Physical-layer Wireless Security of Reconfigurable Antennas in Line-of-sight Channels

Rashid Mehmood, Jon W. Wallace and Michael A. Jensen
Department of Electrical and Computer Engineering
Brigham Young University, Provo, UT, USA
E-mail: r.mehmood@ieee.org, wall@ieee.org, jensen@byu.edu

I. Introduction

Secure transmission is one of the most important aspects of wireless communications systems. In contrast to traditional cryptographic methods, physical layer security exploits the propagation channel to ensure security. It has been proven that a time-varying reciprocal channel can be used to generate secret keys which are secure even when an eavesdropper is located near one of the communicating nodes [1]. For line-of-sight (LOS) and slow-fading channels, reconfigurable aperture (RECAP) antennas have demonstrated their utility for physical layer security [2].

In this research, a RECAP refers to a very generic reconfigurable antenna consisting of a dense array of reconfigurable elements (REs) that can change the radiation properties of one or more apertures. RECAPs can provide physical-layer security in static environments by randomly changing the RE states, creating random radiation patterns and generating artificial fading. In our previous work, we have demonstrated both in terms of simulations [2] as well as experiments [3] that RECAPs can effectively enhance security in static multi-path channels. However, a potential weakness of RECAP-based physical security is an eavesdropper on the LOS path between the communicating nodes, allowing the eavesdropper to sample the same random channel used to generate the key. This critical LOS scenario is the topic of this paper.

Figure 1(a) shows the communications scenario considered in this work. Bob and Eve are equipped with a single half-wave ($\lambda/2$) dipole antenna, while Alice has a 5×5 square parasitic RECAP confined to an area of $1\lambda \times 1\lambda$. $\hat{h}_a$ and $\hat{h}_{a'}$ are estimates of the reciprocal channel at Bob and Alice, respectively, while Eve receives the estimated channels $\hat{h}_b$ and $\hat{h}_c$. Angular separation between $\hat{h}_a$ and $\hat{h}_b$ is represented by θ, where $\theta = 0^\circ$ corresponds to the case when Eve is in the LOS path between Bob and Alice. We have assumed a signal-to-noise ratio (ρ) of 10 dB in our analysis.

Since it is unknown to what extent the RECAP configuration affects security, we have also considered a circular RECAP as shown in Figure 1(b). Elements placed in the inner and outer circle have a radius of 0.25λ and 0.5λ respectively. For both square and circular RECAPs, the feed is placed at the center, while all other elements (hollow circles) act as REs. The number of states (N_{RS}) of REs used in simulations is chosen from measured results of a varactor-diode based RE presented in [3].

The goal of this study is to analyze the security of the LOS communications scenario, depending on the angular separation (θ) between $\hat{h}_a$ and $\hat{h}_b$. In this work, we change the states of REs randomly to generate the communications channels, and later corresponding secure bits are computed with respect to a certain θ.

II. Information Theoretic Analysis

Available key bits (I_{K}) represent the number of bits that can be generated per random observation of the channel and is defined as,

$$I_{\mathrm{K}} = \mathrm{E} \log_2 \frac{f(\hat{h}_a, \hat{h}_{a'})}{f(\hat{h}_a) f(\hat{h}_{a'})}, \tag{1}$$

where $\mathrm{E}\{\cdot\}$ is expectation, $f(\cdot)$ represents the probability density function (pdf) and quantities with $\hat{\cdot}$ represent estimated channel quantities.

Secure key bits I_{SK} represents the number of bits safe from the eavesdropper (Eve), defined as

$$I_{\mathrm{SK}} = I(\hat{h}_a; \hat{h}_{a'} | \hat{h}_b, \hat{h}_c) = \mathrm{E} \log_2 \frac{f(\hat{h}_a, \hat{h}_{a'} | \hat{h}_b, \hat{h}_c)}{f(\hat{h}_a | \hat{h}_b, \hat{h}_c) f(\hat{h}_{a'} | \hat{h}_b, \hat{h}_c)}. \tag{2}$$

The detailed algorithm for computation of I_{K} and I_{SK} is presented in [2]. Since the exact distribution of the channels is unknown, we have used the numerical expectation based approach to compute I_{K} and I_{SK}. Results of (1) and (2) are also compared with closed form expressions for the Gaussian case as presented in [1].

III. Analysis and Results

In order to compute (1) and (2) numerically, we have used $N = 10^6$ snapshots of the individual channels. An efficient hybrid approach is used to characterize the RECAP, where full-wave Numerical Electromagnetic Code (NEC) simulations are combined with network analysis, allowing the radiation pattern of the RECAP to be computed for arbitrary RE loading. Simple single-path far-field propagation is assumed between the nodes when computing the different channels. Note that Eve is in the far-field of Alice, so the impact of $\hat{h}_c$ on I_{SK} is almost negligible. The dominant effect will be from $\hat{h}_b$, and it is expected that the worst-case occurs when $\theta = 0^\circ$. Note that in Figure 1, the reference angle $\theta_\circ$ is the direction of channel $\hat{h}_a$. For a square RECAP I_{K} can vary significantly with respect to $\theta_\circ$. For this reason the results are averaged over the reference angles $\theta_\circ = [0^\circ, 5^\circ, ..., 45^\circ]$.

Figure 2(a) plots I_{K} for varying N_{RS} when Alice has a square RECAP. The curves corresponding to the numerical computation and the Gaussian approach are close to each

978-1-4673-5317-5/13/$31.00 ©2013 IEEE

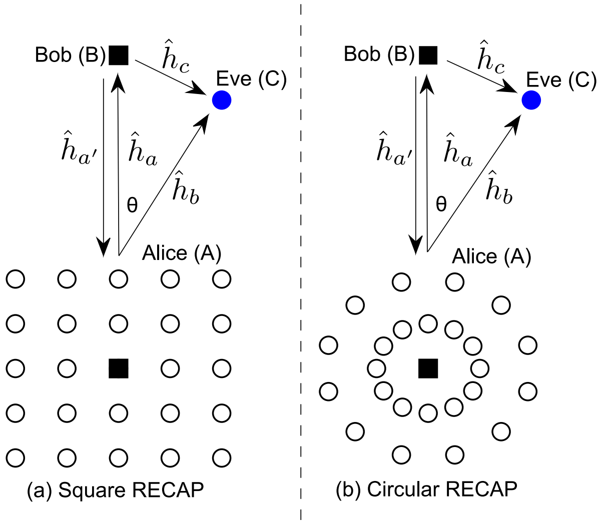

Fig. 1. Top view of nodes in the security simulations, where Bob and Eve have a single antenna and Alice has a RECAP with many programmable REs (hollow circles). Black squares show the location of Bob's antenna and Alice's feed, while the blue circle shows a possible position of Eve's antenna depending on θ.

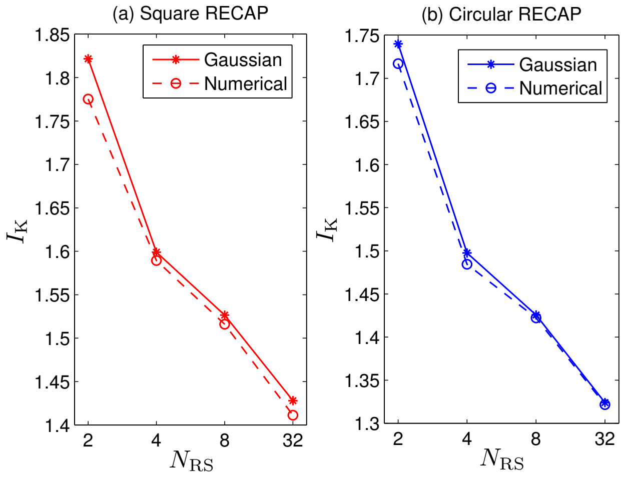

Fig. 2. I_{K} for varying N_{RS} using the numerical expectation method and the Gaussian approximation: (a) Alice having a square RECAP (b) Alice having a circular RECAP.

other, indicating that RECAPs can generate close to Gaussian random channels. In general, the Gaussian approximation upper bounds the numerical computation. I_{K} is maximized for $N_{\mathrm{RS}} = 2$, since extreme RE states appear to maximize the channel variance. Figure 2(b) plots I_{K} when Alice has a circular RECAP. Although the exact values of I_{K} are slightly different for the two configurations of the RECAP, the general trends are the same.

Figure 3 plots I_{SK} with respect to θ for a square RECAP, and as expected, $N_{\mathrm{RS}} = 2$ maximizes I_{SK}. Even for $\theta = \theta_\circ = 0°$ we observe that a small number of bits are secure, which is due to Eve's finite SNR. For $\theta \geq 0°$, I_{SK} increases almost linearly and later converges towards the corresponding I_K value. It is interesting to note that for an angular separation

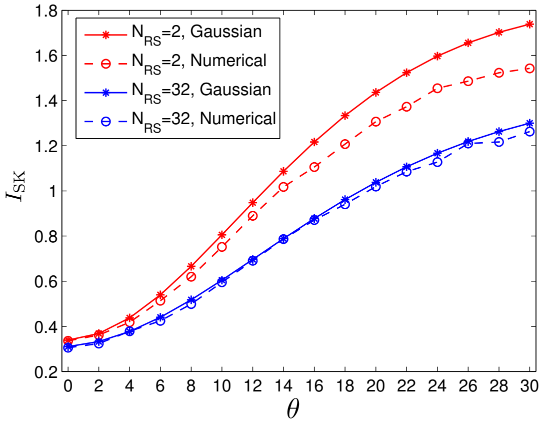

Fig. 3. I_{SK} for varying θ and N_{RS} using the numerical expectation method and the Gaussian approximation when Alice has a square RECAP.

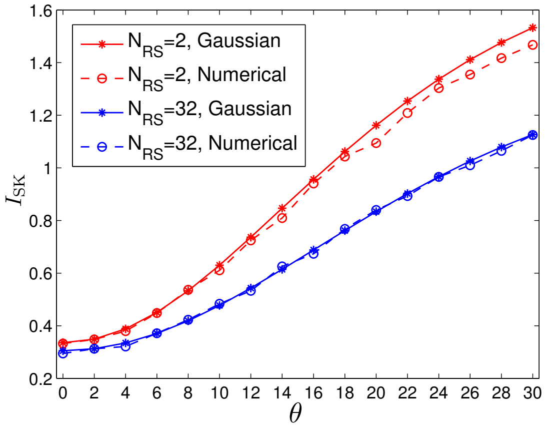

Fig. 4. I_{SK} for varying θ and N_{RS} the numerical expectation method and the Gaussian approximation when Alice has a circular RECAP.

of 30° approximately 90% of the bits are secure, while at $\theta = 10°$ approximately 40% of key bits are secure. Also, we observe that the gap between the numerical approach and the Gaussian approximation increases with θ for $N_{\mathrm{RS}} = 2$, which likely occurs from the lower N_{RS} value producing less Gaussian statistics, where this effect would be more prominent for high values of I_{SK}.

Figure 4 plots the corresponding results for a circular array. The general trends of curves are similar to the square array, emphasizing that exact configuration of parasitic RECAP does not appear to have a significant impact on security.

References

[1] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 381–392, 2010.

[2] R. Mehmood and J. W. Wallace, "Wireless security enhancement using parasitic reconfigurable aperture antennas," in *Proc. 5th European Conf. Antennas and Propagation (EUCAP)*, 2011, pp. 2761–2765.

[3] R. Mehmood and J. W. Wallace, "Experimental assessment of secret key generation using parasitic reconfigurable aperture antennas," in *Proc. 6th European Conf. Antennas and Propagation (EUCAP)*, 2012, pp. 1151–1155.