 and σ_N^2, respectively. X is modeled as a random variable with a log-normal distribution with 0 mean and variance σ_S^2.

4. Identification Metric and Identity Test

In order to perform the channel comparison, R would require an authentication metric based on the channel information. The metric corresponding to the two channel realizations can be then used to make a decision about the transmitter's identity. We start with a decision vector that is given by:

$$\hat{\mathbf{h}} = \left[\left|\hat{h}_1\right| \quad \left|\hat{h}_2\right| \quad \cdots \quad \left|\hat{h}_N\right| \right]^T, \tag{5}$$

where $\hat{\mathbf{h}}$ is a vector that consists of channel amplitudes corresponding to different receiver antenna modes. The vector $\hat{\mathbf{h}}$ can be considered as the spatial signature or fingerprint associated with a terminal at a particular location. The angle between two spatial signatures $\hat{\mathbf{h}}_i$ and $\hat{\mathbf{h}}_l$ in the N dimensional space is now proposed as the test statistic to test if the signatures correspond to the same terminals:

$$\theta = \cos^{-1}\left(\frac{\hat{\mathbf{h}}_i \cdot \hat{\mathbf{h}}_l}{\left\|\hat{\mathbf{h}}_i\right\| \left\|\hat{\mathbf{h}}_l\right\|} \right), \tag{6}$$

where i and l denote the packet indices whose corresponding channel vectors are compared. Other candidates for a test statistic include the Euclidean distance between the channels [15–17, 19] and difference in total channel power. However the angle-based statistic has two properties that makes it attractive for a reconfigurable antenna-based authentication scheme. Depending on the environmental conditions, channels from certain modes may be stronger than the others. Such stronger channels tend to dominate the value of the computed test statistic in distance- or power-based metrics, rendering the information contained in the weaker channels useless. However the angle-based test statistic weights channels from all the modes equally, resulting in better utilization of all the available information. Second, the support of the test statistic is naturally limited ($0^\circ \le \theta \le 360^\circ$) and hence smoother distribution functions can be formed with limited number of training samples. This same property will also be desirable when offline learning techniques based on standard wireless channel models are employed to train the system in the future. Since the test statistic is the angle between the two spatial signatures, the vectors can be normalized without altering its value. Therefore θ can now be written as:

$$\theta = \cos^{-1}\left(\overline{\mathbf{h}_i} \cdot \overline{\mathbf{h}_1} \right), \tag{7}$$

$$\theta = \cos^{-1}\left(\sum_{n=1}^{N} \left|\overline{h}_{ni}\right| \left|\overline{h}_{nl}\right| \right), \tag{8}$$

where $\overline{\mathbf{h}_i} = \hat{\mathbf{h}}_i / \|\hat{\mathbf{h}}_i\|$ and $\overline{h}_{ni}$ denotes the elements of the normalized vector. Moreover a bar denotes the modified quantity after normalization in the proceeding discussion. The duration of shadowing is long compared to the packet transmission times and considered to be constant for all antenna configurations at any channel estimation period. Therefore at time instant i, the channel corresponding to a terminal is given by:

$$\overline{\mathbf{h}}_i = \begin{bmatrix} \left|\overline{X_i}\overline{h_{i1}} + \overline{\epsilon_{i1}} + \overline{n_{i1}}\right| \\ \left|\overline{X_i}\overline{h_{i2}} + \overline{\epsilon_{i2}} + \overline{n_{i2}}\right| \\ \vdots \\ \left|\overline{X_i}\overline{h_{iN}} + \overline{\epsilon_{iN}} + \overline{n_{iN}}\right| \end{bmatrix}. \tag{9}$$

From (9) and (8), the angle between this vector and another spatial signature at time instant l is given by:

$$\theta = \cos^{-1}\left(\sum_{n=1}^{N} \left|\overline{X_i}\overline{h_{in}} + \overline{\epsilon_{in}} + \overline{n_{in}}\right| \left|\overline{X_l}\overline{h_{ln}} + \overline{\epsilon_{ln}} + \overline{n_{ln}}\right| \right), \tag{10}$$

$\overline{X_i}\overline{h_{in}} + \overline{\epsilon_{in}} + \overline{n_{in}}$ involves the sum of a log-normal random variable and a normal random variable for which a tractable closed form pdf expression does not exist. Therefore we will resort to empirical density functions for θ obtained from measurements in our analysis.

However, previous studies have shown that that the variable component ϵ is usually between 20 to 50 dB lower than the static component for majority of the time [24]. Therefore for a simpler case where $|\epsilon + n| \ll |Xh|$, $\hat{h}_n$ can be written as:

$$\begin{aligned} \hat{h}_n &\approxeq X h_n, \\ \mathbf{h}_i &= X_i\Big[|h_{i1}| \quad |h_{i2}| \quad \cdots \quad |h_{iN}|\Big]. \end{aligned} \tag{11}$$

Normalizing $\mathbf{h}_i$ removes the effect of X_i and can be written as:

$$\begin{aligned} \bar{\mathbf{h}}_i &= \Big[\left|\overline{h_{i1}}\right| \quad \left|\overline{h_{i2}}\right| \quad \cdots \quad \left|\overline{h_{iN}}\right|\Big], \\ \theta &= \cos^{-1}\left(\sum_{n=1}^{N}\left|\overline{h_{in}}\right|\left|\overline{h_{ln}}\right|\right), \end{aligned} \tag{12}$$

which is the "true" angle between the two channels corresponding to the two locations from which packets i and l originated.

Given the authentication metric θ, the problem of classifying the transmitter now becomes a hypothesis testing problem. We pick the null hypothesis $\mathcal{H}_0$ to be that the incoming packet is from the same legitimate transmitter T and the alternate hypothesis $\mathcal{H}_1$ to be otherwise. Denoting the transmitter corresponding to $\mathbf{h}_i$ as $T(\mathbf{h}_i)$, the test can be written as:

$$\begin{aligned} \mathcal{H}_0 &: T(\mathbf{h}_i) = T(\mathbf{h}_l), \\ \mathcal{H}_1 &: T(\mathbf{h}_i) \neq T(\mathbf{h}_l). \end{aligned} \tag{13}$$

The conditional probability distributions of the authentication metric θ and the corresponding cumulative distribution functions will be denoted as follows:

$$\begin{aligned} \mathcal{H}_0 &: p_\theta(d \mid \mathcal{H}_0), \phi_0(\theta), \\ \mathcal{H}_1 &: p_\theta(d \mid \mathcal{H}_1), \phi_1(\theta). \end{aligned} \tag{14}$$

For a given false alarm rate α a threshold λ can be found such that

$$\begin{aligned} \alpha &= p_\theta(\theta > \lambda \mid \mathcal{H}_0) \\ &= 1 - \phi_0(\lambda), \\ &\Longrightarrow \lambda = \phi_0^{-1}(1 - \alpha). \end{aligned} \tag{15}$$

The probability of missed detection β can be defined for this threshold as:

$$\beta = p(\theta < \lambda \mid \mathcal{H}_1) = \phi_1(\phi_0^{-1}(1 - \alpha)). \tag{16}$$

For a given authentication metric θ we can now form estimates for α and β.

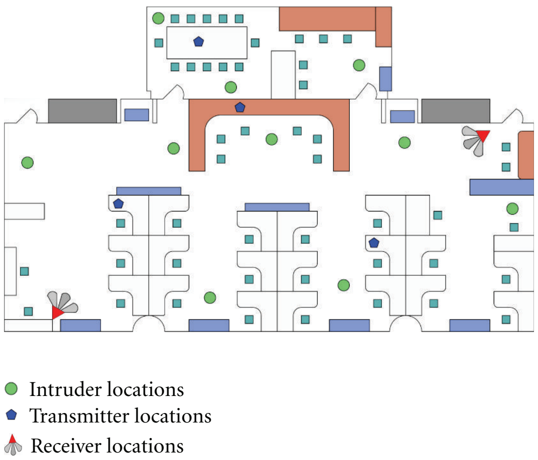


FIGURE 3: 2D CAD model of test environment. Test locations of R, T, and I are indicated. The reconfigurable antenna's beams were approximately oriented at R as shown in the diagram.

5. Measurement Setup and Reconfigurable Antenna

Channel measurements to evaluate the performance of the reconfigurable antenna-based user identification scheme were performed using a four-port vector network analyzer (VNA) (Agilent N5230A) by measuring S_{21} between the transmitter and receivers. The location chosen for the measurements was a medium-sized laboratory on Drexel University campus. The laboratory is 20 m long, 8 m wide, and 4 m high. The lab has a back room separated from the main lab by a plaster wall and several cubicles segmented by metallic walls and has other typical laboratory furniture, electronic equipment, and cabling scattered throughout the room. The measurement layout and setup is shown in Figure 3. T and I locations were chosen so that there were a combination of both LOS and NLOS links. R was equipped with the reconfigurable antenna to be described shortly. T and I were equipped with omnidirectional whip antennas. The antenna at the receiver was mounted at a height of 2.5 m while the antennas at the transmitters were mounted at the desk level of approximately 0.75 m.

The frequency was swept over a 22 MHz bandwidth centered at 2.484 GHz which corresponds to channel 14 of the IEEE 802.11n standard. 64 evenly spaced frequency samples were measured over this bandwidth. Two locations for R and four locations for T were chosen yielding a total of eight links. For each of these links, ten different I locations were considered. For each (R, T, I) pair, channels corresponding to the T-R and I-R links were measured for 5 different antenna configurations at R every 10 seconds for a total of 1000 samples. The time to complete each sweep was automatically set by the VNA to 130 msec. Due to speed limitations in the control board for changing antenna modes, a 0.25 second delay was introduced while switching between different antenna modes. Measurements were taken over

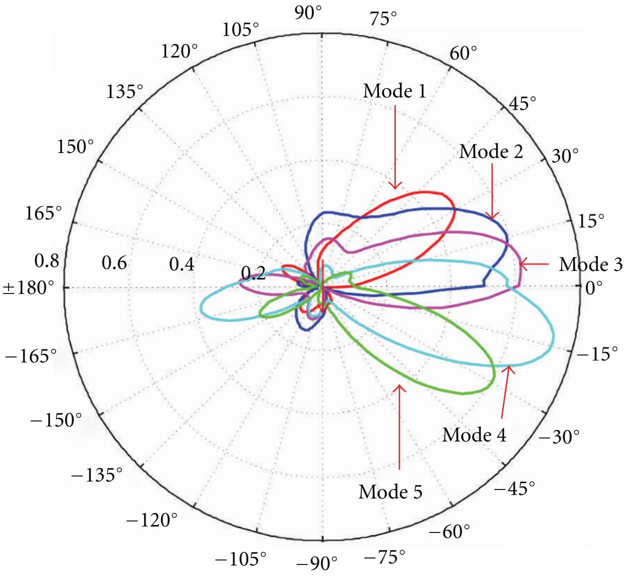


Figure 4: Radiation patterns of the LWA in the elevation plane (corresponds to the plane of the 2D model defined in Figure 3) for the 5 different configurations used in our measurements. Patterns are vertically polarized for all modes.

several days during both morning and evening hours when the human traffic was moderate and low, respectively.

The reconfigurable antenna used in this work is a two-port microstrip composite right/left-hand (CRLH) transmission line leaky wave antenna (LWA) which is an antenna design inspired by metamaterial transmission lines [27]. Pattern reconfiguration in this antenna is achieved by varying the right and left handed capacitances of a leaky CRLH transmission line by means of varactor diodes placed on the structure. The phase constant of the unit cells that constitute the antenna is changed by varying the bias voltage on the varactor diodes which results in beams directed in different directions for a fixed frequency of operation. The patterns in the elevation plane for the five modes used in this study are shown in Figure 4. The choice of this antenna is justified by its ability to electrically steer the antenna beam while having a significantly compact form factor.

6. Channel Correlation

The N elements of the decision vector $\hat{\mathbf{h}}$ correspond to channel estimates for the different antenna modes used in the reconfigurable antenna (i.e., this scheme is based on exploiting pattern diversity). However, we could devise a similar scheme by utilizing channel coefficients corresponding to N different frequencies (frequency diversity) or spatial snapshots (spatial diversity). In this section we will empirically quantify the amount of correlation that exists between the elements in $\hat{\mathbf{h}}$ for different diversity schemes.

Table 1: 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

The pattern correlation coefficient between radiation patterns corresponding to antenna modes i and j is defined as [23]:

$$\rho_{i,j} = \frac{\int_{4\pi} E_j(\Omega) E_i^{\dagger}(\Omega) d\Omega}{\sqrt{\int_{4\pi} |E_i(\Omega)|^2 d\Omega \int_{4\pi} \left| E_j(\Omega) \right|^2 d\Omega}}, \tag{17}$$

where $E_i(\Omega)$ is the radiation pattern for the ith mode and † denotes complex conjugation. The correlation coefficients generated by this definition between azimuthal patterns for five different modes used in our study is listed in Table 1.

Channel correlation coefficients with respect to the first antenna mode, averaged over the eight T-R links are shown in Figure 5. The first row of Table 1 is superimposed on Figure 5 to illustrate the influence of pattern correlation on the resulting channel correlations. Figure 5 follows the conventional wisdom that uncorrelated patterns lead to uncorrelated channels in rich multipath environments. The channel correlation coefficients with respect to the first measured frequency for the other frequencies are also shown in the figure. This result agrees with well known published results as well [28]. However, of interest to us is the comparison between the correlations arising from pattern and frequency correlations.

In our measured environment, approximately a 5 MHz frequency separation was required to achieve a correlation factor of 0.2 and 11 MHz separation for 0.1. However relying on frequency separation for channel decorrelation presents two problems. The first problem is that it is not straightforward to estimate the frequency separation required for a given level of decorrelation without proper knowledge of the RMS delay spread of the environment. Second, most wireless systems are band limited and our ability to span the frequency axis to achieve a required level of decorrelation may not be possible for many applications. On the other hand, using pattern diversity for applications requiring decorrelated channel realizations is a more “controlled” approach where antenna modes can be designed to exhibit a certain level of decorrelation which will translate to a similar level of decorrelation in the realized channels. For example with just two modes (mode 1 and 5) we are able to achieve correlation levels of less than 0.05. These correlation trends will serve to gain insights on some of the results to be discussed in the next section.

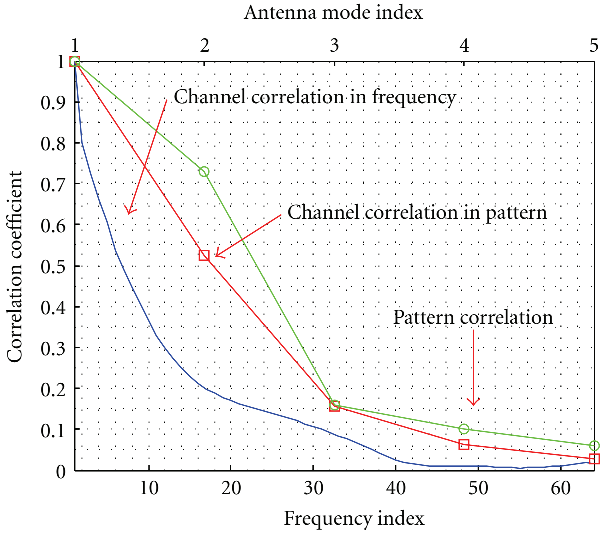


Figure 5: Pattern and channel correlation coefficients. The upper X axis corresponds to indices of antenna modes and lower X corresponds to indices of different frequencies. Correlations are defined w.r.t. to mode 1 and the first measured frequency, respectively.

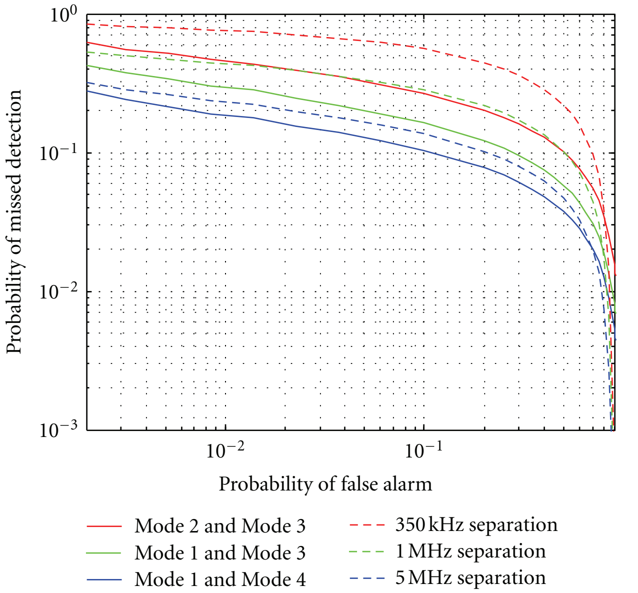


Figure 6: Observed β as a function of α for pattern and frequency diversity for $N = 2$. (The remaining 7 pairs for pattern diversity follow similar trends and were omitted to avoid clutter.)

7. Numerical Results

The measurements gathered as described in Section 5 were analyzed to quantify the performance of the reconfigurable antennas-based authentication scheme.

For a given N, α and β were obtained as follows.

(1) Pick a (R, T, I) combination and a frequency.

(2) Pick N antenna modes. (e.g., for $N = \mathfrak{N}$, there are $\binom{5}{\mathfrak{N}}$ possible selections.) $\hat{\mathbf{h}}$'s used in the following steps are formed by stacking the channels corresponding to the modes present in this combination.

(3) Compute $p_\theta(\theta \mid \mathcal{H}_1)$ by gathering θ's corresponding to T-R's $\hat{\mathbf{h}}$ at time instants i and $i + 1$ $(1 \leq i \leq 999)$.

(4) For different α determine the corresponding λ from this distribution.

(5) Compute $p_\theta(\theta \mid \mathcal{H}_1)$ by gathering θ corresponding to T-R $\hat{\mathbf{h}}$ at time instant $i - 1$ and I-R $\hat{\mathbf{h}}$ at time instant i $(2 \leq i \leq 1000)$.

(6) From the different λ computed in step (3), determine the corresponding miss rate β.

(7) Repeat steps (3–6) for all possible mode combinations.

(8) Repeat steps (2–7) for all possible (R, T, I) combinations.

(9) β is averaged over all the possible combinations repeated in steps (7) and (8).

Similarly for frequency diversity, different antenna modes instead of frequencies are picked in step (1) and N adjacent frequencies are chosen instead of antenna modes in step (2).

Figure 6 shows the ROCs obtained for three different mode pairs (out of ten possible pairs) when two modes are used for authentication. The worst performing mode corresponds to the mode pair of (2, 3). This pair can be seen to have the highest pattern correlation from Table 1. The best performing mode corresponds to the mode pair (1, 4) which is near the lowest correlation level observed among the radiation patterns. Similar trends can be observed when frequency diversity is employed as well. However, large frequency separations (more decorrelation) are required between the frequency points used to obtain good performance.

The reason for the detection rate dependence on the correlation between the elements in $\hat{\mathbf{h}}$ can be explained: let us assume two modes or frequencies that are highly correlated. Due to environmental conditions or by deliberate manipulation (such as transmit power control, trying out different locations), the intruder's channel corresponding to one mode may fall close to that of the legitimate transmitter. Now the probability of the other mode to fall close to that of the transmitter is also increased due to the high correlation and thus the addition of the new mode does not increase the quality of the spatial signature contained in $\hat{\mathbf{h}}$. However if the modes are decorrelated, the ability for another user to accidentally or intentionally match all the channels of another user becomes probabilistically more difficult. Thus more decorrelated elements in the decision vector $\hat{\mathbf{h}}$ lead to improvement in detection rates. It is therefore clear that higher levels of pattern correlation impede performance and hence the different antenna modes used in the scheme should have low decorrelation between them.

Figure 7 shows the performance of the pattern diversity-based scheme in detecting intruders for different values of N. For an α of 1% β decreases from 30% to 3% when N is increased from 2 to 5. For a given α, β decreases with N. As N grows higher, the probability for the intruder channel

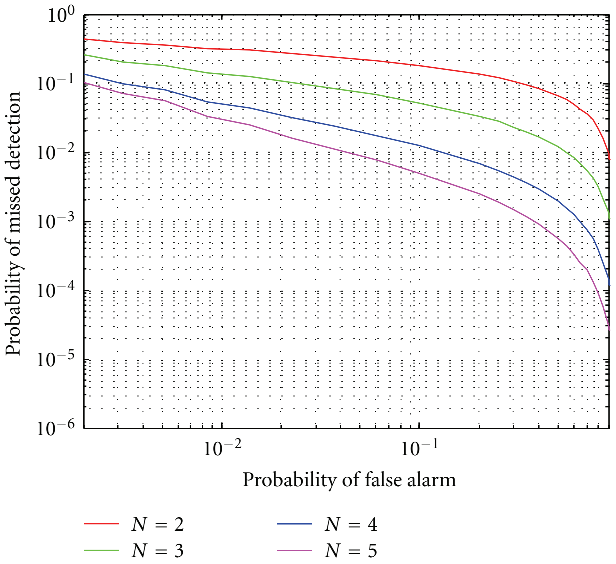


FIGURE 7: Observed β as a function of α for reconfigurable antenna based authentication at different values of N.

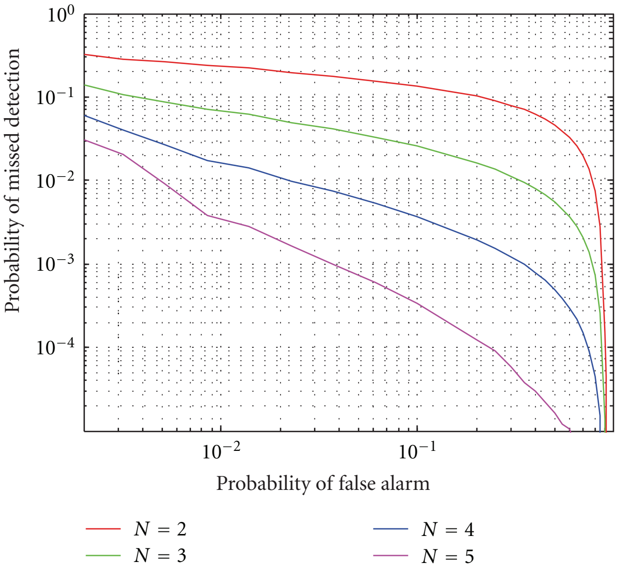


FIGURE 8: Observed β as a function of α when the average correlation between different elements in $\hat{\mathbf{h}}$ remains the same with increasing N. Elements correspond to frequency points spaced at 5 MHz.

to closely match all the channel elements in $\hat{\mathbf{h}}$ such that θ falls below threshold λ becomes low and hence detection rate improves.

It can be observed that the improvement in performance starts to reduce as N is increased. For example for an α of 1%, β improves by 15% when N goes from 2 to 3. This improvement reduces to 2% when N increases from 4 to 5. Introducing an additional mode into $\hat{\mathbf{h}}$ does not necessarily keep the average interelement correlation at the same level before its introduction due to the different levels of correlation that exists between different modes. Due to the limited number of modes used in our study, this is especially true for higher $N(\geq 4)$ since $\hat{\mathbf{h}}$ consists of highly correlated modes and their contribution to the detection rate is only minimal. Hence we observe the diminishing returns in performance improvement as the number of modes increases. To demonstrate this effect, we resort to frequency diversity where the multiple elements in $\hat{\mathbf{h}}$ are picked to have low correlation between each other and the average correlation does not change when a new element is introduced. We pick frequencies that are separated by 5 MHz (resulting channel correlation <0.2 from Figure 5) for different values of N. Figure 8 shows the resulting ROCs which indicates that as long as the average correlation among the elements is not diminished, introducing new modes or frequencies in $\hat{\mathbf{h}}$ will maintain the rate of improvement in detection rates. However this phenomena should not discourage the use of a reconfigurable antenna-based solution since a multitude of reconfigurable antenna geometries exist that can generate several modes with very low correlation between all their patterns [29].

Finally, the performance of this scheme when operating in an online mode was analyzed. During this analysis, the number of samples from T used for initially estimating $p_\theta(\theta \mid \mathcal{H}_0)$ is denoted by N_T. θ corresponding to all the $N_T(N_T - 1)/2$ samples are used to form this distribution from which λ was computed for different α. The most recent channel estimate to pass the authentication process was held in memory for the next test. Figure 9 shows the realized α during this online operation for two different values of N_T. The ideal curve for realized α versus designed α should be a straight line with gradient 1, since the designed and realized false alarm rates should be the same. However this behavior cannot be achieved perfectly in practice: the resolution of the support of $p_\theta(\theta \mid \mathcal{H}_0)$ is determined by the number of training samples used and therefore a smaller N_T results in coarse estimates for λ. This in turn will result in a significant variation between the designed and achieved false alarm rates. Therefore the realized α versus designed α curve can be expected to approach the ideal case as N_T increases which can be observed in Figure 9.

Achievable ROCs in real time with respect to the achieved α are shown in Figure 10. The observed trends with respect to N are comparable to that of the loose upper bound for performance obtained from the offline mode of analysis shown in Figure 7. Again it can be observed that due to better estimates for λ, higher N_T yields better detection performance for a given α. Interestingly, the ROC corresponding to $N_T = 10$ can be observed to terminate near the $\alpha = 0.02$ region. This is due to the fact that, with $N_T = 10$ at most 45 different θ's can be computed which sets the smallest resolvable false alarm rate to approximately 0.02. Similarly, though not shown in the figure, for $N_T = 25$, the curve will terminate near the region where $\alpha = 0.003$. Therefore using a larger value for N_T will (i) improve the agreement between designed and achieved false alarm rates,

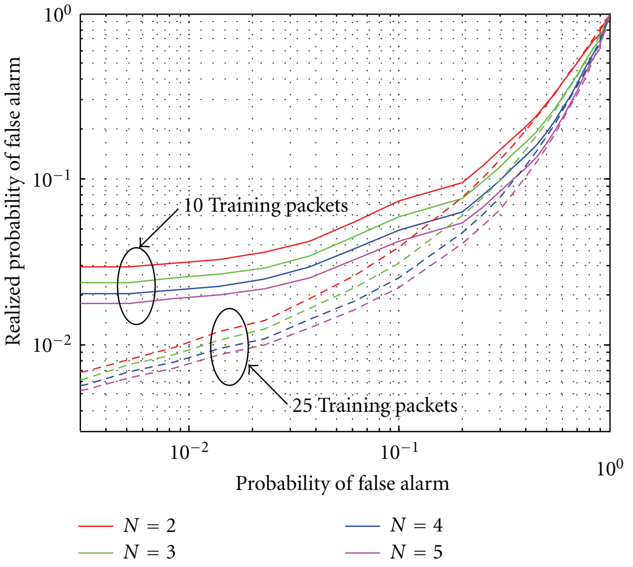


FIGURE 9: Realized false alarm rates as a function of designed false alarm rates during online mode of operation.

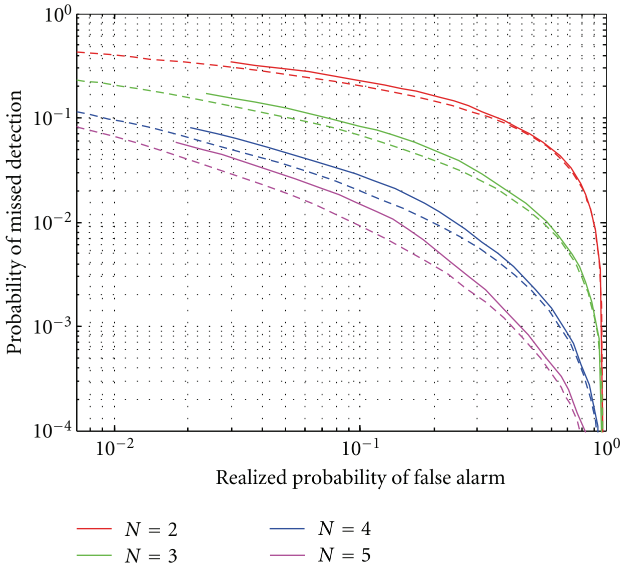
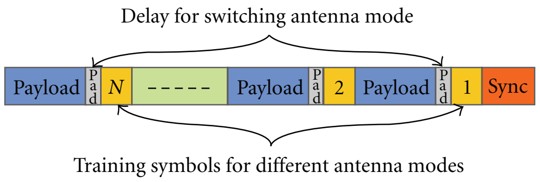


FIGURE 10: Observed β as a function of realized α during online operation. Solid lines correspond to 10 training packets and dashed lines to 25 training packets.

(ii) improve the detection rate for a given false alarm rate, and (iii) enable the user to set much lower values for α if required. Practical considerations regarding number of training packets are discussed in Section 8.


Delay for switching antenna mode
Payload
Pad
N

Payload
Pad
2
Payload
Pad
1
Sync
Training symbols for different antenna modes

FIGURE 11: Modified transmit frame that can be used to obtain channel estimates corresponding to different antenna modes during a single transmission.

8. Practical Considerations

There are several practical issues that need to be addressed in order to implement this reconfigurable antenna layer-based authentication system. We will briefly point out some of the issues and proposed solutions.

8.1. Channel Estimation. A key issue is on how the channel estimates can be obtained for all the different modes without degrading throughput and power consumption. Figure 11 shows a possible structure of a transmit frame for use with this security scheme. The antennas can cycle through the modes during the transmission of an extended packet during which the channel estimation is also performed for the different modes. Padding is inserted between the payload and next training sequence to leave sufficient time for the antenna to change modes. Switches with speeds on the order of picoseconds do exist currently and can lead to shorter pad lengths required while switching between modes.

8.2. Missed Detections/False Alarms. As in the case of any intruder detection systems, certain conditions may trigger too many false alarms such as significant changes in environmental conditions near the transmitter or receiver in our scheme. Upper-layer-based protocols can be designed to handle such situations. Similarly due to finite missed detection rates, intruder packets may go undetected. As noted previously, the purpose of this scheme is to add an additional layer of security to the system. Hence higher layer security measures should continue to play their part and should secure the system from such undetected malicious packets. Moreover the scheme is designed to thwart spoofing and man-in-the-middle attacks. Therefore it is assumed that the intruder will not commence transmission until the connection has been established between the legitimate transmitting ends during which initial training is performed and the scheme is initialized.

8.3. Training. As discussed in the previous section, more training packets will significantly enhance system performance. However training for long periods of time can have detrimental effects in terms of system throughput and power consumption. Therefore the amount of training required should be adaptively picked based on the required minimum false alarm rate as well as throughput requirements.

9. Conclusion and Future Work

A novel reconfigurable antenna-based physical layer authentication scheme for stationary devices was presented and analyzed. By taking channel measurements on a VNA it was shown that the ability to combine channel information from different antenna configurations can result in improved intruder detection. The relationship between the correlation among the elements in the decision metric and the authentication performance was analyzed. The results showed that the achieved performance improves as the average decorrelation that exists between the different antenna modes decreases. It was shown that by choosing modes that are highly decorrelated, high performance levels can be obtained even when operating in a system with very limited bandwidth. It was also seen that the performance of the scheme improves with more training in terms of detection rates as well as with realized false alarm rates approaching designed false alarms rates. Therefore next generation wireless systems that will be equipped with reconfigurable antennas can benefit from this scheme by employing the antennas to add an additional layer of security at the physical layer.

As a concluding remark, we would like to point out some research aspects of this scheme that are currently being pursued. As discussed in Section 4, the proposed scheme requires a decision threshold based on which the channel comparisons are made. Algorithms to adaptively pick and adjust the decision threshold during runtime is a topic for future research. Better authentication metrics than can be formulated by resorting to more complex signal processing techniques to extract the spatial features found within the channels arising from the different antenna modes is another topic for future research. The end goal of this research would be a complete system capable of employing the reconfigurable antenna adaptively to provide an additional layer of reliable and robust security.

Acknowledgment

This paper 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 Professional, New York, NY, USA, 2001.

[2] 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*, Rome, Italy, July 2001.

[3] W. A. Arbaugh, N. Shankar, and Y. C. J. Wan, "Your 802.11 wireless network has no clothes," in *Proceedings of the IEEE Wireless Communications*, vol. 9, pp. 44–51, 2001.

[4] K. Beaver and P. T. Davis, Understanding WEP Weaknesses, 2011.

[5] M. Debbah, H. El-Gamal, H. V. Poor, and S. Shamai, "Editorial: wireless physical layer security," *Eurasip Journal on Wireless Communications and Networking*, vol. 2009, Article ID 404061, 2009.

[6] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, Article ID 4543070, pp. 2180–2189, 2008.

[7] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '09)*, pp. 2613–2616, April 2009.

[8] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *Proceedings of the IEEE 15th Workshop on Statistical Signal Processing (SSP '09)*, pp. 417–420, Cardiff, UK, September 2009.

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

[10] J. E. Kleider, S. Gifford, S. Chuprun, and B. Fette, "Radio frequency watermarking for OFDM wireless networks," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '04)*, pp. V-397–V-400, May 2004.

[11] 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, November 2007.

[12] 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.

[13] 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.

[14] 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*, Auckland, New Zealand, December 2008.

[15] 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.

[16] 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, Los Angeles, Calif, USA, September 2007.

[17] 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, Scotland, June 2007.

[18] 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, Article ID 4570223, pp. 2571–2579, 2008.

[19] 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, Article ID 5351714, pp. 5948–5956, 2009.

[20] 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.

[21] 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, NY, USA, June 2006.

[22] J. T. Bernhard and C. Balanis, *Reconfigurable Antennas (Synthesis Lectures on Antennas and Propagation)*, Morgan and Claypool, San Rafael, Calif, USA, 2006.

[23] A. Forenza and J. R. W. Heath, "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.

[24] J. Medbo, J. E. Berg, and F. Harrysson, "Temporal radio channel variations with stationary terminal," in *Proceedings of the IEEE Vehicular Technology Conference*, May 2004.

[25] 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. 3198–3206, 2006.

[26] 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. 3143–3150, 2006.

[27] D. Piazza, M. D'Amico, and K. 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.

[28] H. Nakabayashi and S. Kozono, "Theoretical analysis of frequency-correlation coefficient for received signal level in mobile communications," *IEEE Transactions on Vehicular Technology*, vol. 51, no. 4, pp. 729–737, 2002.

[29] D. Piazza, P. Mookiah, M. D'Amico, and K. 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.