Experimental Assessment of Secret Key Generation Using Parasitic Reconfigurable Aperture Antennas

Rashid Mehmood and Jon W. Wallace
Jacobs University Bremen, Campus Ring 1, 28759 Bremen, Germany
E-mail: r.mehmood@ieee.org, wall@ieee.org

***Abstract*—The potential of automatically generating secret keys by randomly changing the state of a reconfigurable antenna is investigated through direct measurement. Measurements are performed with a 5×5 parasitic reconfigurable aperture (RECAP) antenna at 2.54 GHz in an indoor laboratory environment, illustrating that keys can be generated with physical-layer reciprocal channel key generation (RCKG) even in static or line-of-sight (LOS) conditions. Details of the parasitic array, varactor-diode reconfigurable elements, and network-analyzer based measurement setup are presented. Analysis of the data shows that secure key bits is lower when an eavesdropper is in the LOS path between legitimate nodes as opposed to a direction perpendicular to that path. It is also illustrated that the statistics of fading induced with the reconfigurable array are not strictly Gaussian for LOS channels. Encouragingly, measurements show that around 80% of generated key bits are secure even in the worst case conditions.**

I. Introduction

Channel security is one of the most important concerns of present wireless communication systems, and methods that exploit the physical channel to enhance security are gaining interest. One attractive feature of these physical-layer methods is that perfect information theoretic security can be guaranteed in some cases, which is the strongest possible notion of secure communications. As demonstrated in [1], a reciprocal time-varying channel can be exploited with low-complexity quantization algorithms to generate long secret keys that are secure with respect to even very close eavesdroppers (i.e. sub-wavelength separation). Unfortunately, such methods are of limited value in static or very slowly varying channels.

The work in [2] proposed the novel and useful idea of using a parasitic array to create artificial channel fading, allowing secret keys to be generated in static environments using a simple power comparator. To study the potential utility and possible limitations of this idea, this work considers similar reconfigurable architectures, but with more arbitrary complexity. Specifically, we consider reconfigurable aperture (RECAP) antennas, which are dense arrays of reconfigurable elements (REs). In a RECAP, each RE can have a number of reconfigurable states (RSs), which can be changed in order to alter the characteristics (radiation pattern and input impedance) of the aperture. Hence, by changing the states of REs randomly, artificial channel fluctuations can be generated.

In [3] it has been demonstrated through simulation that a high level of security (more than 90% of the generated key bits are secure) is possible using RECAPs, even in the case of line-of-sight (LOS) scenario when an eavesdropper is very close to one of the nodes. Further, the level of complexity required to avoid brute-force attacks and the non-Gaussian nature of synthesized channel fading were investigated.

The purpose of this paper is to present a recent experimental campaign to augment the results in [3] that were pure simulation, indicating that synthetic fading induced by reconfigurable architectures with sufficient complexity can indeed be used to produce secure keys in cases of practical interest. We consider the specific case where Alice and Bob are legitimate nodes with a RECAP and single monopole antenna, respectively, and Eve is equipped with a single monopole antenna near Alice. Specifically, we study how proximity of the eavesdropper with respect to the RECAP affects security, even in the case when the eavesdropper antenna is inside of the parasitic RECAP antenna. We also investigate the role of the Alice-Eve channel in leaking information about the secret key to Eve and the non-Gaussian nature of artificially induced channel fluctuations. Finally, we assess how security is affected when the eavesdropper is either on or perpendicular to the line-of-sight (LOS) path connecting the legitimate nodes.

The remainder of the paper is organized as follows: Section II briefly reviews how information-theoretic key-generation metrics can be computed numerically for channels with non-Gaussian statistics. Section III presents the measurement system and placement of the different nodes. Section IV describes the results of the measurement campaign and the salient observations. Some concluding remarks are provided in SectionV.

II. Information Theoretic Analysis

Information-theoretic secrecy metrics as presented in [3] for non-Gaussian channels are employed in this work. We consider a communications scenario consisting of two legitimate nodes (Alice and Bob) and an eavesdropper node (Eve), connected by the channels depicted in Figure 1. Bob and Alice have channel estimates $\hat{h}_a$ and $\hat{h}_{a'}$ and exploit reciprocity to generate a secret key, while Eve receives the estimated channels $\hat{h}_b$ and $\hat{h}_c$ that are used to try to steal the secret key. Available key bits (I_{K}) represents the maximum number of independent key bits that can be generated per observation of the channel, given by

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

978-1-4577-0919-7/12/$26.00 ©2011 IEEE

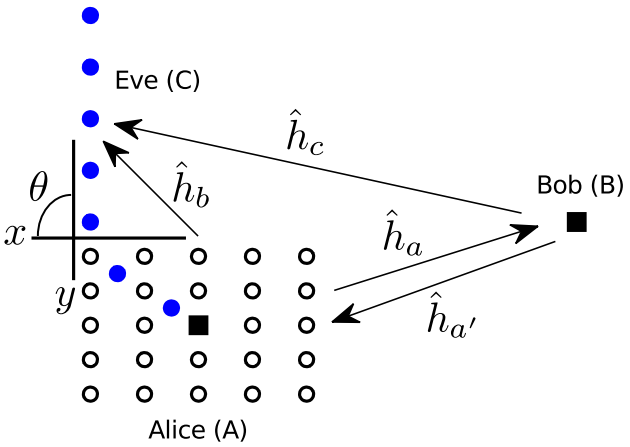

Fig. 1. Top view of nodes in the security measurements, where Bob and Eve have a single monopole antenna and Alice has a RECAP with many programmable REs (hollow circles). Black squares show the location of Bob's antenna and Alice's feed, while blue circles show the positions of Eve's antenna that were measured

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

Secure key bits (I_{SK}) represents the number of generated key bits per channel observation that are secure with respect to a specific eavesdropper, given by

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

Vulnerable key bits (I_{VK}) are defined as $I_{\mathrm{VK}} = I_{\mathrm{K}} - I_{\mathrm{SK}}$.

Since the fading statistics of synthetically generated channel fluctuations cannot be guaranteed to be Gaussian, closed-form expressions are not available for (1) and (2), and the method in [3] that is based on numerical computation of the required expectations is used. Note that 10 dB SNR is assumed for all computations of I_{K} and I_{SK} in this paper.

III. Measurement Configuration

This section outlines how the measurements were carried out, including information on the relative locations of the measurement nodes, the vector-network analyzer based measurement setup, and details on the RECAP antenna and required reconfigurable elements.

A. Relative Node Locations

Figure 1 depicts the basic configuration used for the channel measurements. Nodes A (Alice) and B (Bob) are legitimate users separated by 4.5 m, while Node C (Eve) is an eavesdropper close to Alice. Alice is equipped with a RECAP antenna used to induce random channel fluctuations, where the RECAP consists of a center feed (solid square) surrounded by multiple parasitic antennas (open circles). Several positions for Eve are considered (solid blue circles), including positions inside the RECAP near the feed and positions outside of the RECAP. Two values for the relative angle θ for the arrays

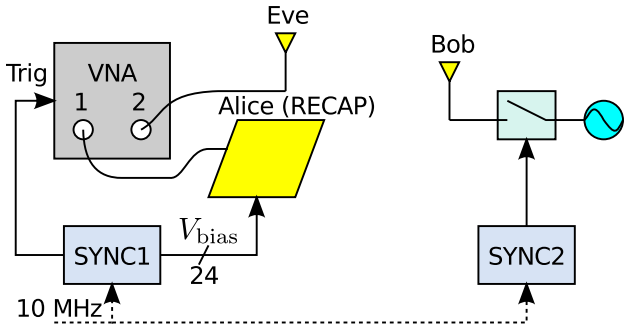

Fig. 2. Vector network analyzer based measurement setup

are considered, where for $\theta = 90°$ Eve is placed at positions perpendicular to the line-of-sight (LOS) path and for $\theta = 180°$ Eve is in the LOS path.

B. Channel Measurement setup

Figure 2 depicts the arrangement that was used to measure the three required channels ($h_a = h_{a'}$, h_b, h_c) with better than 20 dB SNR using a 2-port Rohde & Schwarz ZVB20 vector network analyzer (VNA). A continuous wave (CW) source at 2.54 GHz at Bob is fed to a microwave switch that allows RF to be selectively transmitted from Bob's single antenna. At the other side of the link, Alice's Feed and Eve's antenna are connected to the two ports of the network analyzer. Separate synchronization (SYNC) units [4] at Alice/Eve and Bob are synchronized with a common 10 MHz reference and used to orchestrate a two-phase measurement. During the first phase, Bob transmits (switch is on), the VNA internal source is off, and the incoming waves at the VNA ports $b_1 = h_{a'}$ and $b_2 = h_c$ are measured for 100 different RE states. During the second phase, Bob's antenna is switched off, Port 1 of the VNA is driven, and $S_{21} = h_b$ and $S_{11} = \Gamma_{\mathrm{RX}}$ (input RECAP reflection coefficient) are measured and stored for the same RE states as in phase one. Each phase requires 5 s, and therefore measurements are performed under quasi-static conditions, where repeatability of the results has been checked with back-to-back measurements. The two-phase measurement is repeated N times to obtain sufficient data to compute I_{K} and I_{SK}.

A limitation of the current setup is that although the relative phase $\phi_{ac} = \angle h_a - \angle h_c$ can be computed, the VNA trigger input does not have sufficient accuracy to allow the phase of h_b to be related to h_a and h_c. Thus, the data has been analyzed in two ways, depending on who we assume is able to use the relative phase information. In Case 1, we assume that Eve estimates the relative phase, and the legitimate nodes use only $|h_a|$ and $|h_{a'}|$ to generate a key. This can be considered a lower bound on I_{SK}, since Eve would only be able to estimate $\angle h_c$, not the relative phase. In Case 2, we assume that Alice can use ϕ_{ac}, but Eve only has access to $|h_c|$, representing an upper bound on I_{SK}. Note that when Eve is sufficiently far from Alice, the channel h_c is static (unaffected by the REs), and variation in ϕ_{ac} is due only to change in $\angle h_a$. Here, Case 2 is usually more appropriate, since Eve would not know anything

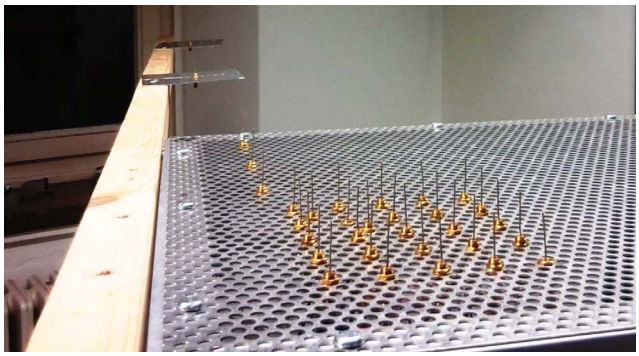

Fig. 3. Measurement setup depicting RECAP antenna at Alice (Node A) with 24 REs and different placement for Eve's antenna (Node C)

about $\angle h_a$. In addition to Cases 1 and 2, we also compute I_{SK} either including or excluding h_b, indicating how important this information is for Eve. Furthermore, we study the effect of change in reflection coefficient Γ_{RX}, which indicates the matching efficiency of the RECAP. Thus, a total of eight cases are considered for each measurement.

C. RECAP Antenna and REs

Figure 3 provides a photo of Alice and Eve in the measurement setup, which were located in laboratory room having dimensions 4.7 m $\times$ 13.5 m located on the Jacobs University campus. Note that line-of-sight (LOS) conditions were maintained in all the presented measurements. The RECAP antenna at Alice consists of a 5×5 array of parasitic monopole antennas confined to a $1\lambda\times1\lambda$ aperture over a finite ground plane. The center element is the feed while other 24 monopole antennas are terminated below with reconfigurable elements (REs).

Figure 4 shows the basic design of the varactor-diode-based reconfigurable element, including the circuit schematic, the printed-circuit-board with components, and the completed circuit with integrated SMA connector. As can be seen the circuit is a very compact design based on a single SMV1232 varactor diode providing a tunable capacitance from 1.05 pF to 4.15 pF for a reverse bias range from 0 to 5 volts. In order to enhance the phase shift given by the varactor diode in this reversed biased region, a 1.2 nH inductor is used in parallel, resulting in almost 200° phase shift corresponding to 0 to 5 volts at our target frequency of 2.54 GHz. In the measurements, the useful bias range of 1 to 5 volts was uniformly divided into 32 possible reconfigurable states.

Figure 5 plots the magnitude and phase of S_{11} of the reconfigurable element at 2.54 GHz using a Rohde & Schwarz VNB20 vector network analyzer. Although it can be seen that phase variation is very low from 0 to 1 volts, biases from 1 to 5 volts produce nearly linear phase variation with increasing reverse bias. The variation in the magnitude of S_{11} indicates that our simple RE circuit exhibits loss, which results mainly from the 1.2Ω series resistance of the varactor diode. The amplitude drop can be overcome by increasing the value of the inductor, but this also decreases the phase tunability of the RE. Since we feel that phase tunability is more important in this initial study than the absolute antenna efficiency, we have chosen to use the simple design in this research.

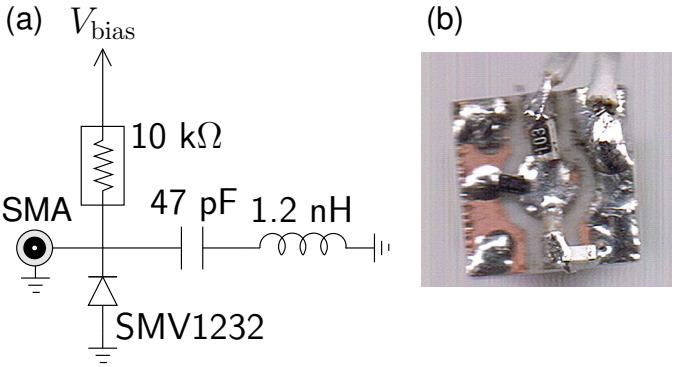

Fig. 4. Reconfigurable element circuit: (a) schematic, (b) printed-circuit board with components, (c) completed RE with SMA connector

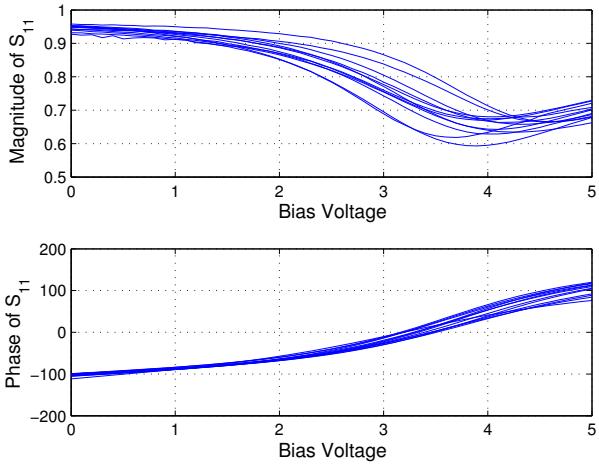

Fig. 5. Reflection coefficient of the 24 REs, indicating loss and phase tunability with respect to bias voltage

IV. Measurement Results

Figure 6 shows a representative result of the channel measurements for configuration $\theta = 180°$ where Eve is on the

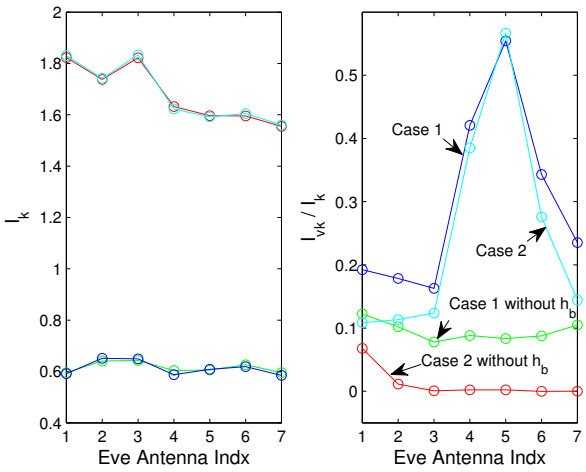

Fig. 6. I_{K} and $I_{\mathrm{VK}}/I_{\mathrm{K}}$ when the reduction in SNR due to Γ_{RX} is ignored, and Eve is on the LOS path of Alice-Bob ($\theta = 180°$). For Cases 1 and 2, relative phase information is assumed to be known only by Eve or the legitimate nodes, respectively. The effect of assuming Eve either with or without access to the Alice-Eve channel h_b is also considered.

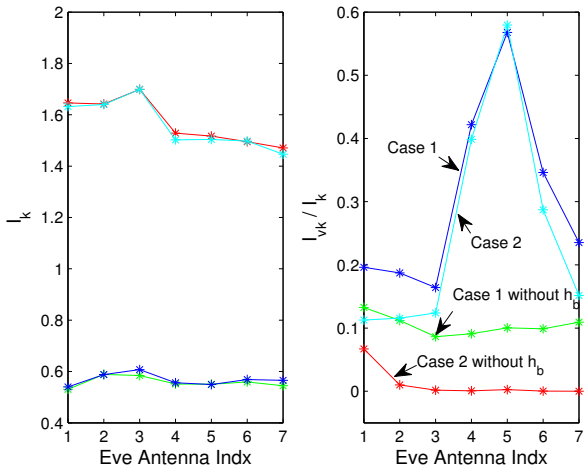

Fig. 7. I_{K} and $I_{\mathrm{VK}}/I_{\mathrm{K}}$ when the reduction in SNR due to Γ_{RX} is accounted for, and Eve is on the LOS path of Alice-Bob ($\theta = 180°$)

LOS path between the legitimate nodes and RECAP channels are normalized so that a reduction in SNR due to antenna mismatch is ignored. We expect that placing Eve on the LOS path will be the worst case for security, since for a single-path environment (ideal LOS), fluctuations in the Alice-Bob channel due to reconfigurability can be directly estimated by Eve using the Alice-Eve and Bob-Eve channels. Indices 1 through 7 for Eve's position correspond to separation distances of 0.17λ, 0.51λ, 0.85λ, 1.53λ, 2.21λ, 8.6λ, and 15.8λ between Eve's antenna and Alice's RECAP feed, where λ is the free-space wavelength. In this (and all other plots) we note that the number of available bits I_{K} is much smaller for Case 1 than Case 2, since Alice and Bob do not use phase information to generate key bits in Case 1. The plot also shows the relative vulnerable bits ($\mathrm{RVB} = I_{\mathrm{VK}}/I_{\mathrm{K}}$).

A number of observations can be made from the data. First, consider the case when we disregard h_b. In Case 2, relative phase information ϕ_{ac} is given to Alice/Bob, and RVB decreases to 0 as Eve moves farther away from Alice and her channel becomes insensitive to RE changes. Interestingly, for Case 1 when Eve is given ϕ_{ac}, RVB only drops to 0.1 even for large separation, indicating that knowing the phase ϕ_{ac} reveals some information about the magnitude $|h_a|$. Although not intuitive, this effect is due to the fact that when Eve is far, changes in ϕ_{ac} are only due to changes in $\angle h_a$, and the phase and magnitude of h_a are not completely independent for uniformly distributed RE phases.

Second, when h_b is included, we see that RVB is below 0.2 inside the array, increases to a peak value outside the array, and then begins to drop again. Although also not intuitive, the result is reasonable since if Eve is inside of Alice's RECAP, Eve will have a difficult time deducing the random pattern generated in Bob's direction from only a single near-field sample. As Eve moves outside of the RECAP, she is in the LOS path and h_b gives her information about the random pattern that Bob will see, leading to a higher RVB value.

Figure 7 shows the effect of taking the SNR reduction due to mismatch ($\Gamma_{\mathrm{RX}} \neq 0$) with varying RECAP state into account. It is observed that I_{K} drops only slightly in this case, which results from the fact that our RECAP presents a fairly good match for most RECAP states. We also see very little effect on the RVB.

Figure 8 shows the result for the same scenario when Eve is no longer on the LOS path ($\theta = 90°$), and in this case RVB is always below 0.25. This higher security is expected since Eve now observes fluctuations of the RECAP radiation pattern in a different direction than the LOS Alice-Bob channel, where that LOS channel is the one primarily exploited for key generation. Note that in Case 1, the phase information helps Eve (higher RVB), again due to dependence of the amplitude and phase of h_a. Figure 9 extends the result in Figure 8 to the case where change in SNR in now incorporated.

The channel distribution of h_a obtained using reconfigurable antennas to generate synthetic channel fluctuations is an important factor to study, since this fading may not follow a Gaussian distribution, not only complicating the computation of available and secure key bits, but also reducing security relative to the ideal Gaussian case. Below we compute empirical cdfs for the magnitude and phase of RECAP-induced channel fading and compare to the ideal Gaussian distribution.

Figure 10 shows the amplitude and phase distribution of h_a compared to the ideal Gaussian case both for Case 1 and Case 2. We observe that the amplitude distribution of h_a is the same as that of Gaussian, but the phase shows moderate deviation from a uniform distribution. Note that for Case 1, phase is just zero since it is normalized from the Alice-Bob channel h_a and instead used in Eve's channel h_c. Figure 11 shows the distribution of h_c at the various locations of Eve's antenna for Case 1, where Eve 1 corresponds to

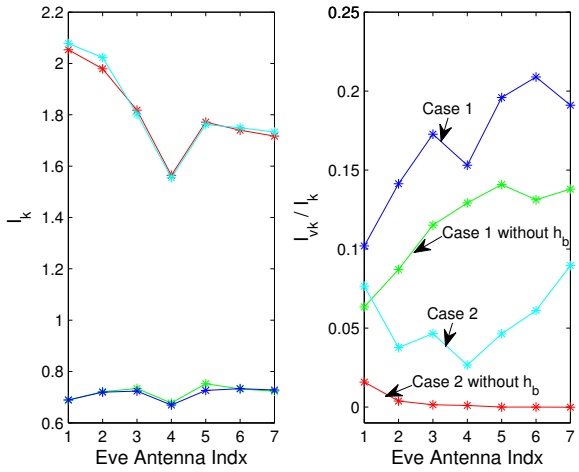

Fig. 8. I_{K} and $I_{\mathrm{VK}}/I_{\mathrm{K}}$ when the reduction in SNR due to Γ_{RX} is not considered, and Eve is not on the LOS path of Alice-Bob ($\theta = 90^{\circ}$)

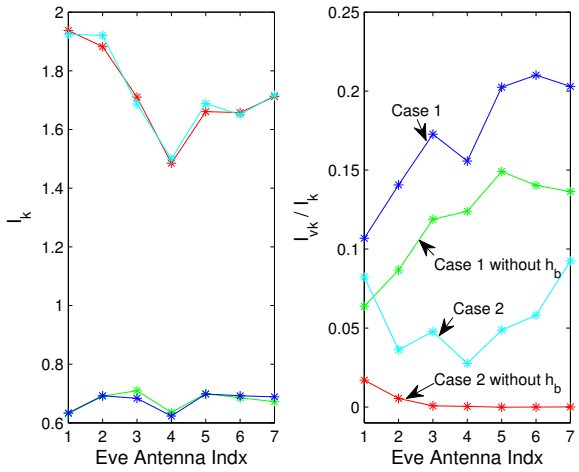

Fig. 9. I_{K} and $I_{\mathrm{VK}}/I_{\mathrm{K}}$ when the reduction in SNR due to Γ_{RX} is accounted for, and Eve is not on the LOS path of Alice-Bob ($\theta = 90^{\circ}$)

the position closest to the feed. It is observed that as we move away from the center of the RECAP, the variance of the amplitude distribution decreases as expected. Note that the cdf of the phase distribution deviates strongly from Gaussian for all considered separations, indicating that computation of I_{SK} must account for these non-Gaussian statistics.

V. Conclusion

In this work we have analyzed a practical RECAP structure equipped at the node near to Eve for generation of secret keys by inducing random fluctuations in the channel. A detailed design of the RECAP with the corresponding phase shift capability as well as the losses of REs have been presented. It has been observed that a high degree of security (where approximately 80% of the bits are secure) can be obtained using the RECAP provided that Eve is not lying in the LOS

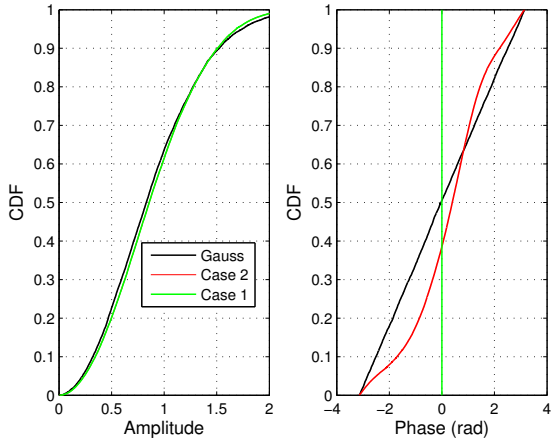

Fig. 10. Amplitude and phase cdfs of the channel h_a for Cases 1 and 2 and $\theta = 90^{\circ}$

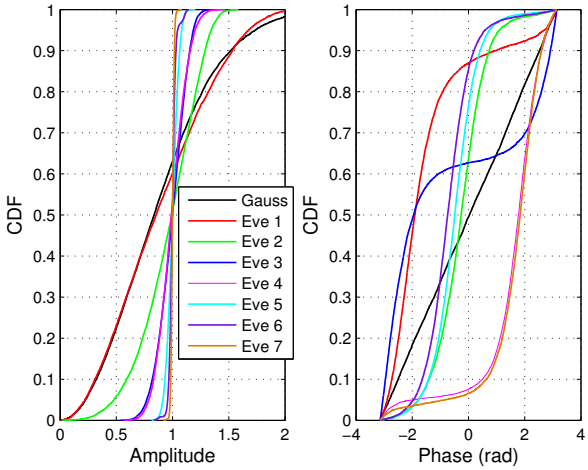

Fig. 11. Amplitude and phase cdfs of the channel h_c for Case 1 and $\theta = 180^{\circ}$

path between the two communicating nodes. Also, for the given RECAP complexity the statistics generated are similar to a Gaussian channel especially in terms of magnitude.

References

[1] J. Wallace and R. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Trans. Inf. Forensics and Security*, pp. 381–392, Sep. 2010.

[2] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas Propag.*, vol. 53, pp. 3776–3784, Nov. 2005.

[3] 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.

[4] B. T. Maharaj, J. W. Wallace, M. A. Jensen, and L. P. Linde, "A low-cost open-hardware wideband multiple-input multiple-output (MIMO) wireless channel sounder," *IEEE Trans. Instrum. Meas.*, vol. 57, pp. 2283 – 2289, Oct. 2008.