Experimental Characterization of Channel-Based Key Establishment Using Reconfigurable Antennas

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

***Abstract*—Generation of secret encryption keys from the reciprocal electromagnetic channel represents an emerging topic within the broad field of propagation channel research. This paper uses multi-antenna channel measurements to assess the potential performance of such techniques, with the emphasis on using a reconfigurable antenna element controlled by the channel sounder to create time-variation in the wireless channel that enables establishment of long encryption keys. The results demonstrate that reconfigurable antennas can significantly enhance the security, even when the eavesdropper antennas are adjacent to or surround one of the legitimate nodes.**

I. Introduction

Because electromagnetic propagation is reciprocal, if two radios use half-duplex communication to transmit training data to each other from which each estimates the channel transfer functions, the observed channel estimates will be approximately the same and therefore can be used to construct encryption keys [1]. Establishment of long keys requires collection of several channel estimates when either the propagation characteristics or the antenna responses (through reconfigurability) vary in time. The idea of using reconfigurable antennas to create increased randomness is a relatively new concept, and little work has appeared detailing the potential of this technology in practical applications.

The objective of this work is to use measurements of the multi-antenna propagation channel to study the potential of using reconfigurable antennas in secure key establishment. Analysis of the measured data reveals the conditions under which reconfigurable antennas provide good key generation rates and the level of security achieved using the approach in the presence of a proximate, multi-antenna eavesdropper. The results show that in a multipath channel, a highly-configurable antenna offers a significant increase in the number of key bits that can be securely established even when the eavesdropper's array surrounds the reconfigurable antenna.

II. Communication Scenario

Figure 1 shows the scenario considered in our analysis in which two legitimate nodes designated as *Alice* and *Bob* communicate in the presence of an eavesdropper *Eve*. Alice possesses a reconfigurable antenna consisting of a *feed* antenna placed at the center of a uniform $1\lambda \times 1\lambda$ grid with N_{RE} *parasitic* reconfigurable elements (REs) terminated in varactor-diode-based tunable reactances placed at other locations in the grid. Eve possesses an array of N_{E} elements that is assumed to surround Alice's antenna, while Bob has a single antenna.

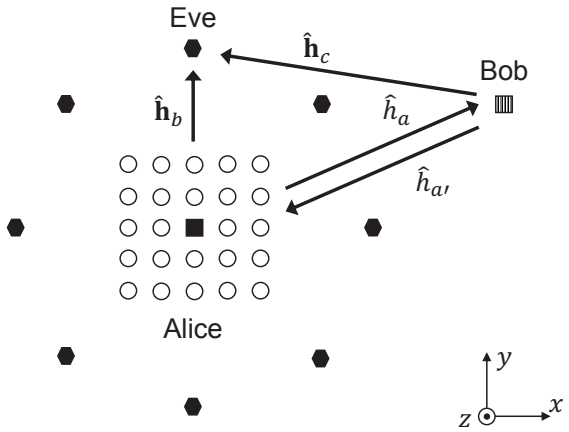

Fig. 1. Top view of the antenna arrangement in the security analysis, where Bob has a single antenna, Alice has a reconfigurable antenna, and Eve has an array of antennas surrounding Alice.

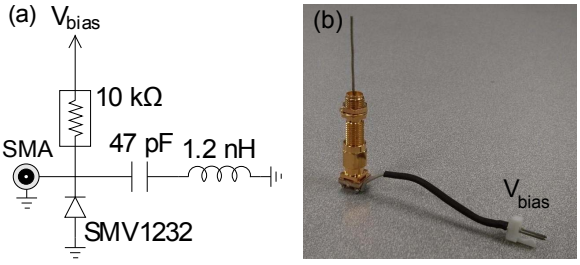

Fig. 2. RE circuit: (a) schematic, (b) completed RE with circuit board holding components, bias lead, and a monopole inserted into the SMA connector.

The estimated narrowband scalar channels at Bob and Alice are respectively denoted as $\hat{h}_a$ and $\hat{h}_{a'}$, while the vectors $\hat{\mathbf{h}}_b$ and $\hat{\mathbf{h}}_c$ respectively represent Eve's estimates of the multi-antenna channels from Alice and Bob.

Figure 2 shows the design of the varactor-diode-based RE used in measurements [2]. The tuning voltage V_{bias} is supplied by an FPGA-controlled circuit that generates N_{RS} unique uniformly-quantized bias voltages for each RE, with each bias voltage representing an RE *state*. The tuning circuitry is fabricated on the lower side of a small printed circuit board at the base of the SMA connector. In operation the bulkhead adapter attached to the wire monopole is fed through a ground plane with the SMA connector/tuning circuitry connected to the adapter below the ground plane.

978-88-907018-4-9/14/$31.00 ©2014 IEEE

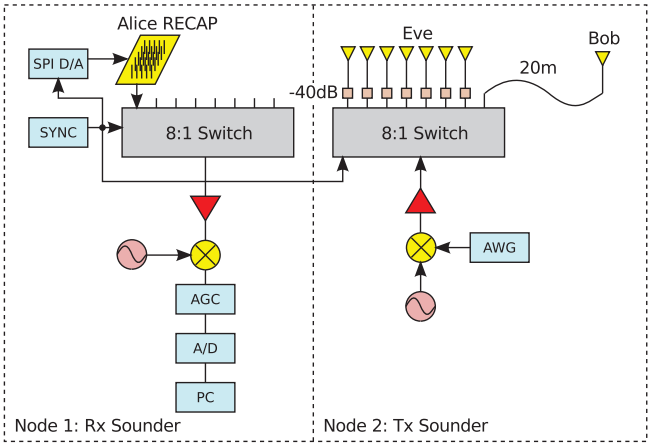

Fig. 3. 2-node measurement configuration used to measure channel responses for the legitimate nodes and eavesdropper.

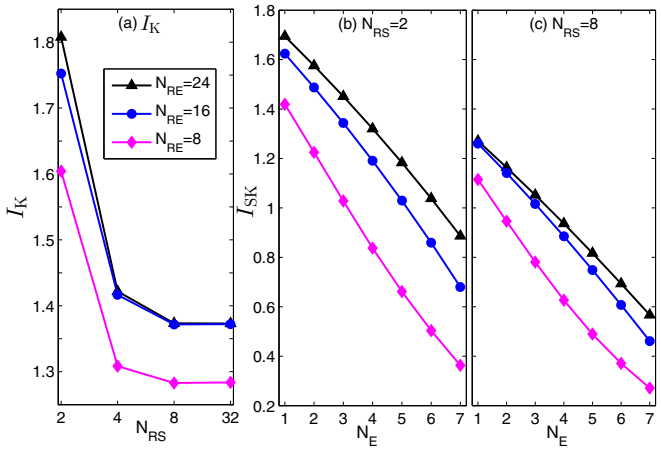

Fig. 4. Measured (a) I_{K} as a function of N_{RS} for different values of N_{RE} and (b)-(c) I_{SK} as a function of N_{E} for different values of N_{RE} and N_{RS}.

The mutual information I_{K} between the two channel estimates $\hat{h}_a$ and $\hat{h}_{a'}$ represents the *available key rate*, which is the maximum number of independent key bits that can be generated for each channel observation. Similarly, the *secure key rate* I_{SK} is the number of generated key bits per channel observation that are secure from Eve. Both can be computed from experimental observations of the channel using expressions provided in [3].

The experiments accommodate *2-node* measurements ($\hat{h}_a$ and $\hat{\mathbf{h}}_b$) or *3-node* measurements ($\hat{h}_a$, $\hat{\mathbf{h}}_b$ and $\hat{\mathbf{h}}_c$). However, our analysis shows that $\hat{\mathbf{h}}_c$ provides little information to Eve, and therefore most of the data is collected using the 2-node arrangement shown in Figure 3. The measurements use an 8×8 multiple-input multiple-output (MIMO) channel sounder with transmit signals consisting of eight frequency tones spaced at 10 MHz intervals from 2.515 to 2.575 GHz. The channel for each transmit-receive antenna pair is measured sequentially, with synchronization accomplished using Rubidium references and synchronization (SYNC) units. The reconfigurable antenna is connected to the MIMO channel sounder receiver, with the FPGA-based RE bias controller integrated with the sounder to allow synchronization between antenna switch states and RE states. Bob's antenna is connected to one sounder transmit port via a 20 m cable and Eve's antennas are connected to the remaining 7 transmit ports.

III. Results

Measurements were taken at four different locations within the Research I building on the Jacobs University Bremen campus, with Locations 1, 3, and 4 in different laboratories and Location 2 in a hallway. All measurements were collected over weekends or at night to reduce temporal variations. The measured results use 10^6 channel snapshots to allow good statistical representations and are averaged over the 8 frequency tones in the transmit signal. For $N_{\mathrm{E}} < 7$, the results are averaged over all possible N_{E}-element sub-arrays.

Figure 4(a) plots I_{K} as a function of N_{RS} for several values of N_{RE}, with the results averaged over the four indoor measurement locations. The results show that I_{K} decreases with increasing N_{RS} because of the resulting reduction in the observed channel variances. However, since increasing the number of states per RE (N_{RS}) dramatically increases the number of overall unique combinations of states in the reconfigurable antenna, it may be better to have a larger number of states (more possible channel observations) than to maximize the number of bits achievable per channel observation

Figures 4(b)-(c) plot I_{SK} as a function of N_{E} for different values of N_{RE} and N_{RS}, where again the results represent averages over the four indoor measurement locations. The results show that I_{SK} decreases as N_{E} increases, but they also reveal that increased reconfigurability (large N_{RE}) improves performance. In fact, provided that N_{RE} is adequately large, the reduction in I_{SK} created by having a large number of antennas at the eavesdropper relative to an eavesdropper with a single antenna is limited to approximately 50%.

IV. Conclusion

This work explores the effectiveness of using a reconfigurable antenna to generate time-varying channel estimates that are in turn used to establish secret encryption keys. The results demonstrate that an increase in the number of reconfigurable elements increases the number of key bits that can be securely generated and also show that using only two impedance states per RE maximizes the number of bits available per antenna state. The findings suggest that reconfigurable antennas represent a promising candidate for key establishment based on reciprocal channel estimates for static or slow-fading channels.

References

[1] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[2] R. Mehmood and J. W. Wallace, "Measurement of capacity enhancement with parasitic reconfigurable aperture antennas in interference-limited scenarios," in *Proc. Int Smart Antennas (WSA) ITG Workshop*, 2012, pp. 140–144.

[3] J. Wallace, "Secure physical layer key generation schemes: Performance and information theoretic limits," in *Proc. IEEE Int. Conf. Communications ICC '09*, 2009, pp. 1–5.