Wireless Security Enhancement 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 ability of parasitic reconfigurable aperture (RECAP) antennas to generate secret keys is investigated, which allows physical-layer reciprocal channel key generation (RCKG) methods to be employed even in the case of static and line-of-sight channels. Since the artificial channel fluctuations created by RECAP structures are not necessarily Gaussian, a numerical procedure for computing available and secure key bits is developed that is applicable to channels with arbitrary fading. It is identified that for limited RECAP complexity, a reduced-complexity brute-force attack is possible, and a lower bound on the required RECAP complexity to avoid this possibility is developed. Numerical examples of a 9×9 parasitic RECAP with varying levels of complexity illustrate the importance of controlling the reflection coefficient to ensure Gaussian statistics, the need for sufficient complexity to attain maximum secure key bits, and the importance of placing the RECAP on the node near the eavesdropper.**

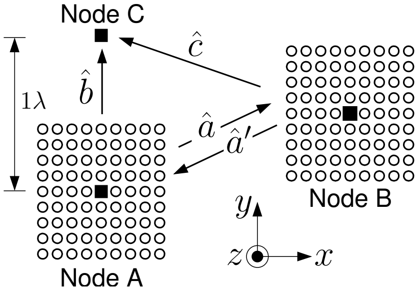

Fig. 1. System model for secure communications provided by RECAPs at legitimate Nodes A and B, and Node C is an eavesdropper. Active antenna (feed) denoted by squares and circles are parasitic reconfigurable elements.

I. Introduction

Security is a vital consideration for today's wireless communications systems, and there is growing interest in physical layer security methods that exploit the antennas and propagation channel to provide an additional layer of protection over existing cryptographic techniques. One such method involves generating secret keys from random reciprocal channel fluctuations [1, 2], allowing keys to be automatically generated at two nodes without the need for secret information to be shared a priori. As shown in [1], very long keys can be generated rapidly for fading, non line-of-sight (NLOS) channels that exhibit Gaussian statistics and low temporal correlation of channel observations. However, such methods will be hindered by channels with high temporal correlation, like line-of-sight (LOS) and static channels.

The ability to improve security by inducing artificial channel fading with reconfigurable parasitic arrays was introduced in [3], allowing reciprocal channel key generation (RCKG) to be applied to both LOS and static channels. Although this represents a very encouraging solution for applying RCKG in quasi-static situations, there are several outstanding questions that need to be addressed: Are artificially induced channel fluctuations as secure as naturally occurring ones, and does the channel richness (number of multiple paths) affect this? For limited antenna reconfigurability is it possible for an eavesdropper to use the limited number of antenna states to easily learn the key? If so, how much reconfigurability is necessary to avoid this possibility? What is the distribution of channels created by reconfigurable antennas, and can they be made Gaussian by careful system design? In the case that signals are not Gaussian, how can the secrecy capacity be efficiently computed, and how much security is lost due to non-Gaussian fading?

This paper provides initial answers to these questions based on simulated channel fading that is created by a parasitic reconfigurable aperture (RECAP) antenna [4, 5]. Simulations are performed for the case where transmit and/or receive employ RECAPs and an eavesdropper is near one of the nodes, allowing both the available key bits per channel observation and those secure from the eavesdropper to be analyzed. The complexity of the RECAP can be arbitrarily scaled to determine the minimum level needed for secure key generation and how the key generation rate scales with additional complexity. Channel fading induced by the RECAP is found to be non-Gaussian, unless the input reflection coefficient is carefully controlled. An efficient method for computing information theoretic secrecy metrics for non-Gaussian channels is developed, and it is demonstrated that significant secrecy capacity is lost when reflection coefficient is not controlled.

II. System Model and RECAP Antenna

Figure 1 shows the system model considered in our analysis, consisting of two communicating nodes that represent the legitimate users (Node A and Node B) and an eavesdropper (Node C). The forward and reverse channels estimated at the legitimate nodes are $\hat{a}$ and $\hat{a}'$, while channels $\hat{b}$ and $\hat{c}$ are assumed to be known to the eavesdropper. As shown in [1], when channels $\hat{b}$ and $\hat{c}$ are independent of channels $\hat{a}$ and $\hat{a}'$, keys generated via RCKG are perfectly secure. It was also shown through direct measurement that for real indoor fading, most key bits are secure from the eavesdropper even when the eavesdropper is very close to one of the nodes.

The RECAP antenna considered in this work is shown in Figure 1, consisting of a 2-dimensional 9×9 square array of half-wave dipoles [4] and occupying an area of $1\lambda \times 1\lambda$ in the xy plane and height $\lambda/2$ in z, where the center dipole is the feeding element and other elements are terminated with electrically tunable capacitive loads.

The complexity or amount of reconfigurability of the RECAP is defined in terms of the number of reconfigurable

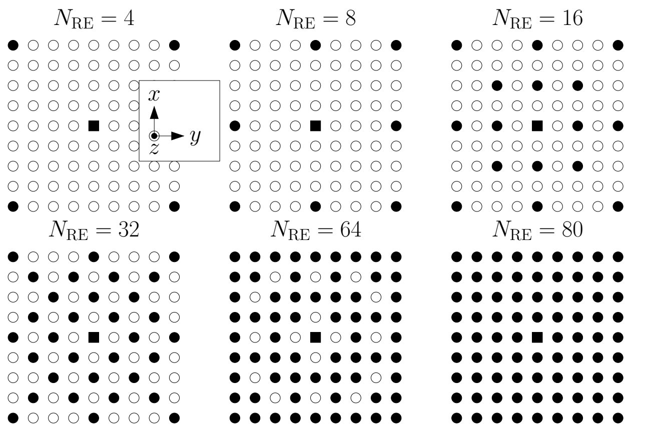

Fig. 2. RECAP structure consisting of a 9×9 dipole array, where $N_{\rm RE}$ elements are terminated with REs (filled circles) and the center element is the feed. Dipoles are aligned along the z axis (extend out of the page).

elements ($N_{\rm RE}$) and the number of reconfigurable states ($N_{\rm RS}$), representing the number of dipoles that are loaded with a tunable capacitance and the number of different capacitance values that can be realized, respectively. Figure 2 shows the distribution of reconfigurable elements over the whole aperture for different $N_{\rm RE}$.

III. Information Theoretic Analysis

Information-theoretic secrecy metrics were presented in [1] and are employed in this work. Available key bits ($I_{\rm K}$) represent the number of independent key bits that can be generated per observation of the random channel by the two nodes, whereas ($I_{\rm SK}$) is the number of secure key bits or those that are safe from a specific eavesdropper. The number of vulnerable key bits is defined as $I_{\rm VK} = I_{\rm K} - I_{\rm SK}$.

A. Key Generation Rate Metrics

The analysis in [1] assumed Gaussian channels, allowing secrecy capacity to be computed in terms of channel covariances alone. Since it is not known whether the distribution of channels generated with the RECAP will be Gaussian, this paper develops a numerical technique that allows $I_{\rm K}$ and $I_{\rm SK}$ to be computed directly from Monte-Carlo simulations.

Consider the computation of available key bits

$$I_{\rm K} = {\rm E} \log_2 \frac{f(\hat{a}, \hat{a}')}{f(\hat{a}) f(\hat{a}')}, \tag{1}$$

where ${\rm E}\{\cdot\}$ with and without a subscript indicates expectation over the subscripted random variables, or *all* random variables in the expression, respectively. Random variables $\hat{a}$ and $\hat{a}'$ are the jointly distributed channel estimates at Nodes B and A, respectively, of the ideal reciprocal channel $a = a'$, and $f(\cdot)$ is a probability density function (pdf) of the named arguments. In our case, $\hat{a}$ and $\hat{a}'$ may follow a non-Gaussian distribution, and the pdf $f(\hat{a}, \hat{a}')$ is not known. However, since the estimation error at nodes A and B can be considered independent, the conditional pdf $f(\hat{a}, \hat{a}|a)$ is just the product of two known noise pdfs for additive noise. Using this fact

$$\begin{aligned} f(\hat{a}, \hat{a}') &= \int f(\hat{a}, \hat{a}'|a) f(a) da = {\rm E}_a f(\hat{a}, \hat{a}'|a), && (2) \\ &= {\rm E}_a \{ f_n[(\hat{a} - a)/\sigma_a] \, f_n[(\hat{a}' - a)/\sigma_{a'}]\}, && (3) \end{aligned}$$

where $f_n(\cdot)$ is a unit variance complex Gaussian pdf, and σ_a^2 and $\sigma_{a'}^2$ are estimation error variance at Nodes B and A, respectively. Likewise, we have

$$\begin{aligned} f(\hat{a}) &= {\rm E}_a f(\hat{a}|a) = {\rm E}_a f_n[(\hat{a} - a)/\sigma_a], && (4) \\ f(\hat{a}') &= {\rm E}_a f(\hat{a}'|a) = {\rm E}_a f_n[(\hat{a}' - a)/\sigma_{a'}]. && (5) \end{aligned}$$

Combining (3)-(5) with (1) allows $I_{\rm K}$ to be computed with a direct Monte-Carlo procedure without any need to empirically estimate the pdfs of the artificial non-Gaussian channels. First, we observe M random realizations of $\hat{a}$ and $\hat{a}'$ (jointly distributed) denoted $\hat{a}_m$, $\hat{a}'_m$. For each of these realizations, we observe N random realizations of a (independent of $\hat{a}$ and $\hat{a}'$), denoted a_{mn}. The mutual information is estimated using

$$I_{\rm K} \approx \frac{1}{M} \sum_m \log_2 \frac{N \sum_n f(\hat{a}_m, \hat{a}'_m | a_{mn})}{\sum_{n'} f(\hat{a}_m | a_{mn'}) \sum_{n''} f(\hat{a}'_m | a_{mn''})}. \tag{6}$$

Safe key bits $I_{\rm SK}$ are defined as

$$I_{\rm SK} = I(\hat{a}; \hat{a}' | \hat{b}, \hat{c}) = E \log_2 \frac{f(\hat{a}, \hat{a}' | \hat{b}, \hat{c})}{f(\hat{a}|\hat{b}, \hat{c}) f(\hat{a}'|\hat{b}, \hat{c})}, \tag{7}$$

and a similar Monte-Carlo procedure can be employed after establishing the following theorem for conditional distributions.

Theorem 1: $f(x, y|z) = \int f(x, y|z, \alpha) f(\alpha|z) d\alpha$.

Proof:

$$\begin{aligned} \int f(x, y|z, \alpha) f(\alpha|z) d\alpha &= \int \frac{f(x, y, z, \alpha)}{f(z, \alpha)} \frac{f(z, \alpha)}{f(z)} d\alpha && (8) \\ &= \frac{1}{f(z)} \int f(x, y, z, \alpha) d\alpha && (9) \\ &= \frac{f(x, y, z)}{f(z)} = f(x, y|z). && (10) \end{aligned}$$

■

Theorem 1 can be used to compute the unknown pdf $f(x, y|z)$ when we have knowledge of the conditional distribution $f(x, y|z, \alpha)$.

The unknown pdfs in (7) can be obtained using Theorem 1 and a Monte-Carlo procedure. Specifically,

$$\begin{aligned} f(\hat{a}, \hat{a}'|\hat{b}, \hat{c}) &= \int f(\hat{a}, \hat{a}'|\hat{b}, \hat{c}, a, b, c) f(a, b, c|\hat{b}, \hat{c}) da\, db\, dc, && (11) \\ &= \int \frac{f(\hat{a}, \hat{a}'|\hat{b}, \hat{c}, a, b, c) f(\hat{b}, \hat{c}|a, b, c)}{f(\hat{b}, \hat{c})} f(a, b, c) da\, db\, dc && (12) \\ &= \frac{1}{f(\hat{b}, \hat{c})} {\rm E}_{abc} \Big\{ f(\hat{a}, \hat{a}'|a) f(\hat{b}, \hat{c}|b, c) \Big\}, && (13) \end{aligned}$$

where the second equality comes from applying Bayes' rule to the second term under the integral, and the removal of conditioning variables in the last equality results from conditional independence. Likewise, the pdfs in the denominator of (7) are

$$\begin{aligned} f(\hat{a}|\hat{b}, \hat{c}) &= \frac{1}{f(\hat{b}, \hat{c})} {\rm E}_{abc} \Big\{ f(\hat{a}|a) f(\hat{b}, \hat{c}|b, c) \Big\}, && (14) \\ f(\hat{a}'|\hat{b}, \hat{c}) &= \frac{1}{f(\hat{b}, \hat{c})} {\rm E}_{abc} \Big\{ f(\hat{a}'|a) f(\hat{b}, \hat{c}|b, c) \Big\}. && (15) \end{aligned}$$

Combining these results, we have

$$I_{\rm SK} = {\rm E} \log_2 \frac{{\rm E}_{abc} \Big\{ f(\hat{a}, \hat{a}'|a) f(\hat{b}, \hat{c}|b, c) \Big\} f(\hat{b}, \hat{c})}{{\rm E}_{abc} \Big\{ f(\hat{a}|a) f(\hat{b}, \hat{c}|b, c) \Big\} {\rm E}_{abc} \Big\{ f(\hat{a}'|a) f(\hat{b}, \hat{c}|b, c) \Big\}}. \tag{16}$$

Although this looks more complicated than the original expression, note that each of the pdfs involves estimated channels conditioned on the actual channel, and is given directly in terms of the noise pdfs alone. The required pdfs are

$$f(\hat{a}, \hat{a}'|a) = f_n[(\hat{a} - a)/\sigma_a]\, f_n[(\hat{a}' - a)/\sigma_{a'}], \tag{17}$$

$$f(\hat{b}, \hat{c}|b, c) = f_n[(\hat{b} - b)/\sigma_b]\, f_n[(\hat{c} - c)/\sigma_c], \tag{18}$$

$$f(\hat{b}, \hat{c}) = \mathrm{E}_{b,c} f(\hat{b}, \hat{c}|b, c), \tag{19}$$

(4), and (5). As before the Monte-Carlo procedure operates by observing M joint random realizations of the estimated channels ($\hat{a}_m$, $\hat{b}_m$, and $\hat{c}_m$) and for each of these generating N random realizations of the ideal channels (a_{mn}, b_{mn}, and c_{mn}) to compute the inner expectations for each m.

Although not presented in this paper, this numerical procedure for computing I_{K} and I_{SK} has been validated using correlated Gaussian channels and available closed form expressions.

B. *Brute-Force Attack for Low RECAP Complexity*

A potential concern for RECAP-induced channel fluctuations is that if total number of states for RECAPs at Node A and B is too limited, a reduced complexity brute-force attack may be possible. Consider the worst case where Node C has very high SNR, so that the channels b and c are almost exactly observed. For a static propagation channel, Node C observes a 4-dimensional constellation of points (from 2 complex channels) as Nodes A and B pick random RECAP states. Although Node C does not know the *mapping* of key bits to the observed constellation points, it can record the *sequence* of constellation points. If the combined RECAP complexity is too low, Node C can learn the key by simply trying all possible mappings, which may be less complex than trying all possible key sequences.

One way to avoid this possibility is to consider how many total secure key bits (N_{bits}) must be generated during static channel conditions. By making the combined RECAP complexity large enough, such that the number of possible mappings to search is larger than $2^{N_{\mathrm{bits}}}$, a reduced-complexity brute-force attack is avoided. Given a single RECAP at one of the communicating nodes with N_{RE} reconfigurable elements and N_{RS} states, the total number of RECAP states is $N_{\mathrm{RS}}^{N_{\mathrm{RE}}}$. For a quantization order of M symbols per channel observation, each constellation point has M possible mappings. Thus, the total combination of mappings to check for all constellation points is $M^{(N_{\mathrm{RS}}^{N_{\mathrm{RE}}})}$ and we require

$$N_{\mathrm{RS}}^{N_{\mathrm{RE}}} \log_2 M \geq N_{\mathrm{bits}} \tag{20}$$

to avoid a reduced-complexity brute-force attack. Figure 3 plots the left-hand-side of (20) for $M = 4$ and various values of N_{RE} and N_{RS}, indicating that for RECAPs with modest complexity, a very large number of key bits can be generated securely under static conditions. This also suggests the interesting possibility of using analog noise-like sources to bias the reconfigurable elements, creating a virtually infinite number of reconfigurable states, which appears to completely remove the possibility of the reduced-complexity attack.

IV. Security analysis of RECAP-induced fading

Consider the scenario depicted in Figure 1, where Nodes A and B are equipped with RECAPs and the single-antenna eavesdropper is in close proximity (1λ separation) to Node A. The channel from Node B to Nodes A and C is computed using a path-based channel model with varying numbers of multipath (N_{path}). Two methods of randomly changing the RECAP loads are considered to create artificial fading: Case 1) RE states are selected randomly (uniformly) within the set of configurations providing a reflection coefficient $|\Gamma|^2 < 0.1$, and Case 2) RE states are selected randomly without considering the reflection coefficient.

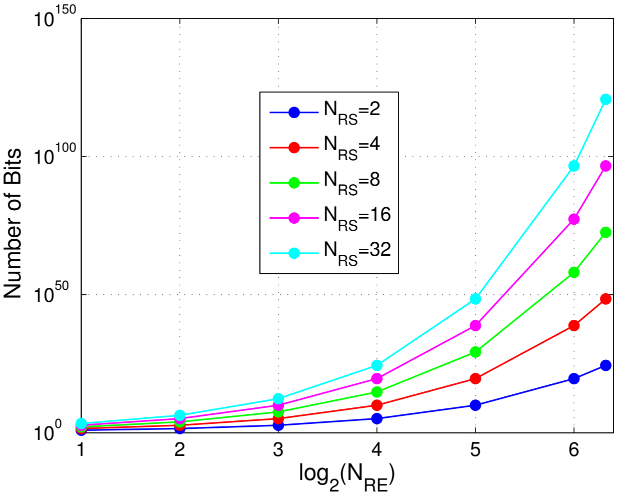

Fig. 3. Maximum key bits that can be securely generated with a RECAP with limited complexity under static conditions

Figure 4 plots available key bits (I_{K}) and fraction of vulnerable key bits ($I_{\mathrm{VK}}/I_{\mathrm{K}}$) computed with 10^4 Monte Carlo simulations with respect to increasing reconfigurability (N_{RE} and N_{RS}) for Case 1. The results are averaged over three different levels of multipath ($N_{\mathrm{path}} = 1, 10, 50$). For a low number of reconfigurable elements ($N_{\mathrm{RE}} = 4, 8$) increasing either N_{RS} or N_{RE} significantly enhances available key bits until the aperture is sufficiently sampled near $N_{\mathrm{RE}} = 16$. Figure 4 also plots fraction of vulnerable key bits $I_{\mathrm{VK}}/I_{\mathrm{K}}$ with increasing complexity, indicating that large complexity ($N_{\mathrm{RE}} \approx 32$) is needed for minimum vulnerability with respect to the eavesdropper.

Figure 5 plots available and ratio of vulnerable key bits for Case 2 where RE states are chosen at random without any consideration of the reflection coefficient. Here it is observed that an increase in the number of REs does not necessarily enhance security, and that higher reconfigurability can mean lower available key bits and increased vulnerability. This effect arises from the non-Gaussian statistics that result for uncontrolled random RE states as well as poor matching for many of those states. Thus, there is a tradeoff between the amount of randomness used in the RE states, and the security level attained.

A. *Effect of Multipath*

RCKG exploiting natural channel fluctuations requires a sufficient number of propagation paths N_{path} to be present for secure operation, and here we consider the role of multipath for RCKG with RECAP-induced synthetic fluctuations. Figure 6 shows the effect on the ratio of vulnerable key bits while increasing N_{path} for varying N_{RE} where $N_{\mathrm{RS}} = 8$. It is observed that for low reconfigurability ($N_{\mathrm{RE}} = 2, 4$), increased multipath is highly beneficial. However, as N_{RE} increases,

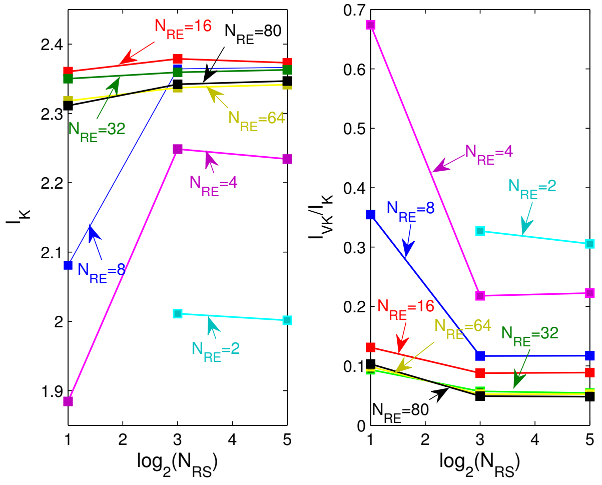

Fig. 4. I_{K} and $\mathrm{I_{VK}/I_K}$ for varying N_{RS} and N_{RE} with $|\Gamma|^2 < 0.1$

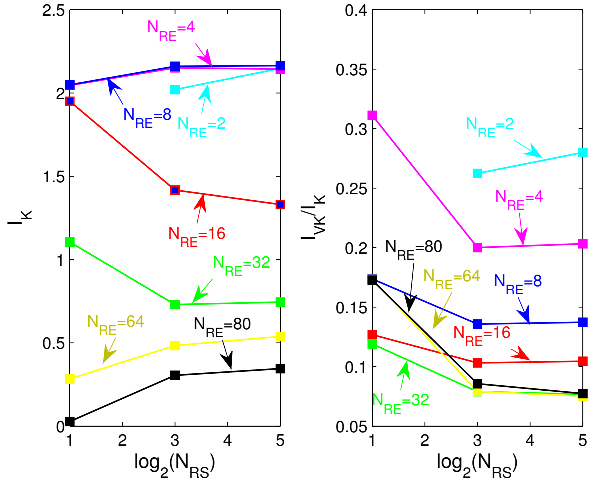

Fig. 5. $\mathrm{I_K}$ and $\mathrm{I_{VK}/I_K}$ for varying $\mathrm{N_{RS}}$ and $\mathrm{N_{RE}}$ with no constraint on $|\Gamma|^2$

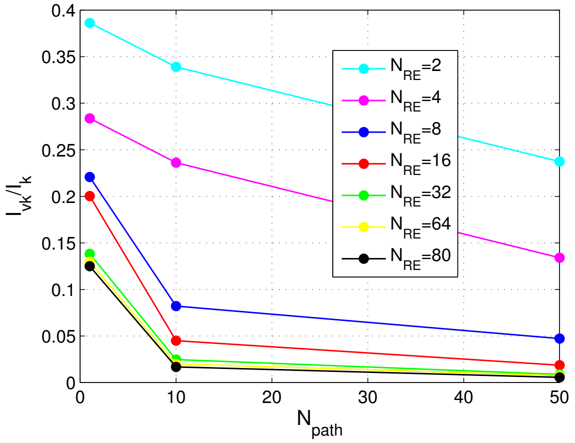

Fig. 6. $I_{\mathrm{VK}}/I_{\mathrm{K}}$ for varying N_{RE} and N_{path} with N_{RS}=8

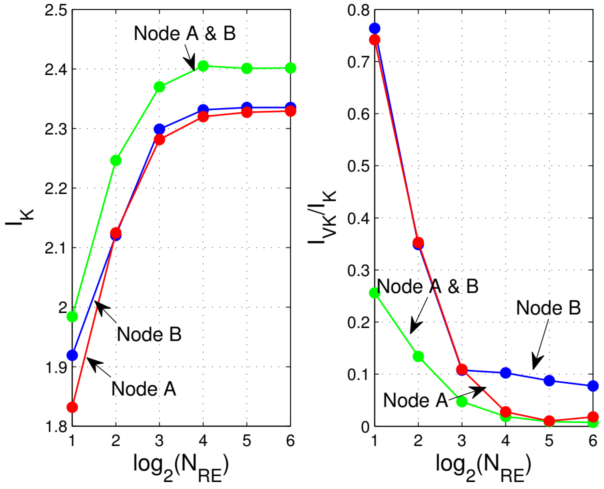

Fig. 7. $\mathrm{I_K}$ and $\mathrm{I_{VK}/I_K}$ for varying $\mathrm{N_{RE}}$ with $\mathrm{N_{RS}}$=8, $\mathrm{N_{path}}$=50 and RECAP at Node A, B or both of them.

the effect of increasing N_{path} becomes less significant and performance saturates at above $N_{\mathrm{path}} = 10$. It suggests that with enough reconfigurability ($N_{\mathrm{RE}} \geq 16$), a high degree of secrecy can be achieved without significant multipath.

B. Effect of having RECAP at Node A or B

In our study so far we have considered that both Node A and B are equipped with RECAP structures as shown in Figure 1. However, it is instructive to compare this case to the case when only one of the nodes (only Node A or Node B) has a RECAP. Figure 7 plots the I_{K} (left) and relative I_{VK} (right) for the three possible cases in the presence of $N_{\mathrm{path}} = 50$ paths while Figure 8 plots it for $N_{\mathrm{path}} = 1$ path.

For rich multipath, we see that having a RECAPs simultaneously at Nodes A and B is the most beneficial, but this only provides a modest improvement over having a RECAP at one side of the link. When only one path is present, however, we see that although having a RECAP at Node A or B does not matter in terms of I_{K}, the choice is critical for I_{VK}. In this case, it is more beneficial for the node near the eavesdropper (Node A) to be equipped with the RECAP. This makes intuitive sense, since if the distant Node B has the RECAP, the same synthetic channel fluctuations will be observed by both Node A and Node C. If instead Node A changes its pattern with a RECAP, Node C has no way of observing this except through possible near-field coupling, which is only weakly connected to the far-field pattern in the direction of Node B.

This result suggests that for robustness, the RECAP should be placed on the node that can be approached by the eavesdropper. In the case that both nodes are openly accessible, RECAPs should likely be placed on both nodes.

C. Channel Distribution

The channel distribution obtained by using RECAPs is another important parameter affecting security. Since channel fluctuations are artificially created, it is not necessarily the case that the random channel will follow a Gaussian distribu-

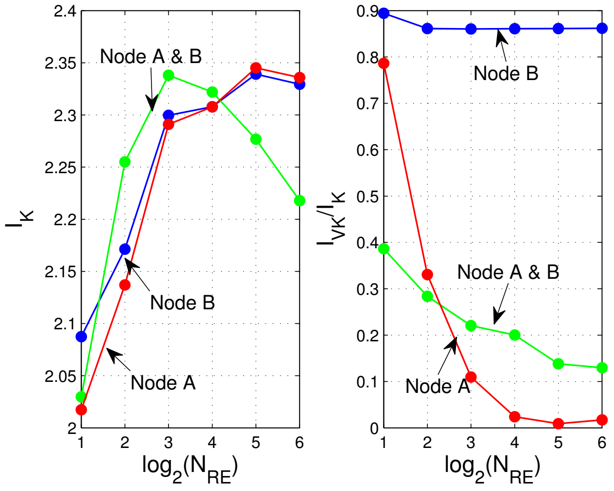

Fig. 8. I_K and I_{VK}/I_K for varying N_{RE} with N_{RS}=8, N_{path}=1 and RECAP at Node A, B or both of them.

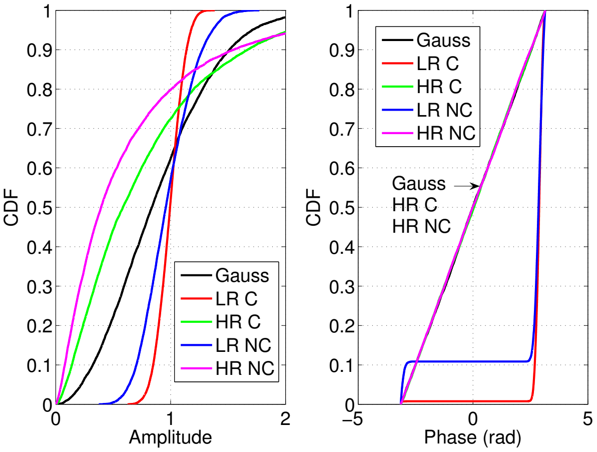

Fig. 9. Amplitude and angle distribution of channel obtained using RECAPs and Gaussian distribution for $N_{path} = 1$.

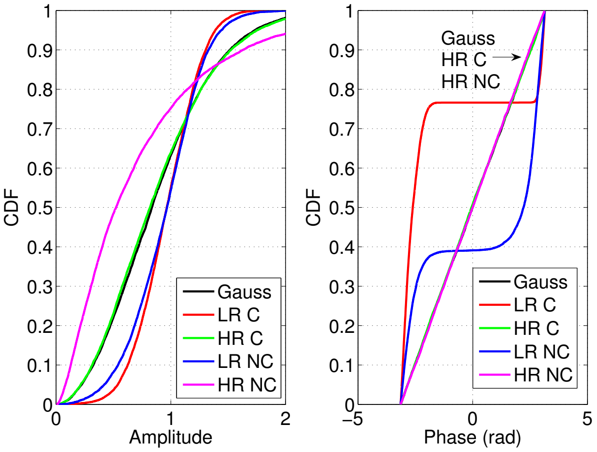

Fig. 10. Amplitude and angle distribution of channel obtained using RECAPs and Gaussian distribution for $N_{path} = 50$.

tion. Here we study the empirical distribution of the channel amplitude and phase, where the physical propagation channel is static with either $N_{\rm path} = 1$ or $N_{\rm path} = 50$, and synthetic fluctuations are generated by a RECAP with $N_{\rm RS} = 32$ and either high $N_{\rm RE} = 64$ or low $N_{\rm RE} = 4$ reconfigurability. We also consider the cases where only RECAP states with low reflection ($|\Gamma|^2 < 0.1$) are used (control) or all states are used (no control).

Figures 9 and 10 consider the cases of $N_{\rm path} = 1$ and $N_{\rm path} = 50$, respectively, where each plots shows shows the magnitude and phase cumulative distribution function (cdf) for five different cases: ideal complex Gaussian (Gauss), low reconfigurability and reflection control (LR C), high reconfigurability and reflection control (HR C), low reconfigurability and no control of reflection (LR NC), and high reconfigurability and no control of reflection (HR NC).

For the case of a single path, we see that having low reconfigurability or no reflection control leads to non-Gaussian statistics. Although still not strictly Gaussian, the best fit occurs for high reconfigurability and control of the reflection (HR C). For rich multipath, deviation of all cases from Gaussian is lower than the single path case, and very close conformance to Gaussian is seen for high reconfigurability with reflection control.

V. Conclusion

This paper has studied the ability of RECAP antennas to generate secret keys by inducing random channel fluctuations, which is possible even in LOS conditions or static channels. Due to the potential for non-Gaussian statistics of RECAP-induced fluctuations, a numerical method for computing the information-theoretic metrics was first developed. It was identified that for limited RECAP complexity, a reduced-complexity brute-force attack is possible, and a lower bound on the required RECAP complexity to avoid this possibility was developed. Subsequent analysis of a specific 9×9 RECAP structure illustrated that peak security requires careful control of the input reflection coefficient of the structure, since otherwise non-Gaussian statistics result. It was also identified that having a RECAP at the node closest to the eavesdropper provides the highest level of security.

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] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, “Information-theoretically secret key generation for fading wireless channels,” *IEEE Trans. Inf. Forensics and Security*, vol. 5, pp. 240–254, June 2010.

[3] 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.

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

[5] J. H. Schaffner, R. Y. Loo, D. F. Sievenpiper, F. A. Dolezal, G. L. Tangonan, J. S. Colburn, J. J. Lynch, J. J. Lee, S. W. Livingston, R. J. Broas, and M. Wu, “Reconfigurable aperture antennas using RF MEMS switches for multi-octave tunability and beam steering,” in *Proc. 2000 IEEE Antennas and Propag. Society Intl. Symp.*, Salt Lake City, UT, July 16-21, 2000, vol. 1, pp. 321–324.