Key Establishment Employing Reconfigurable Antennas: Impact of Antenna Complexity

Rashid Mehmood, *Student Member, IEEE*, Jon W. Wallace, *Senior Member, IEEE*, and Michael A. Jensen, *Fellow, IEEE*

***Abstract*—When establishing secret encryption keys using estimates of the reciprocal wireless channel, the number of key bits that can be generated for a static or slowly varying propagation environment can be enhanced by randomly changing the radiation properties of a reconfigurable antenna. However, prior studies of this approach have been limited and have not considered a high degree of antenna reconfigurability. This paper uses simulations and experimental measurements to characterize the impact of reconfigurable antenna complexity on the performance of key establishment in different static propagation environments and in the presence of a multi-antenna eavesdropper. 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. The results further demonstrate that increasing the number of reconfigurable parasitic elements notably increases the achieved performance.**

***Index Terms*—Antennas and propagation, security, reconfigurable antennas.**

I. Introduction

WHILE traditional security measures for wireless communication are implemented at the upper layers of the communication protocol stack, applying appropriate techniques at the physical layer can serve to enhance security. For example, in [1], [2] the idea of exploiting common randomness for secure communications was established, showing that two nodes can achieve perfectly secure communications in an information theoretic sense without the need for a-priori shared information. In [3]–[5], the ability to generate secure keys by exploiting this common randomness was analyzed, proving the conditions under which perfectly secret keys can be generated by two nodes.

Since electromagnetic propagation and antennas are reciprocal, if two radios transmit training data to each other using half-duplex communication and use the received training sequences to estimate the channel transfer function from the transmit-to-receive antenna terminals, the observed channel estimates will be the same to within estimation errors. Thus, a reciprocal channel can be used as a source of common randomness for key establishment, which was suggested as early as [6]. Later work explores the limits of key establishment using a reciprocal scalar channel [7], [8] and develops practical algorithms based on channel quantization [9]–[13]. Analysis and measured performance of key establishment for spatially correlated multi-input multiple-output (MIMO) channels was treated in [14]–[16]. Recently, the impact of channel sparsity in reciprocal channel key generation has been investigated [17].

An important limitation of key establishment using quantization of a shared reciprocal channel occurs when the channel is static or very slowly fading, since the amount of common randomness is limited. In [18] the useful idea of using a reconfigurable antenna for key establishment was presented, where random states of an electronically steerable parasitic array (ESPAR) were used to create a random reciprocal channel state at the two communicating nodes, even for a static underlying propagation channel. Since [18] was only a proof-of-concept and did not consider vulnerability with respect to an eavesdropper, we presented initial simulations and measurements of a scalable reconfigurable antenna in [19] and [20], respectively, suggesting that with sufficient antenna complexity, keys that are secure with respect to a single-antenna eavesdropper can be generated.

The purpose of this paper is to provide a comprehensive analysis of the security of key establishment methods that employ reconfigurable antennas and channel reciprocity to generate common randomness. This new treatment overcomes limitations of previous work through detailed simulation and direct measurement. First, in contrast to [18], the antenna used in our work has scalable complexity, allowing determination of the full potential of this technology. Second, we consider the case of an eavesdropper equipped with multiple antennas, since only a single-antenna eavesdropper was considered in our previous work. Finally, unlike [20] where due to hardware limitations phase had to be handled in an approximate way, we perform phase-coherent three-node measurements in this work, providing a more accurate characterization of the secrecy obtained.

Our analysis reveals not only the conditions under which reconfigurable antennas provide good key generation rates, but also the level of security achieved using the approach in the presence of a close, multi-antenna, passive eavesdropper. The results show that in a multipath channel, a highly configurable antenna offers a significant improvement in the number of key bits that can be securely established even when surrounded by eavesdropper antennas.

Manuscript received November 13, 2013; revised March 22, 2014 and May 23, 2014; accepted May 26, 2014. Date of publication June 13, 2014; date of current version November 7, 2014. This work was supported in part by the German Science Foundation (DFG) through the COIN Priority Program and in part by the U.S. Army Research Office under Grant W911NF-12-1-0469. The associate editor coordinating the review of this paper and approving it for publication was K. Haneda.

The authors are with the Department of Electrical and Computer Engineering, Brigham Young University, Provo, UT 84602 USA (e-mail: r.mehmood@ieee.org; wall@ieee.org; jensen@byu.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2014.2330835

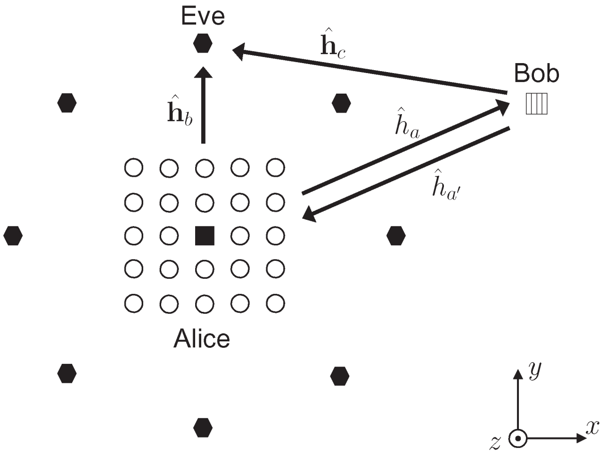

Fig. 1. Top view of the antenna arrangement in the security analysis, where Bob has a single antenna (hatched square), Alice has a RECAP with a single feed antenna (black square) and programmable REs placed on a regular grid (empty circles), and Eve has an array of antennas surrounding the RECAP (filled hexagons).

II. System Model

Antennas with a high degree of reconfigurability that consist of a dense two- or three-dimensional array of reconfigurable elements have been referred to as reconfigurable aperture (RECAP) antennas [21], [22], evolving antennas [23], self-structuring antennas [24], multifunctional reconfigurable antennas [25], and pixel antennas [26], where the first term (RECAP) is adopted in this work.

Fig. 1 shows the system model considered in our analysis in which two legitimate nodes designated as *Alice* and *Bob* communicate in the presence of an eavesdropper *Eve*. While Alice possesses a RECAP, Bob is equipped with a single antenna, allowing us to focus on the performance improvement obtained with a RECAP without the complexity of coordinating reconfiguration at both radios. Eve possesses an array of N_{E} elements that is assumed to surround Alice's RECAP, as this creates a high level of vulnerability.[1] The estimated narrowband scalar (single antenna) channels at Bob and Alice are respectively denoted as $\hat{h}_a$ and $\hat{h}_{a'}$, where the carat $(\hat{\cdot})$ is used to emphasize that these are estimated quantities. Because of reciprocity, the differences between these two estimates result only from channel estimation errors, imperfect calibration designed to remove non-reciprocal contributors to the channel (i.e. radio circuitry), channel time variation between estimation of the two channels, or other practical effects. 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.

A. Parasitic RECAP

Alice's RECAP consists of a single *feed* antenna placed at the center of a uniform two-dimensional 5 × 5 square grid of area $1\lambda \times 1\lambda$ with an inter-element spacing of $\lambda/4$, as depicted by the square in Fig. 1. The terminals of this central antenna are connected to the radio transceiver circuitry. Other identical antennas are placed at the other grid positions (open circles in Fig. 1), with the terminals of each of these *parasitic* antennas connected to a circuit that can tune the reactance loading the antenna. Each tunable parasitic antenna is therefore termed a *reconfigurable element* (RE), with N_{RE} indicating the total number of REs used to construct the RECAP.

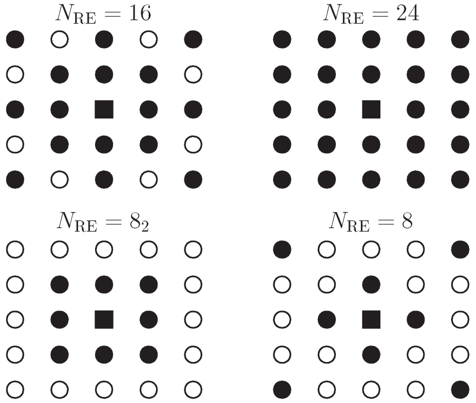

Fig. 2. RECAP structure with elements arranged on a 5 × 5 regular grid, where N_{RE} reconfigurable elements (black circles) are terminated with tunable impedances and the center element (black square) is the feed. Dipole or monopole antennas are aligned along the z-axis (out of the page).

Intuitively, the different reconfigurable states of the RECAP can be understood by using the analogy of a digital image. The number of reconfigurable elements (N_{RE}) is analogous to the number of pixels, and the number of different reactances that can be set on each element (N_{RS}) is like the number of possible colors for each pixel. Thus, like the digital image, the total number of possible states of the RECAP is $N_{\mathrm{RS}}^{N_{\mathrm{RE}}}$. Although we use a very complex structure, a goal of the work is to understand what level and type of reconfigurability is sufficient to capture most of the security benefit (i.e. the point of diminishing returns), and some observations will be drawn at the conclusion.

Fig. 2 shows the four different RECAP arrangements used in this study, where the filled circles represent placement of the REs on the grid. It is expected that with more elements, the RECAP will be able to more fully exploit the spatial degrees of freedom within the propagation channel for key establishment, although REs placed further from the feed element will likely have reduced impact on the achieved performance. Motivated by this observation, we consider two different arrangements for $N_{\mathrm{RE}} = 8$ to allow exploration of the impact of RE proximity to the feed antenna.

For the simulations presented in this work, the feed antenna and REs use z-oriented half-wave dipole elements that are easily modeled with electromagnetic simulation software. In contrast, the experiments use z-oriented quarter-wave monopole antennas due to their fabrication simplicity. While using different antennas for the simulations and experiments may create some differences, the similar (theoretically identical) radiation patterns for the two elements suggests that the simulations and measurements should result in similar performance behaviors.

[1] From an electromagnetics perspective, it is expected that having Eve's antennas surround the legitimate node represents a worst case for security, since the fields everywhere inside a closed surface can be computed from fields sampled on that surface.

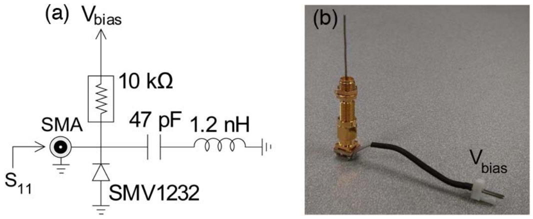

Fig. 3. RE circuit: (a) schematic, (b) completed RE with circuit board holding components, bias lead, and a monopole inserted into the SMA connector.

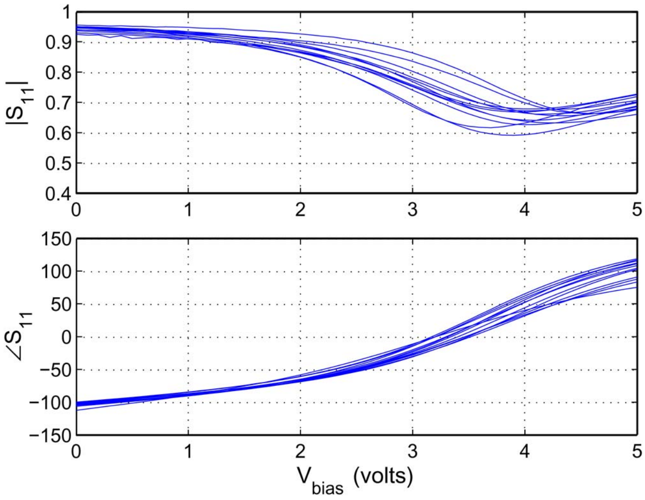

Fig. 4. Reflection coefficient of several REs as a function of the bias voltage (V_{bias}).

B. Reconfigurable Element

Fig. 3 shows the design of the varactor-diode-based RE used in measurements. The tuning voltage V_{bias} is supplied by an FPGA-controlled circuit that generates a uniformly-quantized bias voltage to each RE for each RE *state*. The tuning circuitry is fabricated on the lower side of the small printed circuit board at the base of the SMA connector. While Fig. 3 shows the monopole antenna attached to the tunable circuitry, in operation the bulkhead adapter attached to the wire monopole is fed through the ground plane and the SMA connector attached to the tuning circuitry is then connected to the bulkhead adapter below the ground plane (Fig. 9 shows the monopole array on the ground plane).

Fig. 4 plots the corresponding magnitude and phase of S_{11} measured for several different REs at 2.54 GHz using a Rohde & Schwarz VNB20 vector network analyzer. S_{11} is measured at the input of the SMA connector when the monopole antenna is not attached as depicted in Fig. 3(a). The results show that the REs provide a phase tunability of approximately 200° over $0 \leq V_{\mathrm{bias}} \leq 5$ V and that the loss (as manifest through $|S_{11}|$) increases with bias voltage. The impedance mismatch loss contribution can be reduced by increasing the value of the series inductance in the circuit, but our testing shows that this leads to reduced phase tunability. Since the variation of phase is not significant for $V_{\mathrm{bias}} < 1$ V, we uniformly quantize the range $1 \leq V_{\mathrm{bias}} \leq 5$ V into $N_{\mathrm{RS}} \in \{2, 4, 8, 32\}$ reconfigurable states. The simulations use the measured S-parameter curves shown in Fig. 4 in order to make these computations as realistic as possible.

III. Information Theoretic Analysis

Two information theoretic metrics are used in this work to quantify the impact of RECAP reconfigurability on the key establishment performance. This section briefly discusses the metrics and their computation using channel observations.

A. Key Establishment Metrics

Exploiting common randomness for secure communications was first analyzed in an information theoretic context in [1]. Assuming two legitimate nodes observe random variables X and Y, while an eavesdropper observes Z, [1] shows that secrecy capacity is bounded from above by $\min[I(X;Y|Z), I(X;Y)]$, where $I(\cdot;\cdot)$ is mutual information. Furthermore, it was shown that this bound can be approached by discussion over a public channel. Later, the same authors analyzed the problem of secure key establishment exploiting common randomness [3]–[5], where $I(X;Y|Z)$ is established as a critical security parameter and referred to as the *intrinsic conditional mutual information*. A similar quantity is also used in [17] to measure the theoretical key generation rate.

In the context of our system model in Fig. 1, X and Y correspond to $\hat{h}_a$ and $\hat{h}_{a'}$, which represent common random information that can be used to establish a common message (or secret key) at the two legitimate nodes. The channels $\hat{\mathbf{h}}_b$ and $\hat{\mathbf{h}}_c$ correspond to Z, or the information that Eve can use to guess the secret key. In [14], [15] we considered the possibility of using reciprocal fading MIMO channels as the source of common randomness to generate a shared secret key, where we adopted the intrinsic conditional mutual information bound to define two useful security metrics, as described below.

The first metric is *available key bits*, which refers to the maximum number of independent key bits that can be generated from each observation of the random channel, or

$$I_{\mathrm{K}} = I(\hat{h}_a; \hat{h}_{a'}) = \mathrm{E}\left\{\log_2 \frac{f(\hat{h}_a, \hat{h}_{a'})}{f(\hat{h}_a) f(\hat{h}_{a'})}\right\}, \qquad (1)$$

where $\mathrm{E}\{\cdot\}$ is expectation, and $f(\cdot)$ is a probability density function (pdf).

Because Eve's channel estimates may be correlated with $\hat{h}_a$ and $\hat{h}_{a'}$, she may be able to use these estimates to gain information about the established key. We account for this with a second metric, referred to as *secure key bits* or I_{SK}, which is the number of generated key bits per channel observation that can be secure with respect to Eve, given by

$$\begin{aligned} I_{\mathrm{SK}} &= I(\hat{h}_a; \hat{h}_{a'} | \hat{\mathbf{h}}_b, \hat{\mathbf{h}}_c) \\ &= \mathrm{E}\left\{\log_2 \frac{f(\hat{h}_a, \hat{h}_{a'} | \hat{\mathbf{h}}_b, \hat{\mathbf{h}}_c)}{f(\hat{h}_a | \hat{\mathbf{h}}_b, \hat{\mathbf{h}}_c) f(\hat{h}_{a'} | \hat{\mathbf{h}}_b, \hat{\mathbf{h}}_c)}\right\}. \end{aligned} \qquad (2)$$

When Eve's channels are independent from the Alice-Bob channel, we have $I_{\mathrm{SK}} = I_{\mathrm{K}}$, indicating all available bits are also secure from the eavesdropper.

Note that under static channel conditions and fixed antennas, $I_{\mathrm{K}} = I_{\mathrm{SK}} = 0$, indicating that no secret key can be generated. However, by using random antenna states, the reciprocal end-to-end channel is randomized, leading to nonzero security metrics. Estimation errors also create channel variation, but since this randomness is modeled as independent processes at the communicating nodes, the mutual information metrics do not increase from this effect, indicating that a key cannot be generated from estimation error.

B. Gaussian Channel Assumption

For a static propagation environment, the set of channels created by reconfiguring the RECAP may not exhibit a Gaussian distribution. In this case, the expectations in (1) and (2) can be computed numerically, as detailed in [19]. When Eve has more than one antenna, the large number of realizations required for convergence can lead to excessive computation.

Developing closed-form bounds and low-complexity numerical computations for (1) and (2) is highly desirable, but beyond the scope of this paper. Instead, to reduce the required computation, we can assume that the channels satisfy a Gaussian distribution, allowing closed-form computation of I_{K} and I_{SK}. For channel observations that are correlated zero-mean complex Gaussian random variables,

$$I_{\mathrm{K}} = \log_2 \frac{|\hat{\mathbf{R}}_{aa}||\hat{\mathbf{R}}_{a'a'}|}{|\hat{\mathbf{R}}_{A'A'}|}, \tag{3}$$

where $|\cdot|$ is the matrix determinant and covariances with lowercase subscripts denote

$$\hat{\mathbf{R}}_{x_1 x_2} = \mathrm{E}\left\{\hat{\mathbf{h}}_{x_1}\hat{\mathbf{h}}_{x_2}^{\dagger}\right\} \tag{4}$$

with $\{\cdot\}^{\dagger}$ indicating a conjugate transpose. Note that $\hat{\mathbf{R}}_{aa}$ and $\hat{\mathbf{R}}_{a'a'}$ are scalar variances when Bob has a single antenna and Alice's RECAP has a single feed antenna. Covariances with uppercase subscripts represent those of stacked channel vectors, or

$$\hat{\mathbf{R}}_{X_1X_2\ldots X_N} = \mathrm{E}\left\{\left[\hat{\mathbf{h}}_{x_1}^{\dagger}\hat{\mathbf{h}}_{x_2}^{\dagger}\ldots\hat{\mathbf{h}}_{x_N}^{\dagger}\right]^{\dagger}\left[\hat{\mathbf{h}}_{x_1}^{\dagger}\hat{\mathbf{h}}_{x_2}^{\dagger}\ldots\hat{\mathbf{h}}_{x_N}^{\dagger}\right]\right\}. \tag{5}$$

Similarly, I_{SK} becomes

$$I_{\mathrm{SK}} = \log_2 \frac{|\hat{\mathbf{R}}_{ABC}||\hat{\mathbf{R}}_{A'BC}|}{|\hat{\mathbf{R}}_{BC}||\hat{\mathbf{R}}_{AA'BC}|}. \tag{6}$$

IV. Modeled Key Establishment Performance

This section covers the security versus complexity analysis of a parasitic RECAP using full-wave simulations and network analysis. The electromagnetic propagation channel is assumed to be static, and any change in the channel can only be caused by the RECAP. Since additional time variation in the propagation would likely increase security, the static channel represents a worst-case scenario.

A. RECAP Analysis

Computing I_{K} and I_{SK} requires simulations for thousands of RECAP states (a RECAP state is a unique combination of RE states). However, since the reconfiguration is accomplished by changing the reactance presented to the parasitic element terminals, we can use a single full-wave electromagnetic characterization of the antennas and then evaluate the antenna parameters for different reactance combinations using network analysis [27].

In our scenario, Eve's antennas are near the RECAP, and because mutual coupling between the RECAP and Eve's antennas may reveal information that can help Eve more easily determine the key, this coupling cannot be ignored. Therefore, we use the Numerical Electromagnetic Code (NEC) to model Eve's and Alice's arrays together. Since Bob is far from Alice and Eve, his antenna is modeled separately and is assumed to lie in the far-field of the other arrays. In the following, the term *port* refers to the terminals of any dipole with *feed port* indicating the port for an antenna that is connected to a transmitter or receiver (which includes the RECAP center element, Bob's antenna, and all of Eve's antennas). While the following formulates the mathematics for a general number of RECAP feed antennas N_{RF}, the simulations assume a single RECAP feed ($N_{\mathrm{RF}} = 1$) as shown in Figs. 1 and 2.

In the NEC full-wave simulations, a unit voltage excitation is applied at the kth port with all others terminated in a short-circuit, allowing computation of the short-circuit embedded radiation pattern $e_k^{\mathrm{sc}}(\theta, \phi)$ and the current flowing through the shorted ports of non-excited antennas. Application of this computation for all antennas enables construction of the admittance matrix $\mathbf{Y}$ and the vector $\mathbf{e}^{\mathrm{sc}}(\theta, \phi)$ with kth element $e_k^{\mathrm{sc}}(\theta, \phi)$. For convenience, we formulate the network analysis using S-parameters, and we must therefore compute the S-parameters from

$$\mathbf{S} = (\mathbf{I} + Z_0\mathbf{Y})^{-1}(\mathbf{I} - Z_0\mathbf{Y}) \tag{7}$$

where $\mathbf{I}$ is the identity matrix and Z_0 is the system impedance. We must also compute the radiation patterns with all non-excited ports terminated in the system impedance using

$$\mathbf{e}^{\mathrm{mc}}(\theta, \phi) = \frac{1}{\sqrt{Z_0}}\mathbf{e}^{\mathrm{sc}}(\theta, \phi)\mathbf{Y}^{-1}(\mathbf{I} - \mathbf{S}). \tag{8}$$

The computations use $Z_0 = 72\ \Omega$.

To compute the antenna characteristics for arbitrary loading of the RE ports, we begin with the general formulation

$$\underbrace{\begin{bmatrix}\mathbf{b}_{\mathrm{F}}\\ \mathbf{b}_{\mathrm{R}}\end{bmatrix}}_{\mathbf{b}} = \underbrace{\begin{bmatrix}\mathbf{S}_{\mathrm{FF}} & \mathbf{S}_{\mathrm{FR}}\\ \mathbf{S}_{\mathrm{RF}} & \mathbf{S}_{\mathrm{RR}}\end{bmatrix}}_{\mathbf{S}}\underbrace{\begin{bmatrix}\mathbf{a}_{\mathrm{F}}\\ \mathbf{a}_{\mathrm{R}}\end{bmatrix}}_{\mathbf{a}}, \tag{9}$$

where $\mathbf{a}$ and $\mathbf{b}$ respectively represent vectors of incident and reflected waves at a set of ports. The quantities $\mathbf{a}_{\mathrm{F}}$ and $\mathbf{b}_{\mathrm{F}}$ are $(N_{\mathrm{RF}} + N_{\mathrm{E}}) \times 1$ vectors at the feed ports, $\mathbf{a}_{\mathrm{R}}$ and $\mathbf{b}_{\mathrm{R}}$ are $N_{\mathrm{RE}} \times 1$ vectors at the parasitic RE ports, and $\mathbf{S}$ has been appropriately partitioned. Terminating the kth RE port with a load having reflection coefficient $\Gamma_{\mathrm{R},k}$ (computed using Z_0) that forms the kth diagonal element of the diagonal matrix $\mathbf{\Gamma}_{\mathrm{R}}$, we have $\mathbf{a}_{\mathrm{R}} = \mathbf{\Gamma}_{\mathrm{R}}\mathbf{b}_{\mathrm{R}}$. Using this in (9) yields

$$\mathbf{a}_{\mathrm{R}} = \mathbf{\Gamma}_{\mathrm{R}}(\mathbf{I} - \mathbf{S}_{\mathrm{RR}}\mathbf{\Gamma}_{\mathrm{R}})^{-1}\mathbf{S}_{\mathrm{RF}}\mathbf{a}_{\mathrm{F}} \tag{10}$$

$$\mathbf{b}_{\mathrm{F}} = \underbrace{\left[\mathbf{S}_{\mathrm{FF}} + \mathbf{S}_{\mathrm{FR}}\mathbf{\Gamma}_{\mathrm{R}}\left(\mathbf{I} - \mathbf{S}_{\mathrm{RR}}\mathbf{\Gamma}_{\mathrm{R}}^{-1}\right)\mathbf{S}_{\mathrm{RF}}\right]}_{\mathbf{\Gamma}_{\mathrm{F}}}\mathbf{a}_{\mathrm{F}}, \tag{11}$$

where $\mathbf{\Gamma}_{\mathrm{F}}$ is the $(N_{\mathrm{RF}} + N_{\mathrm{E}}) \times (N_{\mathrm{RF}} + N_{\mathrm{E}})$ reflection coefficient matrix looking into Alice's and Eve's combined feed ports for the RE termination $\mathbf{\Gamma}_{\mathrm{R}}$.

The radiation patterns of Alice's feed antennas $(\mathbf{e}_{\mathrm{A}}^{\mathrm{mc}}(\theta, \phi))$ and Eve's array $(\mathbf{e}_{\mathrm{E}}^{\mathrm{mc}}(\theta, \phi))$ given the RE termination are computed as

$$\begin{bmatrix} \mathbf{e}_{\mathrm{A}}^{\mathrm{mc}} \\ \mathbf{e}_{\mathrm{E}}^{\mathrm{mc}} \end{bmatrix} = \begin{bmatrix} \mathbf{e}_{\mathrm{F}}^{\mathrm{mc}}(\theta, \phi) & \mathbf{e}_{\mathrm{RE}}^{\mathrm{mc}}(\theta, \phi) \end{bmatrix} \begin{bmatrix} \mathbf{a}_{\mathrm{F}} \\ \mathbf{a}_{\mathrm{R}} \end{bmatrix}, \tag{12}$$

where $\mathbf{e}_{\mathrm{F}}^{\mathrm{mc}}(\theta, \phi)$ and $\mathbf{e}_{\mathrm{RE}}^{\mathrm{mc}}(\theta, \phi)$ represent the portions of $\mathbf{e}^{\mathrm{mc}}$ corresponding to the feed antennas and the REs, respectively.

B. Communication Channels

We assume that propagation is confined to the horizontal (xy) plane, and therefore we consider the azimuthal radiation pattern only $(\theta = \pi/2)$. The multipath model consists of L paths, where the ℓth path has angle of departure $(\pi/2, \phi_\ell)$, angle of arrival $(\pi/2, \phi'_\ell)$, and complex amplitude α_ℓ. The channels become

$$h_{a'} = \sum_{\ell=1}^{L} \left[\mathbf{e}_{\mathrm{A}}^{\mathrm{mc}} \left(\frac{\pi}{2}, \phi'_\ell \right) \right]^{\mathrm{T}} \alpha_\ell \mathbf{e}_{\mathrm{B}}^{\mathrm{mc}} \left(\frac{\pi}{2}, \phi_\ell \right) \tag{13}$$

$$h_{c,i} = \sum_{\ell=1}^{L} \left[\mathbf{e}_{\mathrm{E},i}^{\mathrm{mc}} \left(\frac{\pi}{2}, \phi'_\ell \right) \right]^{\mathrm{T}} \alpha_\ell \mathbf{e}_{\mathrm{B}}^{\mathrm{mc}} \left(\frac{\pi}{2}, \phi_\ell \right) \tag{14}$$

where $\{\cdot\}^{\mathrm{T}}$ is a transpose, $h_a = h_{a'}$ is the error-free reciprocal channel between Bob and Alice, $h_{c,i}$ is the channel between Bob and Eve's ith antenna, and $\mathbf{e}_{\mathrm{B}}^{\mathrm{mc}}$ is the azimuthally omnidirectional pattern of Bob's antenna. Because Eve's antennas lie close to the RECAP, the computed coupling between Alice's feed antenna and Eve's array elements gives the channel $\mathbf{h}_b$ with ith element

$$h_{b,i} = \Gamma_{\mathrm{F},(1,i+1)}, \tag{15}$$

where $\mathbf{\Gamma}_{\mathrm{F}}$ has been ordered such that $\Gamma_{\mathrm{F},(1,1)}$ is the input reflection coefficient of the RECAP feed port.

A difficulty in defining the security of our proposed scenario is that Eve may have a much more sensitive receiver than Alice or Bob. Assuming the worst case of zero noise at Eve (or infinite SNR) leads to an information theoretic security of zero, since there will be a one-to-one mapping between the discrete RECAP-induced channel states of the ideal Alice-Bob channel and Eve's channel. In order to not place any assumptions on the sensitivity of Eve's receiver, yet limit Eve's effective SNR, we limit the SNR of the pilot signal used for channel estimation by having Alice and Bob add artificial noise to the pilots they transmit. This synthetic noise is only known by the nodes that transmit it, and therefore cannot be subtracted by any other receiving node. Assuming that Alice and Bob have an intrinsic SNR of 13 dB (due to receiver noise, non-reciprocity, etc.) and that Alice and Bob add synthetic noise that is also 13 dB below the pilot signal level, this 3 dB degradation leads to a composite SNR of 10 dB at Alice and Bob. On the other hand, we assume that Eve's receiver is noiseless, and since she only experiences artificial noise, her SNR is 13 dB.

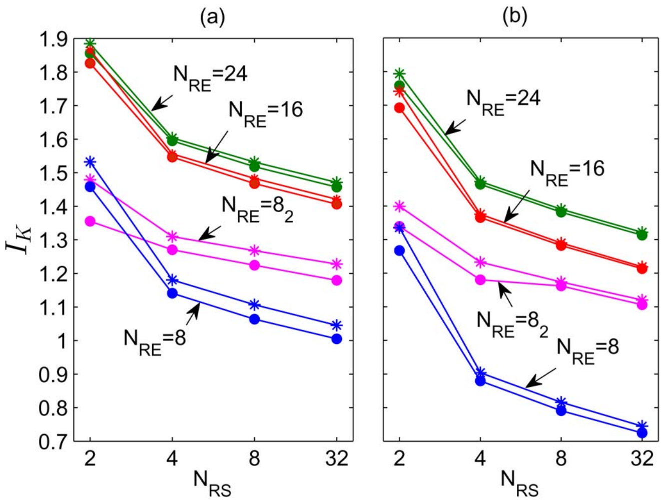

Fig. 5. Simulated I_{K} as a function of N_{RS} for different values of N_{RE}, where curves marked with $*$ and $\bullet$ are respectively obtained using the Gaussian assumption and numerical computation: (a) NLOS channel $(L = 10)$, (b) LOS channel $(L = 1)$.

With these SNR values established, we compute channel estimates at Alice, Bob, and Eve by corrupting the channels in (13)–(15) with additive estimation errors modeled as zero-mean complex Gaussian random processes whose variances are chosen to achieve the specified SNR values. Finally, I_{K} and I_{SK} can be computed.

C. Simulation Study

Our simulations consider two different channel scenarios: (a) Non-line-of-sight (NLOS) using $L = 10$ multipaths and (b) line-of-sight (LOS) using $L = 1$. In both scenarios, propagation path characteristics remain fixed and channel estimates are computed for 10^6 different RECAP states. This allows construction of the relevant covariances required for computing I_{K} and I_{SK} using the Gaussian assumption and, for some scenarios, allows computation of the metric using the accurate numerical technique. When the channel type is not specified, the NLOS channel is used. For all simulations, the results are averaged over 300 different channel realizations and 8 equally-spaced frequencies from 2.515 to 2.575 GHz. When computing I_{SK} for $N_{\mathrm{E}} < 8$, we assume that Eve's antennas represent a subset of the array of $N_{\mathrm{E}} = 8$ elements shown in Fig. 1, and we average the results over all possible sub-array configurations.

1) Security vs. Antenna Complexity: Fig. 5 plots I_{K} as a function of the number of states N_{RS} for different values of the number of reconfigurable elements N_{RE} using the numerical method to compute (1) and Gaussian assumption to compute (3). The error in the Gaussian assumption (difference between the two curves) decreases as both N_{RS} and N_{RE} increase, demonstrating that the distribution of the channel realizations with more REs and more reconfigurable states becomes increasingly Gaussian. As expected, the Gaussian assumption upper bounds the numerical computations of I_{K}.

Fig. 5 further shows that under both LOS and NLOS propagation, the value of I_{K} decreases with increasing N_{RS}. With more reconfigurable states, the variance of the channels obtained for different states decreases, reducing the number of available key bits per channel observation (see (3)). Although these results show that using $N_{\rm RS} = 2$ is beneficial for high $I_{\rm K}$, care must be taken to ensure that the total complexity of the reconfigurable antenna is not too small, as discussed in [19]. If the total number of antenna states ($N_{\rm RS}^{N_{\rm RE}}$) of the reconfigurable antenna is too small, Eve may employ an alternative brute-force attack where instead of searching the set of all possible keys, Eve only needs to search the set of possible mappings from antenna states to key bits. Assuming that the total antenna complexity is well above the lower bound discussed in [19], the antenna configuration giving the highest $I_{\rm K}$ should be chosen.

Finally, Fig. 5 shows that for the same number of RE states, increasing the number of REs improves $I_{\rm K}$. This occurs because increasing $N_{\rm RE}$ physically adds complexity to the coupling between the parasitic array and the feed element in the RECAP, thereby increasing the range of possible RECAP radiation characteristics. However, the relative benefit of additional REs diminishes as $N_{\rm RE}$ increases, a result that is consistent with previous results on RECAP beamforming [28] demonstrating that 8 parasitic elements per wavelength are sufficient to exploit the degrees of freedom in the propagation channel. Note that although $N_{\rm RE} = 8_2$ gives higher $I_{\rm K}$ performance than $N_{\rm RE} = 8$, the more critical $I_{\rm SK}$ metric is usually lower, indicating that a larger array with higher spatial selectivity is more beneficial than high coupling between the feed and parasitic elements.

2) Relative Importance of Eve's Channels: The results for $I_{\rm K}$ do not consider the information ($\hat{\mathbf{h}}_b$ and $\hat{\mathbf{h}}_c$) possessed by Eve that can allow her to more easily determine the established key, and therefore we next consider $I_{\rm SK}$. When evaluating this metric, it is instructive to determine the relative importance of these two channels in providing information to Eve. We therefore consider three different cases for computing $I_{\rm SK}$:

Case 1: Eve knows both $\hat{\mathbf{h}}_b$ and $\hat{\mathbf{h}}_c$,
Case 2: Eve knows only $\hat{\mathbf{h}}_b$, and
Case 3: Eve knows only $\hat{\mathbf{h}}_c$.

Fig. 6 plots the corresponding results for $N_{\rm RE} = 24$ computed using the Gaussian assumption, with the results showing that $\hat{\mathbf{h}}_b$ is the main source of information for Eve for both NLOS and LOS scenarios (lower $I_{\rm SK}$ indicates more information leaked to Eve). This result is logical, since fluctuations in $\hat{\mathbf{h}}_c$ arise only from a change in the patterns of Eve's antennas due to weak near-field coupling with Alice's RECAP, whereas $\hat{\mathbf{h}}_b$ provides direct information about RECAP changes. Given this observation, only $\hat{\mathbf{h}}_b$ is considered when computing $I_{\rm SK}$ in the subsequent analysis. Interestingly, this observation is in contrast to the case where a random propagation channel (not a random antenna) is used to generate the key, where $\hat{\mathbf{h}}_c$ gives information to Eve and $\hat{\mathbf{h}}_b$ is a static channel with no information [15].

Because numerical evaluation of $I_{\rm SK}$ is computationally demanding for $N_{\rm E} > 1$, we construct $I_{\rm SK}^{(1)}$ using (2) and $I_{\rm SK,G}^{(1)}$ using (6) for $N_{\rm E} = 1$ and then compute the ratio $\gamma = I_{\rm SK}^{(1)}/I_{\rm SK,G}^{(1)}$. Then, for $N_{\rm E} > 1$, we compute $I_{\rm SK}$ using the Gaussian assumption in (6) and scale the result by γ to obtain a corrected value of $I_{\rm SK}$. Comparison of this corrected Gaussian result with values obtained using numerical simulations for $N_{\rm E} = 2$ with $N_{\rm RE} = 8$ and $N_{\rm RS} = 2$ in an NLOS channel shows that the error in the corrected Gaussian result is less than 4%.

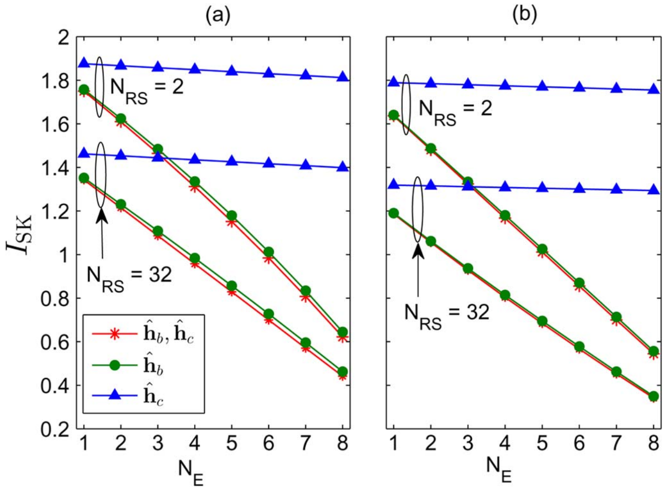

Fig. 6. Simulated $I_{\rm SK}$ as a function of $N_{\rm E}$ for $N_{\rm RE} = 24$ and two values of $N_{\rm RS}$ when Eve knows $\hat{\mathbf{h}}_b$ alone, $\hat{\mathbf{h}}_c$ alone, or both $\hat{\mathbf{h}}_b$ and $\hat{\mathbf{h}}_c$: (a) NLOS channel ($L = 10$), (b) LOS channel ($L = 1$).

3) Dependence on Eve's Array Size: Fig. 7(b)–(e) plot $I_{\rm SK}$ as a function of $N_{\rm E}$ for different values of $N_{\rm RE}$ and $N_{\rm RS}$ using corrected Gaussian assumption. It is interesting to observe that for this worst-case scenario in which Eve can estimate the RECAP pattern that creates the random channel fluctuations, $I_{\rm SK}$ decreases rapidly as $N_{\rm E}$ increases. These results further confirm that the number of key bits per channel observation is maximized for $N_{\rm RS} = 2$ and for large values of $N_{\rm RE}$. However, we emphasize that the channel statistics for small $N_{\rm RS}$ become less Gaussian, as evidenced by the increased difference between the results from the uncorrected and corrected Gaussian assumption for $I_{\rm K}$.

Note that for the case with $N_{\rm RS} = 2$ and $N_{\rm RE} = 24$, comparison with Fig. 7(a) shows that approximately 35% of the available key bits remain secure in the presence of Eve surrounding the RECAP with 8 antennas. This suggests that with proper selection of the antenna topology, key generation using reconfigurable antennas can be made robust to even well-equipped eavesdroppers. On the other hand, having too little or the improper type of reconfigurability may lead to a system that is easily compromised.

V. Measured Key Establishment Performance

While the simulations have provided valuable insights into the potential of using sophisticated reconfigurable antennas for key establishment, the results depend on assumptions that may not always be satisfied. Therefore, we use experimental measurements to validate the observations drawn from the simulations. The communication scenario used is similar to that used for the simulations, with the exception that $\lambda/4$ monopole antennas mounted on a ground plane are used instead of $\lambda/2$ dipoles. Because of the inferior performance of the $N_{\rm RE} = 8_2$ RECAP configuration in terms of $I_{\rm SK}$ predicted by the simulations, this topology is excluded in the measurements.

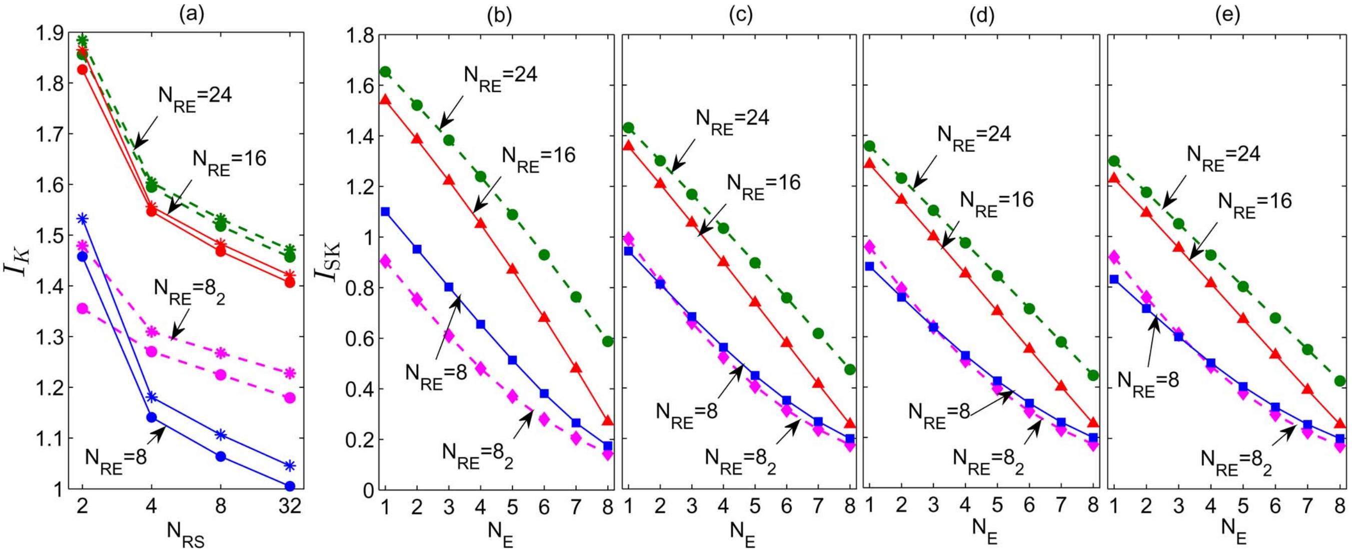

Fig. 7. Simulated I_{K} and I_{SK} as a function of N_{E} for different values of N_{RE} and N_{RS}, where I_{K} curves marked with $*$ and $\bullet$ are respectively obtained using the uncorrected and corrected Gaussian assumption: (a) I_{K}, (b)–(e) I_{SK}.

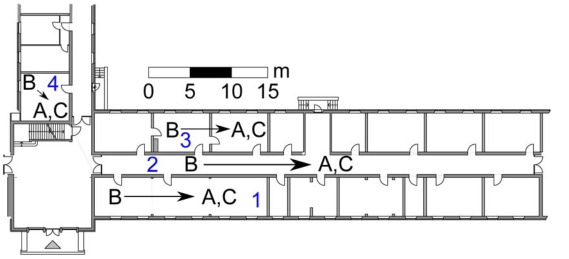

Fig. 8. Relative positions of Bob (B), Alice (A) and Eve (C) at four different locations within an indoor environment. Arrows connect the different node locations for a given location number.

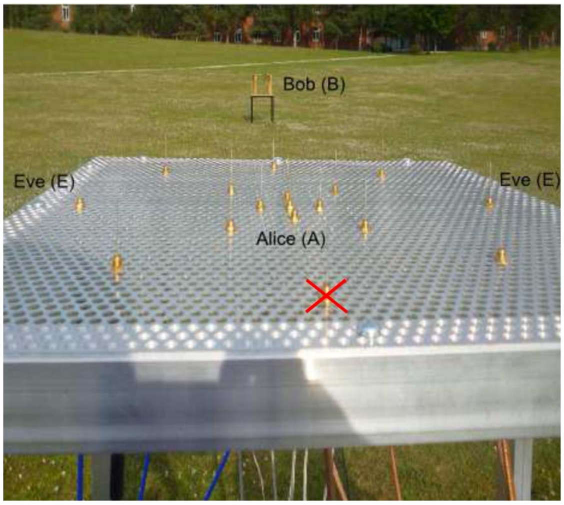

Fig. 9. Photograph of the outdoor measurement environment and the relative positions of Alice, Bob and Eve for $N_{\mathrm{RE}} = 8$. The red '×' indicates the antenna in Eve's array that is not used in measurements.

A. Node Locations

Fig. 8 identifies the relative positions of Bob, Eve and Alice for four different measurement locations within the Research I building on the Jacobs University Bremen campus. Location 2 is within a hallway while the other locations are in different university laboratories. Outdoor measurements were taken on an open lawn as shown in Fig. 9, where the distance between Bob and Alice was approximately 40 m. To minimize temporal variations in the channel, all measurements were collected over weekends or at night.

B. Experimental Setup

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 $\hat{\mathbf{h}}_c$), obtained using the configurations shown in Fig. 10(a) and (b) respectively. In both cases, an 8×8 multiple-input multiple-output (MIMO) channel sounder similar to that presented in [29] is used. The transmit signal consists 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 at the different nodes. Because the sounder only has 8 transmit ports one of which is needed for connection to Bob's antenna, only $N_{\mathrm{E}} = 7$ antennas are used in Eve's array.

The RECAP is connected to the MIMO channel sounder receiver, with RE biases controlled using an SPI-based digital-to-analog (D/A) converter. The FPGA-based SPI implementation is integrated with the channel sounder to allow synchronization between the antenna switch states in the MIMO measurement system and the RECAP states. For the 2-node configuration, Bob's antenna is connected to a single output of the sounder transmitter via a 20 m cable and Eve's antennas are connected to the remaining 7 transmit ports. The feed antenna on Alice's RECAP is connected to a single receive port. To avoid receiver saturation, 40 dB attenuators are placed between the transmitter outputs and Eve's antennas.

In the 3-node configuration, an additional high isolation ($>$ 80 dB) switch is used to connect Eve's antennas to the transmit ports (allowing measurement of $\hat{\mathbf{h}}_b$) or to the receive ports (allowing measurement of $\hat{\mathbf{h}}_c$). Eve's low transmission power of -20 dBm again avoids receiver saturation. Bob is implemented using a third radio node with a switch selectively connecting a 23 dBm transmit signal or a terminator to the power amplifier driving Bob's antenna.

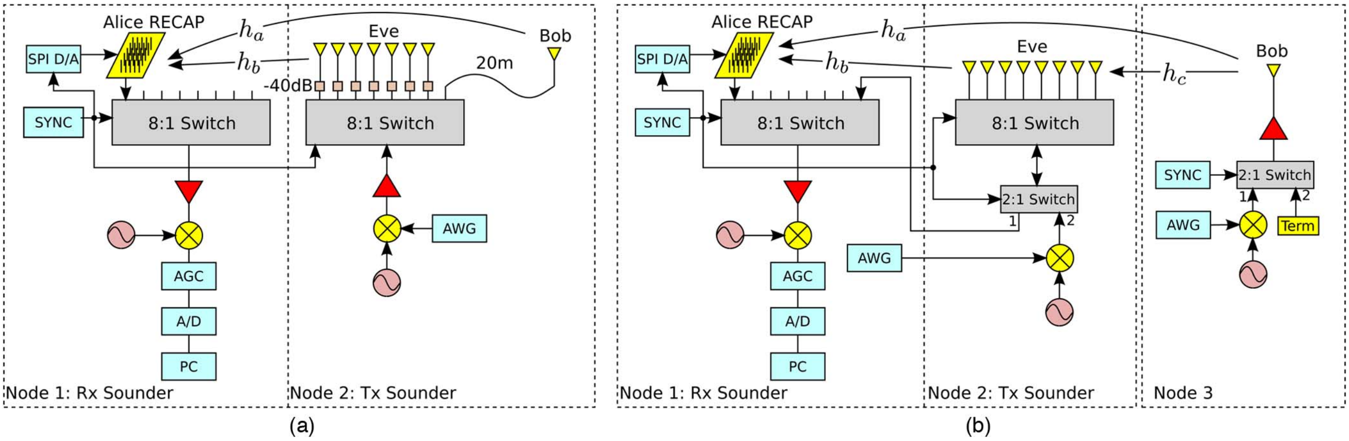

Fig. 10. 2-node and 3-node configurations used to measure channel responses for the legitimate nodes (Alice and Bob) and eavesdropper (Eve). (a) 2-node measurement; (b) 3-node measurement.

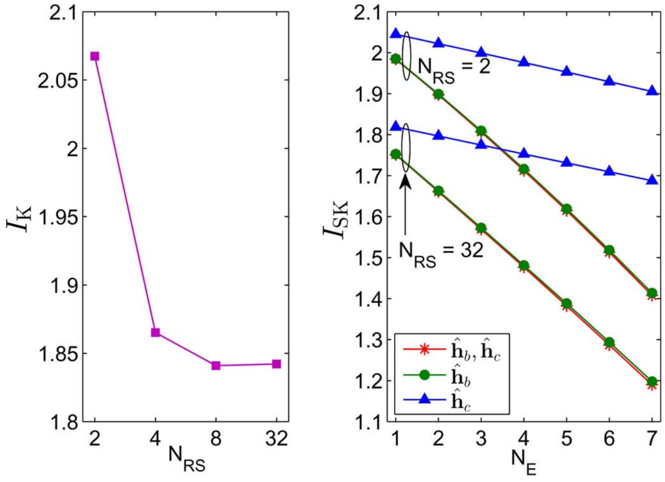

Fig. 11. Measured I_{K} as a function of N_{RS} for $N_{\mathrm{E}} = 7$ and I_{SK} as a function of N_{E} for two values of N_{RS} (both use $N_{\mathrm{RE}} = 24$) at indoor Location 1 using a 3-node measurement setup when Eve knows $\hat{\mathbf{h}}_b$ alone, $\hat{\mathbf{h}}_c$ alone, or both $\hat{\mathbf{h}}_b$ and $\hat{\mathbf{h}}_c$.

C. Results

All measured results use 10^6 channel snapshots to compute covariance matrices using the Gaussian assumption or expectations using the numerical method. All of the results 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.

1) Relative Importance of Eve's Channels: We once again explore the relative importance of $\hat{\mathbf{h}}_b$ and $\hat{\mathbf{h}}_c$ in terms of revealing information to Eve. As explained in Section IV-C, we consider cases where Eve knows $\hat{\mathbf{h}}_b$, $\hat{\mathbf{h}}_c$ or both. Fig. 11 plots I_{K} and I_{SK} for a 3-node measurement conducted at indoor Location 1 when $N_{\mathrm{RE}} = 24$. These results confirm that $\hat{\mathbf{h}}_c$ provides little information to Eve. As a result of this observation, we again assume that Eve only knows $\hat{\mathbf{h}}_b$ in the remainder of this analysis, allowing use of the data from the simpler 2-node measurements. Interestingly, the security metrics appear to be higher for Location 1 as compared to other locations. Since the SNR is fixed in the analysis, the higher metrics are likely due to more favorable multipath.

2) Security vs. Antenna Complexity: Fig. 12(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 difference between the results of the uncorrected and corrected Gaussian assumption observed in the measurements, which for certain circumstances reaches 5%, is larger than that observed in the simulations. As expected, I_{K} decreases with increasing N_{RS}, emphasizing that $N_{\mathrm{RS}} = 2$ again leads to the highest number of key bits per channel observation.

Fig. 12(b)–(e) 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 four indoor measurement locations. I_{SK} decreases as N_{E} increases, confirming the trend observed in the simulations. For this NLOS scenario, provided that Alice has a RECAP with high reconfigurability (large N_{RE}), 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%.

3) Dependence on Eve's Array Size: Fig. 13 compares selected results for I_{SK} from Fig. 12 obtained in the indoor environment to comparable results obtained in the outdoor environment. These curves show that the decrease in I_{SK} with increasing N_{E} is more dramatic for outdoor channels than for the indoor channels, likely due to the fact that the outdoor scenario is characterized by a dominant LOS path while the indoor scenario has stronger multipath components. Even when N_{RE} is large, the value of I_{SK} for $N_{\mathrm{E}} = 7$ is approximately 20% of the value obtained for $N_{\mathrm{E}} = 1$, showing the vulnerability created by the LOS channel that allows Eve to better predict the channels observed at the legitimate nodes.

4) Dependence on Eve's Array Configuration: We have assumed Eve's array surrounds the RECAP, since it is expected that this configuration would allow Eve to best sample the random radiation states of the antenna and track the key generation process. Arguably, this situation would not be feasible in practice, and one may ask if a more natural array configuration for the eavesdropper would exhibit the same behavior. To explore this idea, we have processed each measured data set to determine which subset of Eve's antennas gives the lowest I_{SK} for a given N_{E}, thus indicating the best that Eve can do with a smaller, more practical array.

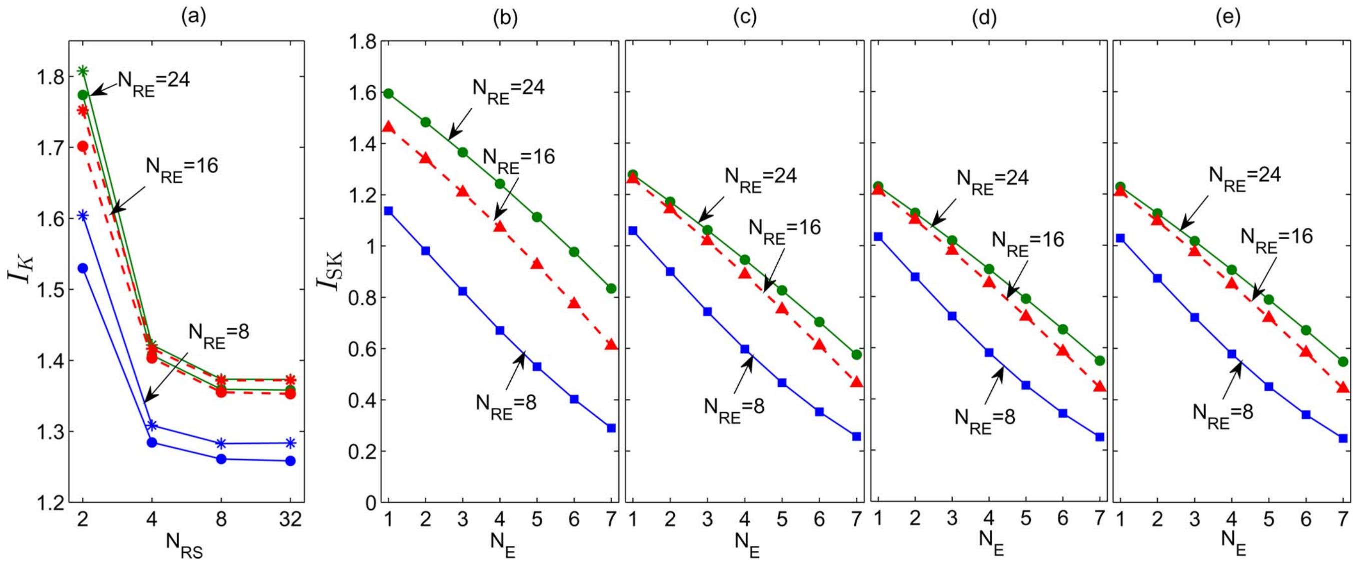

Fig. 12. Measured I_{K} and I_{SK} as a function of N_{E} for different values of N_{RE} and N_{RS}, where I_{K} curves marked with $*$ and $\bullet$ are respectively obtained using the uncorrected and corrected Gaussian assumption: (a) I_{K}, (b)–(e) I_{SK}.

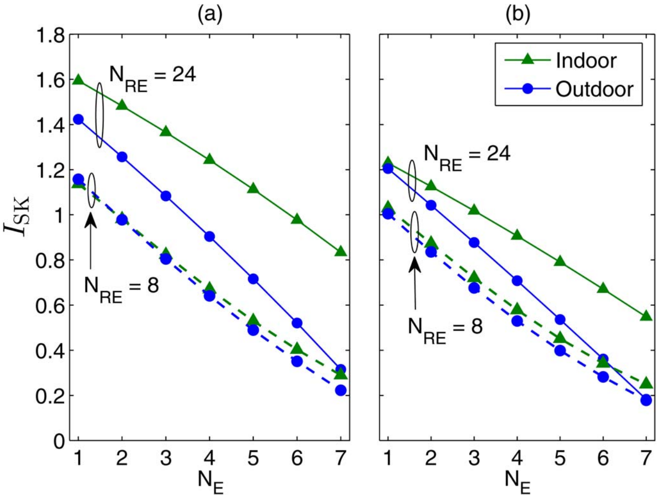

Fig. 13. Measured values of I_{SK} as a function of N_{E} for different values of N_{RE} and N_{RS}, where the curves for indoor and outdoor measurements represent averages over all experimental results.

Fig. 14 depicts two sets of curves. In the first case, I_{SK} is averaged over all possible Eve configurations for a given N_{E}, shown by solid lines. In the second case, we identify Eve's array configuration for each data set that produces the worst-case I_{SK} for a given N_{E}, shown by dashed lines. The results show that for a target I_{SK} level, Eve can typically get by with 1–3 fewer antennas if she can pick her best configuration.

Fig. 15 shows the worst-case configurations of Eve's array for Location 2 for different array sizes at Eve. The results for this and other locations (not plotted) typically show that the worst-case configuration is for Eve to place her antennas on one side of Alice's RECAP. We suspect that this occurs due to a dominant LOS or quasi-LOS component that is present. Therefore, it appears that a more natural and compact array could be judiciously placed by an eavesdropper to obtain nearly the same security reduction as is seen with a full array that surrounds the RECAP.

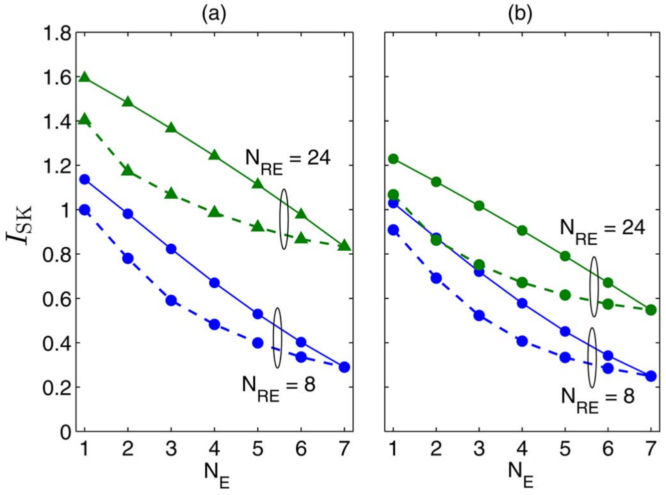

Fig. 14. Measured I_{SK} and as a function of N_{E} for different values of N_{RE} and N_{RS}, where solid and dashed curves are respectively obtained using average and worst case Eve antenna configuration (a) $N_{\mathrm{RS}} = 2$, (b) $N_{\mathrm{RS}} = 32$.

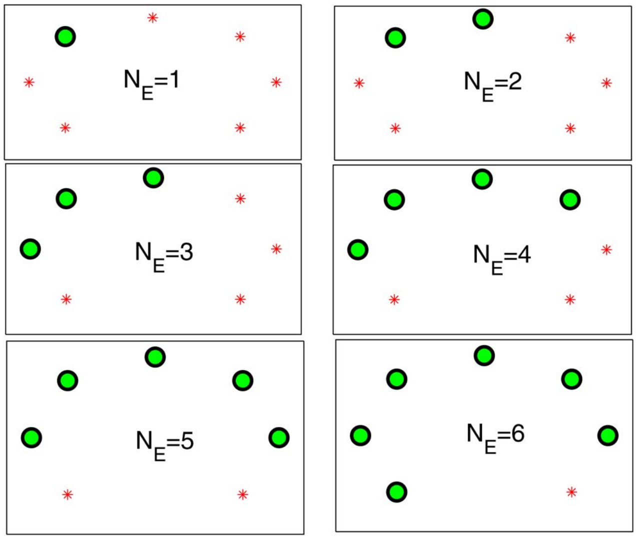

Fig. 15. Worst-case configuration of Eve's array for Location 2 (Hallway) where circles indicate positions of Eve's antennas.

VI. Conclusion

This work explores the effectiveness of using a highly-reconfigurable antenna to generate varying channel estimates that are in turn used to establish secret encryption keys in a time-division duplex communication system. The results demonstrate that an increase in the number of reconfigurable elements plays a vital role in increasing the number of key bits that can be securely generated, where diminishing returns are seen near $N_{\mathrm{RE}} = 16$ elements for the $1\lambda \times 1\lambda$ array size. The results also show that using only two impedance states per RE maximizes the number of bits available per RECAP state, meaning that simple switches may represent a practical RE termination. Simulations and measurements demonstrate that a compact 5×5 parasitic reconfigurable antenna can secure up to 50% of the available key bits in a NLOS scenario, even when an eavesdropper has an array surrounding the RECAP and a 3-dB SNR advantage. The findings show that RECAPs 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. Ahlswede and I. Csiszar, “Common randomness in information theory and cryptography. I. Secret sharing,” *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[3] U. Maurer and S. Wolf, “Secret-key agreement over unauthenticated public channels—Part I: Definitions and a completeness result,” *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 822–831, Apr. 2003.

[4] U. Maurer and S. Wolf, “Secret-key agreement over unauthenticated public channels-Part II: The simulatability condition,” *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 832–838, Apr. 2003.

[5] U. Maurer and S. Wolf, “Secret-key agreement over unauthenticated public channels—Part III: Privacy amplification,” *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 839–851, Apr. 2003.

[6] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, “Unconventional cryptographic keying variable management,” *IEEE Trans. Commun.*, vol. 43, no. 1, pp. 3–6, Jan. 1995.

[7] G. Van Assche, J. Cardinal, and N. J. Cerf, “Reconciliation of a quantum-distributed Gaussian key,” *IEEE Trans. Inf. Theory*, vol. 50, no. 2, pp. 394–400, Feb. 2004.

[8] C. Ye, A. Reznik, and Y. Shah, “Extracting secrecy from jointly Gaussian random variables,” in *Proc. IEEE Intl. Symp. Inf. Theory*, Seattle, WA, USA, Jul. 9–14, 2006, pp. 2593–2597.

[9] C. Ye, A. Reznik, G. Sternberg, and Y. Shah, “On the secrecy capabilities of ITU channels,” in *Proc. IEEE 66th Veh. Technol. Conf.*, Baltimore, MD, USA, Sep. 30–Oct. 3 2007, pp. 2030–2034.

[10] R. Wilson, D. Tse, and R. A. Scholtz, “Channel identification: Secret sharing using reciprocity in ultrawideband channels,” *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.

[11] A. Sayeed and A. Perrig, “Secure wireless communications: Secret keys through multipath,” in *Proc. IEEE Intl. Conf. Acoust., Speech, Signal Process.*, Las Vegas, NV, USA, Mar. 31–Apr. 4 2008, pp. 3013–3016.

[12] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, “Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel,” in *Proc. 14th ACM Intl. Conf. MobiCom*, San Francisco, CA, USA, Sep. 14–19, 2008, pp. 128–139.

[13] C. Ye *et al.*, “Information-theoretically secret key generation for fading wireless channels,” *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–254, Jun. 2010.

[14] J. Wallace, “Secure physical layer key generation schemes: Performance and information theoretic limits,” in *Proc. IEEE Intl. Conf. Commun.*, Dresden, Germany, Jun. 14–18, 2009, pp. 1–5.

[15] J. W. Wallace and R. K. Sharma, “Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis,” *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 381–392, Sep. 2010.

[16] C. Chen and M. A. Jensen, “Secret key establishment using temporally and spatially correlated wireless channel coefficients,” *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 205–215, Feb. 2011.

[17] T.-H. Chou, S. C. Draper, and A. M. Sayeed, “Secret key generation from sparse wireless channels: Ergodic capacity and secrecy outage,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1751–1764, Sep. 2013.

[18] T. Aono, K. Higuchi, M. Taromaru, T. Ohira, and H. Sasaoka, “Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels,” *IEEE Trans. Antennas Propag.*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005.

[19] R. Mehmood and J. W. Wallace, “Wireless security enhancement using parasitic reconfigurable aperture antennas,” in *Proc. Eur. Conf. Antennas Propag.*, Rome, Italy, Apr. 11–15, 2011, pp. 2761–2765.

[20] R. Mehmood and J. W. Wallace, “Experimental assessment of secret key generation using parasitic reconfigurable aperture antennas,” in *Proc. Eur. Conf. Antennas Propag.*, Prague, Czech Republic, Mar. 26–30, 2012, pp. 1151–1155.

[21] J. H. Schaffner *et al.*, “Reconfigurable aperture antennas using RF mems switches for multi-octave tunability and beam steering,” in *Proc. IEEE Antennas Propag. Soc. Intl. Symp.*, Salt Lake City, UT, USA, Jul. 16–21, 2000, vol. 1, pp. 321–324.

[22] L. N. Pringle *et al.*, “A reconfigurable aperture antenna based on switched links between electrically small metallic patches,” *IEEE Trans. Antennas Propag.*, vol. 52, no. 6, pp. 1434–1445, Jun. 2004.

[23] D. S. Linden, “A system for evolving antennas in-situ,” in *Proc. NASA/DoD Conf. Evolvable Hardware*, Long Beach, CA, USA, Jul. 12–14, 2001, pp. 249–255.

[24] C. M. Coleman, E. J. Rothwell, and J. E. Ross, “Investigation of simulated annealing, ant-colony optimization, genetic algorithms for self-structuring antennas,” *IEEE Trans. Antennas Propag.*, vol. 52, no. 4, pp. 1007–1014, Apr. 2004.

[25] B. A. Cetiner *et al.*, “Multifunctional reconfigurable MEMS integrated antennas for adaptive MIMO systems,” *IEEE Commun. Mag.*, vol. 42, no. 12, pp. 62–70, Dec. 2004.

[26] A. Grau and F. De Flaviis, “A distributed antenna tuning unit using a frequency reconfigurable PIXEL-antenna,” in *Proc. Eur. Conf. Antennas Propag.*, Barcelona, Spain, Apr. 12–16, 2010, pp. 1–5.

[27] R. Mehmood and J. W. Wallace, “MIMO capacity enhancement using parasitic reconfigurable aperture antennas (RECAPs),” *IEEE Trans. Antennas Propag.*, vol. 60, no. 2, pp. 665–673, Feb. 2012.

[28] R. Mehmood and J. W. Wallace, “Diminishing returns with increasing complexity in reconfigurable aperture antennas,” *IEEE Antennas Wireless Propag. Lett.*, vol. 9, pp. 299–302, 2010.

[29] B. Maharaj, J. Wallace, M. Jensen, and L. Linde, “A low-cost open-hardware wideband multiple-input multiple-output (MIMO) wireless channel sounder,” *IEEE Trans. Instrum. Meas.*, vol. 57, no. 10, pp. 2283–2289, Oct. 2008.

Rashid Mehmood (S’05) received the B.Sc. (*cum laude*) degree in communication systems engineering from the Institute of Space Technology (IST), Islamabad, Pakistan, in 2007 and the M.Sc. degree in electrical engineering from Jacobs University Bremen (JUB), Bremen, Germany, in 2010. He is currently working toward the Ph.D. degree in electrical engineering with the Department of Electrical Engineering, Brigham Young University (BYU), Provo, UT, USA. From 2011 to 2012, he worked as a Research Associate at JUB. His current research interests include reconfigurable antennas, optimization techniques, physical-layer security, and wireless communications. He was a recipient of the IEEE AP-S Undergraduate Research Award in 2009 and the BYU High Impact Doctoral Research Assistantship Award in 2012.

Jon W. Wallace (S'99–M'03–SM'13) received the B.S. (*summa cum laude*) and Ph.D. degrees in electrical engineering from Brigham Young University (BYU), Provo, UT, USA, in 1997 and 2002, respectively. Until 2002, he worked as a Graduate Research Assistant at BYU. From 2002 to 2003, he was with the Mobile Communications Group, Vienna University of Technology, Vienna, Austria. From 2003 to 2006, he was a Research Associate with the BYU Wireless Communications Laboratory, BYU. From 2006 to 2012, he was an Assistant Professor with the School of Engineering and Science, Jacobs University Bremen, Bremen, Germany. From 2012 to 2014, he was a Senior Design Engineer with Wavetronix, LLC, Provo, researching advanced radar technologies. He is currently an Associate Professor of electrical engineering with Lafayette College, Easton, PA, USA. His current research interests include physical-layer security, MIMO communications and radar, and reconfigurable antennas. He has served as an Associate Editor for the IEEE TRANSACTIONS ON ANTENNAS AND PROPAGATION and the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. He was a recipient of the National Science Foundation Graduate Fellowship in 1998.

Michael A. Jensen (S'93–M'95–SM'01–F'08) received the B.S. and M.S. degrees from Brigham Young University (BYU), Provo, UT, USA, in 1990 and 1991, respectively, and the Ph.D. degree from the University of California, Los Angeles, CA, USA, in 1995, all in electrical engineering. Since 1994, he has been with the Department of Electrical and Computer Engineering, BYU, where he is currently a Professor. His research interests include antennas and propagation for communications, microwave circuit design, multi-antenna signal processing, and physical-layer security.

Dr. Jensen is currently a member of the Publications Committee for the IEEE Antennas and Propagation Society. He previously served as the Editor-in-Chief for the IEEE TRANSACTIONS ON ANTENNAS AND PROPAGATION and an Associate Editor for the same journal and for the IEEE ANTENNAS AND WIRELESS PROPAGATION LETTERS. He has been a member and a Chair of the Joint Meetings Committee for the IEEE Antennas and Propagation Society, a member of the society AdCom, and a Co-Chair or Technical Program Chair for six society-sponsored symposia. In 2002, he received the Harold A. Wheeler Applications Prize Paper Award in the IEEE TRANSACTIONS ON ANTENNAS AND PROPAGATION. He was elevated to the grade of IEEE Fellow in 2008 in recognition of his research on multi-antenna communications.