Securing Wireless Links at the Physical Layer Through Reconfigurable Antennas

Prathaban Mookiah*, John Kountouriotis, Renee Dorsey,
Boris Shishkin, and Kapil R. Dandekar
Drexel University, Philadelphia, PA, 19104
E-mail: {mprathap, jk368, ram54, bs44, dandekar}@drexel.edu

Introduction

Reconfigurable antennas that can be electrically modified to exhibit different radiation patterns and/or polarizations have been shown to significantly improve data rates. Such antennas outperform conventional antennas due to their ability to generate different channel realizations. Apart from their benefits in terms of spectral efficiency, their value could be greatly enhanced if they could be utilized for other system functions, such as security. The purpose of this paper is to demonstrate how the capabilities of reconfigurable antennas can be used to enhance physical layer-based security algorithms for wireless systems.

Wireless systems are inherently vulnerable to security breaches due to the unbounded nature of the wireless medium. Although cryptographic techniques have helped secure wireless links against intrusions such as spoofing attacks and man-in-the-middle attacks, it has been repeatedly demonstrated that a determined intruder can circumvent such measures relatively quickly. However security of a wireless network can be significantly boosted by assigning a unique location-based identifier to each device in the network since a device cannot exist at two different locations simultaneously. Based on the idea of using the wireless channel that exists between the transmitter and the receiver as the location identifier, several researchers have proposed different techniques to strengthen wireless network security [1–3].

Previous work that explored the use of channel information as a location identifier are based on the use of conventional antennas. However reconfigurable antennas that generate different radiation patterns can yield a more reliable identifier due to the smaller degree of correlation that exists between the different channel realizations. Motivated by these features of reconfigurable antennas, we investigate the security gains achievable in a system that uses such an antenna. Measurements made on a software defined radio (SDR) testbed that employs reconfigurable antennas are analyzed to quantify performance in differentiating between different transmitters at the receiver.

Problem Description and System Model

The problem consists of a receiver (R), a transmitter (T) and an intruder (I). To simplify our study, we consider a reconfigurable antenna with N_R different configurations only at R. T and R initiate a connection and are in the process of exchanging information when I tries to pose as T to mislead R. It is assumed that R periodically measures and holds the most recent copy of the channel information between itself and T for all different antenna configurations at the time I enters the scene. In reconfigurable antenna literature, this information can be obtained through direct training or by statistical means.

The goal is to enable R to distinguish between T and I at the physical layer based on the channel information corresponding to multiple antenna configurations. R makes this distinction by comparing the estimated channels for each incoming packet with the most recent estimate stored in memory. It is assumed that the channels are wide sense stationary such that probability distribution functions can be utilized in the decision making process. We note that this scheme would also require coordination with upper layers to handle issues such as repeated false alarms due to changes in the environment or movement of T or R.

978-1-4244-4968-2/10/$25.00 ©2010 IEEE

We consider a OFDM based communication system similar to IEEE 802.11a/g/n standards. The channel corresponding to each of the M (=52 in our system) data carrying subcarriers is modeled as a linear time-invariant filter. Through training over pilot symbols, we obtain a frequency domain estimate of the channel $\mathbf{h}$ where $\mathbf{h}$ is a $M \times 1$ vector whose elements contain a complex fading coefficient for each subcarrier. We define the $M \times 1$ vector $\mathbf{p}$ as containing the power gain of al the subcarriers.

$$\mathbf{p} = \begin{bmatrix} |h_1|^2 & |h_2|^2 & \dots & |h_K|^2 \end{bmatrix}^T \tag{1}$$

where h_j is the channel coefficient of the jth subcarrier.

Identification Metric

R requires an identification metric to differentiate between T and I. This metric is based on the vector $\mathbf{g}_l$ obtained from stacking $\mathbf{p}$ corresponding to any L ($\leq N_R$) antenna configurations and is given by:

$$\mathbf{g}_l = \begin{bmatrix} \mathbf{p}^1 & \mathbf{p}^2 & \dots & \mathbf{p}^L \end{bmatrix}^T \tag{2}$$

where $\mathbf{p}^i$ denotes the power gain vector corresponding to the ith antenna configuration. $\mathbf{g}_l$ would a vector of length LK. Let the $\mathbf{g}_l$ of a newly arriving packet be $\mathbf{g}_l^a$ and a stored estimate from previous packets be $\mathbf{g}_l^s$. The metric to decide if the packet corresponds to the same transmitter who initiated the connection or not is then given by:

$$D = \sum_{n=0}^{LK} |\mathbf{g}_{ln}^a - \mathbf{g}_{ln}^s| \tag{3}$$

where index n denotes the nth element of $\mathbf{g}_l$.

The channel estimates for each configuration are normalized in order to avoid the configurations leading to stronger channels out weighing the others in D so that the relative differences between all channels are preserved. This will prevent I from circumventing the scheme by simply tuning it's radiated power levels to match the D resulting from T.

A hypothesis test can be performed based on D to decide the identity of the transmitter. We pick the alternate hypothesis $\mathcal{H}_1$ to be that the incoming packet is from I and the null hypothesis $\mathcal{H}_0$ to be from T. Conditional probability density functions (pdf) for authentication metric D for the null and alternate hypothesis are given by $p_D(d|\mathcal{H}_0)$ and $p_D(d|\mathcal{H}_1)$ respectively. Based on the hypothesis test we can form estimates for the false alarm rate (α) and miss rate (β).

Measurement Setup and Analysis

The performance of the user identification scheme was evaluated by taking measurements using the wireless open-access resarch platform (WARP) [4]. The measurements were performed inside an atrium situated in the Bossone research building on Drexel University campus using 2 nodes. The measurement setup is shown in figure 1 which indicates the fixed R position along with the 41 measurement points which could serve as potential locations for both T and I. R was equipped with a two-port microstrip composite right/ left-hand (CRLH) leaky wave antenna (LWA) [5]. This antenna uses varactor diodes whose capacitances are controlled by 2 independent bias voltages in order to steer the excited beam to a required direction. For our work we use only one of the ports with the other port terminated with a 50Ω load. The measured radiation patterns corresponding to the 5 ($N_R = 5$) different configurations we used in our measurements are shown in figure 2. The second node corresponding to both T and I was equipped with a whip antenna that exhibits

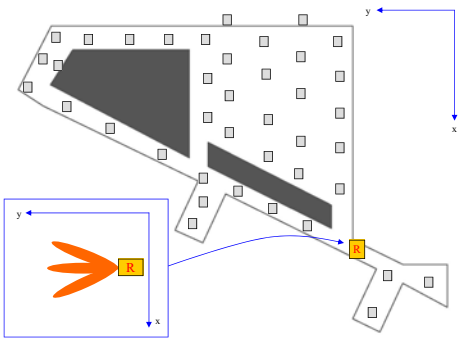

Figure 1: Layout of Measurement environment. The boxes denote the measurement points. Inset shows LWA's orientation.

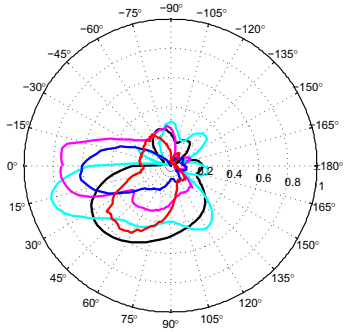

Figure 2: Radiation patterns of the LWA in the elevation plane for the 5 different configurations chosen for our measurements.

an omni-directional radiation pattern. For each measurement point, 25 channel snapshots were measured for each configuration.

The analysis was performed by considering each point as a T with the remaining 40 points treated as a I. Thus a total of 41 T-R links each with 40 different I-R links were studied. For each T-R link, D between subsequent snapshots of the T-R channel realizations was computed. The computed D's were gathered to form $p_D(d|\mathcal{H}_0)$ for the T-R link under consideration. Using this pdf, a threshold θ in D to distinguish between $\mathcal{H}_0$) and $\mathcal{H}_1$) was picked for a given α. $p_D(d|\mathcal{H}_1)$ was formed by considering D's between corresponding snapshots of the measured T-R channel and I-R channel for each of the 40 intruder points. Based on the computed θ and $p_D(d|\mathcal{H}_1)$, β was determined for the link. The final probability of detection for the system was computed by averaging β over all the T-R links. In a real time implementation, probability density functions can be computed off-line in a similar manner based on standard channel models and continually adjusted during online operation.

Results and Discussion

The receiver operating characteristics (ROC) obtained for the 5 "non-reconfigurable" antenna configurations, i.e., using each configuration of the reconfigurable antenna as if it were a conventional antenna, is shown in figure 3. It shows that the average detection rate performance does not change significantly between different antenna configurations. However as seen in figure 4, the detection rate approximately increases linearly with the number of configurations when multiple configurations are used. The detection rate improves to around 90% with 5 configurations from about 68% in the single configuration case. The improvements in detection rates are also higher for low false alarm rates; when 5 configurations are used in our system, detection rates were increased by up to 22% at an α of 1% which drops to 10% at an α of 10%. This implies that an authentication scheme based on reconfigurable antennas can provide a good first line of defense against intruders while not degrading the communications with the legitimate transmitter.

It may be argued that the improved performance when using reconfigurable antennas is due to the larger cardinality of the resulting power gain vector used to compute D. In order to study the effect of vector length, an analysis was performed by holding the power gain vector length a constant as the number of configurations was increased. In order to maintain a constant vector length, an evenly spaced subset of all the available subcarrier's channel coefficients were picked. Table 1 lists the number of subcarriers (M) for different number of antenna configurations (L). The resulting ROC shown in figure 5 confirms that it is in fact the decorrelation of the channels arising from different configurations in a reconfigurable antenna that leads to performance improvement. The reduction in the vector cardinality amounts to very little loss in performance.

It should also be noted that the different radiation patterns of the reconfigurable antenna we employed in this study are not highly de-correlated which results in channel realizations that are not highly de-correlated as well. This limits the improvement achieved by using the different configurations. Our ongoing research is studying the effects of antenna correlation on the performance of the described authentication scheme.

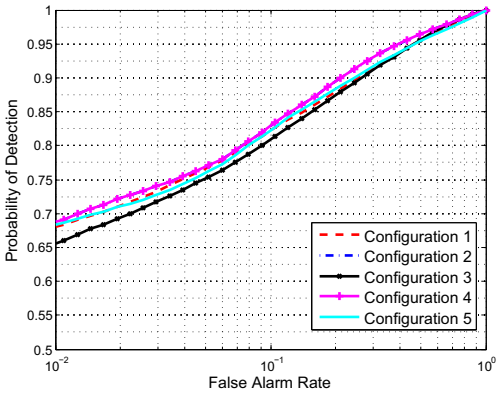

Figure 3: ROCs for the non-reconfigurable modes.

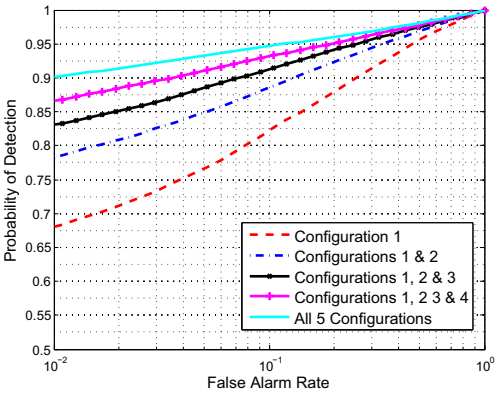

Figure 4: Observed ROCs for the reconfigurable modes.

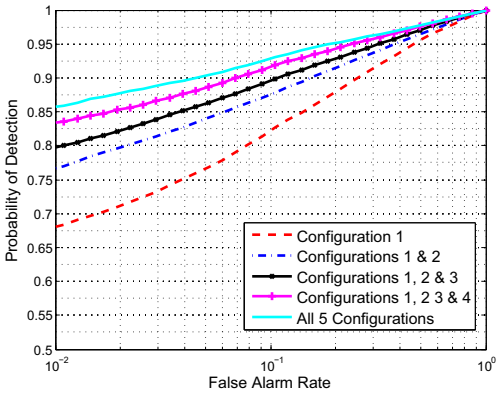

Figure 5: Observed ROCs when holding the authentication vector length a constant.

No. of Conf.	Subcarriers	$\lvert\mathbf{g}_p\rvert$
1	52	52
2	26	52
3	17	51
4	13	52
5	10	50

Table 1: Number of subcarriers picked for different number of configurations in order to hold the authentication vector length a constant.

Acknowledgement

This material is based upon work supported by the National Science Foundation under Grant No. CNS-0916480.

References

[1] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *WiSe '06: Proceedings of the 5th ACM workshop on Wireless security*. New York, NY, USA: ACM, 2006, pp. 43–52.

[2] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in *MobiCom '07: Proceedings of the 13th annual ACM international conference on Mobile computing and networking*. New York, NY, USA: ACM, 2007, pp. 111–122.

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

[4] WARP - wireless open-access research platform. [Online]. Available: http://warp.rice.edu/

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