IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 11, 2018, accepted April 11, 2018, date of publication April 17, 2018, date of current version June 19, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2827925

An Upper Bound on PHY-Layer Key Generation for Secure Communications Over a Nakagami-M Fading Channel With Asymmetric Additive Noise

ABDULSAHIB ALBEHADILI[1], (Student Member, IEEE), KHAIR AL SHAMAILEH[2], (Member, IEEE), AHMAD JAVAID[1], (Member, IEEE), JARED OLUOCH[3], (Member, IEEE), AND VIJAY DEVABHAKTUNI[1], (Senior Member, IEEE)

[1]Department of Electrical Engineering and Computer Science, The University of Toledo, Toledo, OH 43606, USA
[2]Department of Electrical and Computer Engineering, Purdue University Northwest, Hammond, IN 46323, USA
[3]Department of Engineering Technology, The University of Toledo, Toledo, OH 43606, USA

Corresponding author: Ahmad Javaid (ahmad.javaid@utoledo.edu)

The work of A. Albehadili was supported by the Higher Committee for Education Development, Iraq.

ABSTRACT The establishment of convenient and reliable cryptographic keys is not always feasible, especially in low-powered wireless devices where a complex key management infrastructure is unaffordable. Physical layer-based key generation approaches, on the other hand, allow two legitimate users to establish a common secret key by exploiting the parameters of the wireless channel, such as the underlying impulse response. In this paper, a fundamental bound on the maximum achievable key generation rate (KGR) over wireless fading channels with asymmetric additive white Gaussian noise (AWGN) is derived. A Nakagami-*m* fading channel is considered, and the effect of non-reciprocity on the forward and reverse channels correlation is demonstrated. We validate the theoretical platform through simulations using a key generation protocol based on the level crossing rate (LCR) of the fading process. The proposed LCR protocol models the Nakagami channel by utilizing the sum-of-sinusoids approach, where Doppler shift, fading severity, and number-of-paths are taken into account. The proposed protocol also incorporates a two-level quantizer to extract keys, where the channel estimates between a wireless transmitter and receiver can be used as the basis. Besides providing an upper bound on the KGR, the analytical and simulation results intertwine the effect of channel reciprocity with the key generation process.

INDEX TERMS Information-theoretic security, key generation rate (KGR), level-crossing rate (LCR), Nakagami-*m* fading, physical layer security (PLS), reciprocity, wireless channel.

I. INTRODUCTION

The ever-growing demand for designing intelligent wireless devices and network protocols to alleviate the impact of eavesdropping has been a recent major challenge [1]–[3]. Numerous encryption techniques were proposed to tackle the problematic attacks launched by adversaries aiming to sniff and/or alter active communications among two or more legitimate users. Such attacks endanger information integrity and increase network vulnerability. The most predominant yet computationally expensive approaches are the one-key (i.e., Data Encryption Standard (DES)) [4] and two-key public key cryptography (PKC) [5]. Nevertheless, such techniques require secret key distribution and protection; needless to mention the significance overhead that results in an added mention the significant overhead that results in an added energy consumption. Quantum cryptography eliminates the dependence on public keys at the expense of cost [6]–[8].

On the other hand, information-theoretic or physical layer security (PLS) uses the physical properties of the wireless channel to establish a higher level of security. Although information-theoretic security is often used interchangeably with PLS, the former addresses security performance under certain strict conditions (e.g., long key lengths as Shannon suggested in [9]). While with PLS, the practical aspect is of a greater significance as the security problem is investigated from the system design viewpoint. PLS techniques try to provide the best effort information secrecy through utilizing the unpredictable and time-varying channel random characteristics along with signal processing techniques. The first work that addressed the practical aspect of information-theoretic secrecy was presented by Wyner [10]. Unlike what Shannon presented in [9], where it was assumed that the legitimate receiver and the eavesdropper observe the same channel conditions, Wyner relaxed such assumption. Wyner suggested that the partial or total stochastic independence of the main channel (from Alice to Bob) and the wiretapper channel (from Alice to Eve) can be exploited to introduce perfect secrecy. In other words, the inherent noise in the main channel is independent of that in the wiretapper channel, which is a more reasonable assumption due to the stochastic nature of many communication channels. Based on the wiretap model, carefully designed error-control codes have been shown to provide a level of information-theoretic secrecy without the need for shared secret keys, by which the amount of information leaked to a wiretapper may be controlled. Accordingly, the use of error-control codes has been the core to develop PLS research [11], [12], and references therein.

Another import direction in PLS research is the generation of secret keys from wireless channel measurements. Two legitimate users, Alice and Bob, generate keys at each end from a set of common channel parameters [13], [14]. Consequently, no key distribution platform is required, presenting an alternative to PKC. Since mobility and the associated fading result in a spatial uncorrelation (i.e., a signal received at adequately distant receivers is affected differently), a key established between a pair of wireless devices using channel measurements is confidential to a third uncorrelated party (i.e., eavesdropper). Thus, the resulting keys are secure and have an advantage over crypto keys whose security strength depends on the intractability of certain mathematical setups. Earliest efforts on PHY-layer secret key generation were reported in [15]–[17]. To facilitate the key establishment, mutual information was considered as a metric to assess the overall performance. In addition, fundamental bounds on the key generation rate (KGR) were studied. The results showed that the KGR is upper bounded by the mutual information between the signal envelopes detected at Alice and Bob.

It is well-known that wireless channels are described as multipath environment with the following properties:

Reciprocity: At a given time instance, channel characteristics (e.g., amplitude, phase difference, and delays) are identical at both directions of the link [18].

Spatial variations: Radiometric properties with respect to a given location are distinctive. In other words, each legitimate party experiences unique characteristics, implying that an eavesdropper at a distance greater than half a wavelength from an authentic user practices uncorrelated measurements.

Temporal variations: Fading is random over time due to the movements of entities and communicating parties themselves. The randomness caused by such an unpredictable movement can be used as a source for secrecy if the legitimate parties have correlated estimates of the channel. It is paramount to point out that fading at two time points is independent if the interval between their channel estimation is larger than the channel coherence time. Furthermore, if the forward and reverse channels are not reciprocal, correlation of estimations at two parties could be affected.

By exploiting such properties, multipath channels were utilized as a source of randomness to generate reliable secret keys with reasonable computational overhead and rapid bits extraction [19]–[36]. In such studies, the statistics of a wireless channel (e.g., propagating signals amplitude and phase) were used to extract secret bits between node pairs. Received signal strength (RSS), for example, is the most widely used parameter due to the feasibility such a radiometric offers even with the traditional off-the-shelf wireless devices. Most of the reported PLS techniques in literature, however, assumed channel reciprocity between legitimate pairs [14, and references therein]. Nevertheless, such assumption does not hold in practice as the channel additive noise is asymmetric, especially in dynamic environments. Moreover, most of the wireless devices operate in a half-duplex mode. Therefore, legitimate users measure the channel at different time instants. Also, hardware noises are independent and cannot be avoided. Hence, received signals at each node are not identically affected [13].

In this paper, a theoretical bound on the KGR in a setup that utilizes fading level crossings to generate secret keys is derived and supported by a simulation platform. Our derivation is based on the level crossing rate (LCR) in Nakagami-m fading environment where reciprocity is not assumed. To facilitate the analysis, we build a protocol to extract secret keys between two nodes communicating over a wireless channel that incurs multipath fading as well as asymmetric additive white Gaussian noise (AWGN). The fading effect is generated according to Nakagami-m fading model developed based on the sum-of-sinusoids approach [37]. The rest of the paper is organized as follows: In Section II, previous efforts are summarized and discussed; whereas in Section III, theoretical derivation of the reciprocity degree under asymmetric AWGN is demonstrated. In Section IV, Nakagami-m and system simulation models, as well as the protocol used to extract secret keys between two end users are illustrated. Finally, conclusions are given in Section VI.

II. RELATED WORK

PLS research has three main directions: 1) Keyless information hiding using error-control codes [12, and references therein], 2) PHY-key generation [13, and references therein], and 3) PHY-authentication [38]–[41]. In this section, related work in the area of PHY-key generation is discussed. A scheme for generating secret bits from correlated observations of deep fades by two users communicating via a time division duplex (TDD) link was proposed in [19]. However, a proper quantification of the KGR versus the parameters adjoined with the fading process or involved within the suggested algorithm was not provided. The concept of deep fades was also applied in [20] and [21], in which a two-level quantizer was utilized to generate a shared key between two communicating nodes. Nonetheless, a low KGR was obtained due to discarding measurements not complying with the binary quantization levels as well as the limited LCR of the adopted Rayleigh fading channel model. Enhanced RSS-based KGR by applying antenna diversity was investigated in [30]. Two nodes, A and B, were assumed to have three transmitting/receiving antennas A_1, A_2, A_3 and B_1, B_2, B_3, respectively. As a result of this arrangement, nine uncorrelated sets of RSS measurements; due to data exchange between antenna sets $(A_1B_1, A_1B_2, ..., A_3B_3)$ enhanced the channel randomness. Moreover, according to the available mutual information (entropy taken as a measure), multi-level quantization was adopted to enhance the KGR four times as compared to a single antenna scenario. In [33], Patwari *et al.* studied the effect of non-simultaneous channel measuring (i.e., reciprocity is no longer maintained), and applied fractional interpolation to recover reciprocity. In the proposed interpolation technique, nodes sample the channel at a rate higher than the Nyquist frequency to estimate what measurements one would get if they were measured simultaneously. Consequently, data-sets obtained by each node were highly correlated due to the virtually high measurements rate, and a discrete Karhunen-Loeve transform (KLT) was applied to remove the resulting correlation. Then, multiple-bit adaptive quantization was incorporated by uniformly dividing the RSS range into quantization bins based on the distribution of the measurements to improve key randomness and rate. Premnath *et al.* [35] proposed adaptive bit quantization at which RSS measurements were divided into smaller blocks each with its own thresholds $\pm q$. RSS above $+q$ or below $-q$ were directly considered in bits extraction, whereas dropped measurements were given indices. The two endpoints exchange their list of dropped RSS estimates and keep those they both decide not to drop. The authors also investigated different real-time measured communication scenarios and showed how each scenario affects the reciprocity and inherent entropy. Secret key extraction in a more challenging wireless link (i.e., vehicular environment) was firstly proposed in [31]. To cope with the increased noise level produced by the continuously moving nodes, weighted sliding window smoothing was adopted. The different weights were optimized considering maximizing the correlation coefficient of the resulting bit sequences (gathered after level-crossing quantization at the two nodes). Correlation maximization was solved by adopting a canonical correlation analysis [42]. Then, a Markov chain was utilized to model the dependency of the quantized bits and used to estimate the entropy [43]. RSS-based collaborative key extraction algorithms for a group of wireless devices were proposed in [27]. Two connectivity topologies; specifically, star and chain, were investigated. The sole of such algorithms was to share the measurements of a specific two-node link between all nodes to extract the same key. However, the KGR significantly decreases with the increase of the network size as all participating nodes should measure RSS data within the coherence time of the channel. In [44]–[46], the effectiveness of using highly reconfigurable antennas was studied to generate varying channel fadings which were used to establish secret keys. In [47], a framework was introduced where fully-autonomous low-power nodes were placed upon the human body for RSS-based secret key generation between two moving legitimate parties in the presence of a stationary eavesdropper. The quality of the key was validated based on indoor and outdoor measurements. Correlation, entropy and mutual information of RSS streams were used to analyze the key generation process. In [48], a system that incorporates the moving average techniques before the quantization process was proposed to improve adaptability to the low variation of RSS, and modify the level crossing algorithm to improve KGR value. However, the resulting key disagreement rate was high. For a recent survey on PHY-key generation works, we refer the reader to [13, and references therein].

As mentioned earlier in Section I, most of the reported PHY-key generation techniques assumed channel reciprocity between legitimate pairs, an assumption that does not hold in practice. Channel non-reciprocity, in general, can be quantified by estimating the asymmetric impairments added to the signal at the legitimate nodes (e.g., using cross-correlation analysis). Once such impairments are quantified, reciprocity calibration can be realized [33], [49]–[52]. However, in this contribution, we introduce a thorough probabilistic reciprocity analysis based on an information-theoretic approach, giving rise to a rigorous mathematical treatment. The proposed approach can be adopted whether the association between two random signals is linear (as in the case of cross-correlation) or non-linear. Moreover, our information-theoretic-driven analysis allows for modeling the channel reciprocity even if the instantaneous channel state information (CSI) at Alice and Bob is unavailable. Our theoretical platform is derived under practical assumptions, and unlike previous works which used mutual information as a bound on the KGR, the proposed analysis adopts the LCR in a Nakagami-m fading environment.

III. RECIPROCITY DEGREE AND KGR DERIVATION

In this section, a mathematical framework for reciprocity degree in a Nakagami-m fading channel model and asymmetric AWGN is derived. Reciprocity degree and LCR are then used to characterize the KGR. For an added convenience, the key symbols and their corresponding notations are summarized in Table 3 (Appendix A).

Based on the nature of the propagation environment, various statistical models are used to characterize the random behavior of the multipath fading channel (e.g., Rayleigh, Rician, Hoyt, and Nakagami-m) [53]. The Nakagami-m fading model is considered as the most comprehensive model [54]. According to this model, the probability density function (PDF) of a received signal envelope is described as:

$$f_Y(y) = \frac{2m^m}{\Gamma(m)\Omega^m} y^{2m-1} e^{-\frac{my^2}{\Omega}}, \quad for\ y \geq 0 \tag{1}$$

where m is the Nakagami parameter that characterizes fading severity, $\Gamma(m)$ is the Gamma function, and $\Omega = E[y^2]$

is the average power. This gamma distribution-based PDF was proposed to describe experimental data as compared to the Rayleigh fading model that fails to accurately predict wireless environments where long distance and high-frequency transmissions exist. It was later shown by independent experimental studies [55], [56] that Nakagami-m model provides better characterization for less and more severe fading conditions than Rayleigh and Rician models and provides a better fit to the mobile communication data channel in diverse multipath propagation [57], [58]. As a result, it finds applications in many software and hardware fading channel simulators [59], [60]. It is also of interest to remark that Nakagami-m fading model is featured with universality in classifying wireless channels based on fading severity (represented by m) [37], [54], [61]. That is, it explicitly includes other distributions as special cases. For example, a one-sided Gaussian distribution (the most severe fading scenario) corresponds to $m = 1/2$, whereas $m = 1$ represents a Rayleigh distribution, and a one-to-one mapping between the Rician factor k and m is obtained for $m > 1$, which allows a close approximate of the Rician distribution. Such facts have motivated us to use Nakagami-m model as the basis for our mathematical and simulation analysis.

The received signal in a multipath environment at the channel output can be represented as:

$$y = hu + n = x + n \tag{2}$$

where $u\{+1, -1\}$ is the input signal, n is AWGN with zero mean and variance σ^2, and h expresses the fading gain of the channel. Reciprocity can be derived by calculating the conditional probability density function: $f(y|u) = \int\big[p(u)f(x|u)f(y|x,u)/p(u)\big]dx = \int f(x|u)f(y|x,u)dx$ where $f(y|x,u) = f(y|x)$ due to the fact that u, x, and y form a Markov chain, while $p(u)$ denotes the probability of the occurrence of u. Since $uh = x$:

$$f_X(x|u) = \frac{2m^m x^{2m-1}}{\Gamma(m)} ue^{-mx^2} U(ux) \tag{3a}$$

where $U(.)$ is the unit step function. Furthermore, we have:

$$f_Y(y|x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(y-x)^2}{2\sigma^2}} \tag{3b}$$

Hence:

$$\begin{aligned} f_Y(y|u=1) &= \int_0^\infty \frac{2m^m x^{2m-1}}{\Gamma(m)} e^{-mx^2} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(y-x)^2}{2\sigma^2}} dx \\ &= \frac{2m^m e^{\frac{-y^2}{2\sigma^2}}}{\sqrt{2\pi}\sigma\Gamma(m)} \int_0^\infty x^{2m-1} e^{-\alpha x^2 + \frac{y}{\sigma^2}x} dx \end{aligned} \tag{3c}$$

where $\alpha = (m + 1/2\sigma^2)$, by applying the integral solution provided in [62, eq.(3.462.1)], $f_Y(y|u=1)$ is found as:

$$\begin{aligned} f_Y(y|u=1) = \sqrt{\frac{2}{\pi}} (\frac{m}{2\alpha})^m \frac{\Gamma(2m) e^{\frac{-y^2}{2\sigma^2}}}{\sigma\Gamma(m)} \\ \times \left[e^{\frac{(y/\sigma^2)^2}{8\alpha}} D_{-2m}(\frac{-y/\sigma^2}{\sqrt{2\alpha}}) \right] \end{aligned} \tag{4a}$$

Here, $D_{-v}(z)$ is the parabolic cylinder function of order v and argument z defined in [62, eq. (9.240)]. Similarly:

$$\begin{aligned} f_Y(y|u=-1) = \sqrt{\frac{2}{\pi}} (\frac{m}{2\alpha})^m \frac{\Gamma(2m) e^{\frac{-y^2}{2\sigma^2}}}{\sigma\Gamma(m)} \\ \times \left[e^{\frac{(y/\sigma^2)^2}{8\alpha}} D_{-2m}(\frac{y/\sigma^2}{\sqrt{2\alpha}}) \right] \end{aligned} \tag{4b}$$

From (4a) and (4b), $f_Y(y|u)$ in a Nakagami-m fading channel can be expressed as:

$$f_Y(y|u) = \sqrt{\frac{2}{\pi}} (\frac{m}{2\alpha})^m \frac{\Gamma(2m) e^{\frac{-y^2}{2\sigma^2}}}{\sigma\Gamma(m)} \left[e^{\frac{(y/\sigma^2)^2}{8\alpha}} D_{-2m}(\frac{-uy/\sigma^2}{\sqrt{2\alpha}}) \right] \tag{5}$$

For the case of a Rayleigh fading channel ($m = 1$):

$$f_Y(y|u) = \frac{2\sigma e^{\frac{-y^2}{2\sigma^2}}}{\sqrt{2\pi}(1+2\sigma^2)} \left[e^{\frac{(y/\sigma^2)^2}{8(1+1/2\alpha^2)}} D_{-2}(\frac{-uy/\sigma^2}{\sqrt{2(1+1/2\alpha^2)}}) \right]$$

From [62, eq. (9.254.2)], $D_{-2}(z)$ is given by:

$$D_{-2}(z) = e^{-z^2/4} - \sqrt{2\pi} z e^{z^2/4} Q(z) \tag{6}$$

where $Q(.)$ is the tail of the Gaussian distribution. Then:

$$\begin{aligned} f_Y(y|u) = &\frac{2\sigma e^{\frac{-y^2}{2\sigma^2}}}{\sqrt{2\pi}(1+2\sigma^2)} [e^{\frac{(\frac{y}{\sigma^2})^2}{8(1+\frac{1}{2\sigma^2})}}] \Bigg[e^{\frac{-\frac{u^2y^2}{\sigma^4}}{8(1+\frac{1}{2\sigma^2})}} \\ &+ \frac{\sqrt{2\pi}uy/\sigma}{\sqrt{1+2\sigma^2}} e^{\frac{\frac{u^2y^2}{\sigma^4}}{8(1+\frac{1}{2\sigma^2})}} Q(\frac{-uy/\sigma}{\sqrt{1+2\sigma^2}}) \Bigg] \\ = &\frac{2\sigma e^{\frac{-y^2}{2\sigma^2}}}{\sqrt{2\pi}(1+2\sigma^2)} \Bigg[e^{\frac{y^2/\sigma^2}{4(1+2\sigma^2)}(1-u^2)} \\ &+ \frac{\sqrt{2\pi}uy/\sigma}{\sqrt{1+2\sigma^2}} e^{\frac{\frac{y^2}{\sigma^2}}{4(1+2\sigma^2)}(1+u^2)} Q(\frac{-y/\sigma}{\sqrt{1+2\sigma^2}}) \Bigg] \end{aligned} \tag{7}$$

It can be seen that $f_Y(y|u)$ obtained in (7) complies with the results in [63], where a Rayleigh fading model was used. To maintain reciprocity over a Nakagami-m fading channel, $f_Y(y_{AB}|u_{BA})$ must equal $f_Y(y_{BA}|u_{AB})$. That is:

$$\begin{aligned} &\frac{(2\alpha_{BA})^{-m}}{\sigma_{BA}} e^{-\frac{y_{AB}^2}{2\sigma_{BA}^2}} \left[e^{\frac{(\frac{y_{AB}}{\sigma_{BA}^2})^2}{8\alpha_{BA}}} D_{-2m}(\frac{-\frac{u_{BA}y_{AB}}{\sigma_{BA}^2}}{\sqrt{2\alpha_{BA}}}) \right] \\ &= \frac{(2\alpha_{AB})^{-m}}{\sigma_{AB}} e^{-\frac{y_{BA}^2}{2\sigma_{AB}^2}} \left[e^{\frac{(\frac{y_{BA}}{\sigma_{AB}^2})^2}{8\alpha_{AB}}} D_{-2m}(\frac{-\frac{u_{AB}y_{BA}}{\sigma_{AB}^2}}{\sqrt{2\alpha_{AB}}}) \right] \end{aligned} \tag{8}$$

which leads to the following reciprocity conditions (refer to Appendix B for proof):

$$\frac{(\beta_{AB}/\sigma_{AB}^2)^{-m}}{\sigma_{AB}} = \frac{(\beta_{BA}/\sigma_{BA}^2)^{-m}}{\sigma_{BA}} \tag{9a}$$

$$\frac{1 - 2\beta_{AB} + (8m-1)u_{AB}^2}{4\sigma_{AB}^2\beta_{AB}} = \frac{1 - 2\beta_{BA} + (8m-1)u_{BA}^2}{4\sigma_{BA}^2\beta_{BA}} \tag{9b}$$

where $\beta_{ij} = 2m\sigma_{ij}^2 + 1$. Thus, it can be concluded from (9a) and (9b) that channel reciprocity is a function of the Gaussian noise variance σ^2 and the fading strength m. This is to say; perfect reciprocity is not maintained if the noise variances of the forward channel σ_{AB}^2 and reverse channel σ_{BA}^2 are not identical (assuming the same fading severity in both directions). Hence, we characterize such a remark in the reciprocity degree R as follows:

$$R(\%) = 100\,(1 - r) \tag{10a}$$

where $r \in (0, 1)$ is a function of (9a, 9b) and is given by:

$$\begin{aligned} r = &\left| \frac{(\beta_{AB}/\sigma_{AB}^2)^{-m}}{\sigma_{AB}} - \frac{(\beta_{BA}/\sigma_{BA}^2)^{-m}}{\sigma_{BA}} \right| \\ &+ \left| \frac{1 - 2\beta_{AB} + (8m-1)u_{AB}^2}{4\sigma_{AB}^2\beta_{AB}} \right. \\ &\left. - \frac{1 - 2\beta_{BA} + (8m-1)u_{BA}^2}{4\sigma_{BA}^2\beta_{BA}} \right| \end{aligned} \tag{10b}$$

Reciprocity degree R is analytically depicted in Fig. 1, as a function of the Nakagami fading parameter m for various asymmetric additive noise conditions. As can be noticed, reciprocity degrades as the difference between σ_{AB} and σ_{BA} becomes larger; whereas higher values of m (i.e., less fading severity) has a positive impact on reciprocity.

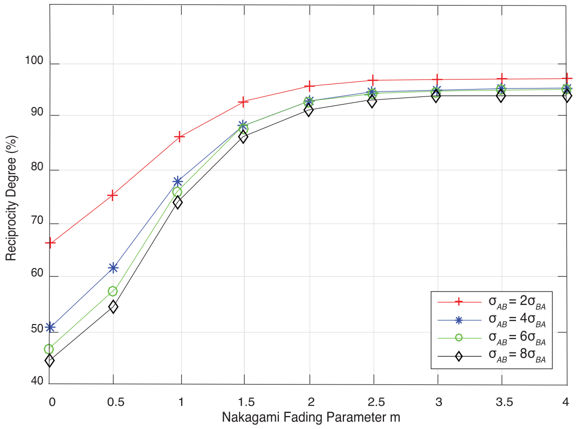


FIGURE 1. Reciprocity degree *R* as a function of the fading parameter *m* for asymmetric forward/reverse noise variance.

The Nakagami parameter m can also be written as a function of the separation distance d between Alice and Bob [64, Table 3]:

$$m = -0.69ln(d) + 4.3 \tag{11}$$

Hence, for a given scenario, the effect of the separation distance d on channel reciprocity can be obtained. As shown in Fig. 2, as d increases, reciprocity decreases mainly due to the increase of the fading gain.

As mentioned earlier, since fading at Bob's and Alice's locations decorrelates at Eve's who is at a distance in the order of half a wavelength, Bob and Alice can rely on the commonalities introduced by level crossings as a source of secrecy.

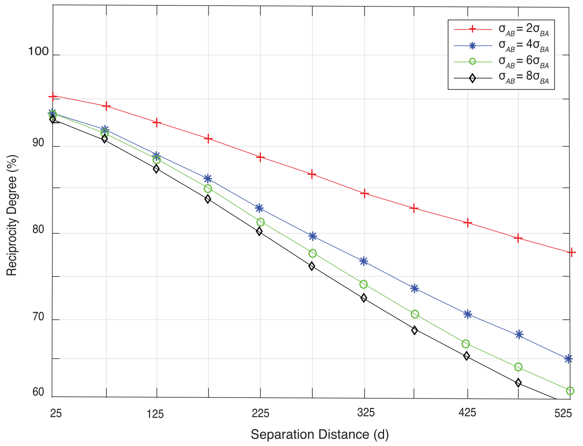


FIGURE 2. Reciprocity degree as a function of *d* separating A and B based on experimental data provided in [64, Table 3].

Therefore, a bound on the KGR based on the randomness of the fading level is derived using the LCR. The LCR for a Nakagami-m fading process is given as [65]:

$$LCR = \sqrt{2\pi} f_m \frac{m^{m-1/2}}{\Gamma(m)} \rho^{2m-1} e^{-m\rho^2} \tag{12a}$$

where ρ is the threshold level normalized to the root mean square signal level and f_m represents the maximum Doppler shift, which equals to [66]:

$$f_m = \frac{\sqrt{v_t^2 + v_r^2}}{\lambda\sqrt{2}} = \frac{v_{eff}}{\lambda\sqrt{2}} \tag{12b}$$

v_t and v_r are the transmitter and receiver velocities magnitudes, respectively, and λ is the wavelength. Given that Alice's and Bob's observations of identical level crossing excursions are affected by how much the channel is reciprocal, an upper bound on KGR can then be calculated as:

$$KGR \le \sqrt{2\pi} f_m (1 - r) \frac{m^{m-1/2}}{\Gamma(m)} \rho^{2m-1} e^{-m\rho^2} \tag{12c}$$

If the channel is reciprocal (i.e., $r = 0$) and $\rho = 1$, it can be inferred that the maximum key size will not exceed the maximum Doppler shift f_m. In other words, it is not possible to obtain key bits per second larger than f_m even with optimally designed key generation protocol.

IV. SIMULATION MODEL

To evaluate the effect of non-reciprocity on the KGR, simulations are performed based on the system model shown in Fig. 3. Two communication parties, Alice and Bob, try

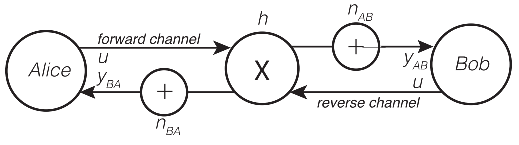


FIGURE 3. Wireless channel model.

to generate secret keys over a wireless channel that incurs multipath fading as well as asymmetric AWGN. Here, h is a stochastic process that represents a time-varying channel parameter. Asymmetric AWGN in the forward and reverse channels is represented by $n_{AB}(t)$, $n_{BA}(t)$, respectively.

Alice and Bob generate keys by estimating the channel coefficient h through exchanging known probes u within a time frame smaller than the channel coherence time T_c. To simulate the channel coefficient h, various approaches are used in the literature. The most commonly used one is the filtering white Gaussian variables method [20], [21], [63], [67]–[72]. However, this method does not take into account the variation of the number of paths or Doppler shift, which are important parameters to characterize various fading conditions. In this paper, instead, we use the sum-of-sinusoids method for its flexibility and parametric inclusivity in characterizing various fading conditions [73]–[76]. The adopted method allows the approximation of multipath fading through the superposition of a finite number of weighted harmonic components. Each component represents one path and is described by amplitude, frequency, and phase values related to the Doppler frequency f_m.

A. SUM-OF-SINUSOIDS NAKAGAMI-M MODEL

While a fair amount of attention has been given to the Nakagami-m distribution, relatively less work has addressed the issue of Nakagami-m channel model simulation. This can be attributed to the fact that such a model was not specified when Nakagami-m distribution was first proposed [77]. Directly generating a Nakagami-m envelope is difficult and, therefore, mostly indirect approaches are used. According to [37], a Nakagami envelope can be generated from Rayleigh and Rician envelopes as follows:

$$R_{Nak} = R_{Ray}\, e^{1-m} + R_{Ric}\,(1 - e^{1-m}) \tag{13}$$

To this end, Rayleigh and Rician models are implemented individually and then combined together to introduce a Nakagami-m multipath model. The random process of Rayleigh fading with N paths can be simulated with the sum-of-sinusoid method described as [76] and [77]:

$$G(t) = Y_c(t) + jY_s(t) \tag{14a}$$

$$Y_c(t) = \frac{1}{\sqrt{N}} \sum_{n=1}^{N} cos[w_m\, t\, cos(\frac{2\pi n + \theta_n}{N}) + \phi_n] \tag{14b}$$

$$Y_s(t) = \frac{1}{\sqrt{N}} \sum_{n=1}^{N} sin[w_m\, t\, cos(\frac{2\pi n + \theta_n}{N}) + \phi_n] \tag{14c}$$

where N is the total number of the paths. θ_n (angle of arrival) and ϕ_n (phase delay) are statistically independent and uniformly distributed random variables over $[-\pi, \pi]$.The maximum angular Doppler shift is denoted by w_m. The presentation of [76] and [77] can also be extended to establish a Rician fading model. Given that a dominant line-of-sight (LOS) component exists, the normalized Rician fading process of an improved sum-of-sinusoids statistical simulation model is described as:

$$Z(t) = Z_c(t) + jZ_s(t) \tag{15a}$$

$$Z_c(t) = [Y_c(t) + \sqrt{N} cos(w_m t cos\theta_0 + \phi_0)]/\sqrt{1+k} \tag{15b}$$

$$Z_s(t) = [Y_s(t) + \sqrt{N} sin(w_m t cos\theta_0 + \phi_0)]/\sqrt{1+k} \tag{15c}$$

where $Y_c(t)$ and $Y_s(t)$ are the non-line-of-sight (NLOS) rays that can be obtained from (14b,c). θ_0= $\pi/4$ is the angle of arrival of the LOS component [75], [76]. The Rician factor k represents the ratio of the specular to scattered power, and has the one-to-one mapping with m as [61]:

$$k = \frac{\sqrt{m^2 - m}}{m - \sqrt{m^2 - m}} \tag{16}$$

A validation of the fading model is carried out through Monte-Carlo simulation by sending a binary phase-shift-keying (BPSK) signal over the multipath fading channel. Simulation parameters are set in Table 1.

TABLE 1. Simulation parameters.

Parameter	Quantity
$Samples\ generated$	10^5
$Sampling\ period$	$0.0001sec$
N	100
f_m	$100Hz$
θ_n, ϕ_n	$U(-\pi, \pi)$
ϕ_0	$\pi/4$
m	$1, 4$

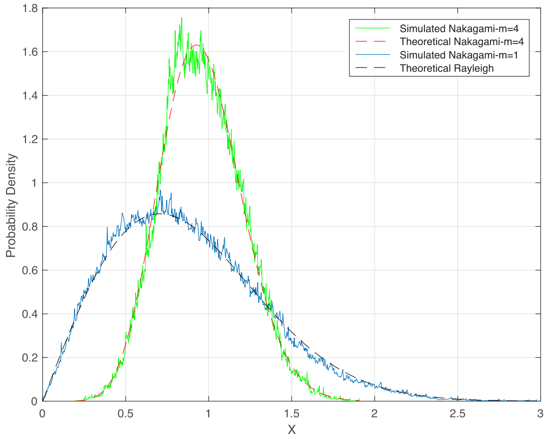


FIGURE 4. Simulated versus analytical PDFs of Nakagami-m fading envelopes with $m = 1$ (Rayleigh) and $m = 4$.

Fig. 4 shows the simulated PDF of the signal envelope considering two fading parameter m values; specifically, $m = 4$, $m = 1$ (Rayleigh), compared to the theoretical distributions. The close agreement between both simulated and analytical PDFs justifies the use of the sum-of-sinusoids method in the channel implementation.

B. LCR QUANTIZER

Fig. 5 shows the fundamental process for extracting PHY-based secret keys from level crossings [20]. Such a process incorporates three main stages: probing, quantization, and converting excursions to bits. In this paper, each stage is elaborated in greater details.

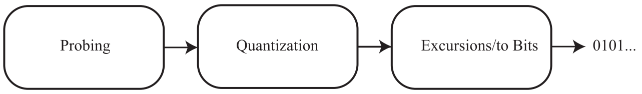


FIGURE 5. **LCR-based key extraction stages.**

Probing: In the system model given in Fig. 3, two communicating parties, Alice and Bob, exchange probing signals u (known to each other) within a certain time frame to gather RSS values affected, naturally, by small-scale fading and AWGN. Theoretically, and based on the reciprocity concept, RSS values measured at Bob (by sensing Alice's transmitted probes) match the ones measured at Alice (by sensing Bob's transmitted probes). This, however, is not the case in practice due to 1) asymmetric additive noise, 2) transmitter/receiver hardware differences, and 3) non-simultaneous measuring attempts because of the half-duplex nature in most wireless networks. The context of this work is devoted for addressing the first effect on reciprocity; i.e., asymmetric additive noise. In our system model, Alice and Bob exchange their probes across a multipath environment characterized by Nakagami-m fading model. Therefore, received signals at both parties:

$$y_{AB} = u(t)h(t) + n_{AB}(t) \tag{17a}$$
$$y_{BA} = u(t)h(t) + n_{BA}(t) \tag{17b}$$

where Alice receives y_{BA} and Bob receives y_{AB}. During each probe exchange, each party can use the received signal y along with the probe signal u to compute one channel estimate $\hat{h}$. Since Alice and Bob know the original probe signal u, they both can estimate a version of the channel coefficient $h(t)$ scaled by additive noise $Z(t)$ [78]:

$$\hat{h}_{AB} = h(t) + Z_{AB}(t) \tag{18a}$$
$$\hat{h}_{BA} = h(t) + Z_{BA}(t) \tag{18b}$$

where Alice estimates $\hat{h}_{BA}$ and Bob estimates $\hat{h}_{AB}$; whereas $Z_{BA}(t)$ and $Z_{AB}(t)$ are asymmetric additive noise processes at Alice and Bob, respectively. By repeatedly exchanging probes over the channel, Alice and Bob can generate a sequence of channel estimates E. That is, Bob generates $\hat{H}_{AB} = [\hat{h}_{AB}(1), \hat{h}_{AB}(2), ..., \hat{h}_{AB}(E)]$, while Alice generates $\hat{H}_{BA} = [\hat{h}_{BA}(1), \hat{h}_{BA}(2), ..., \hat{h}_{BA}(E)]$. Since asymmetric variations could be added at Alice's and Bob's sides, reciprocity cannot be maintained and, therefore, the correlation between $\hat{H}_{BA}$ and $\hat{H}_{AB}$ could be affected. In [20], [21], and [48], in order to mitigate the non-simultaneous measurements limitation of half-duplex transceivers and achieve high correlation between $\hat{H}_{BA}$ and $\hat{H}_{AB}$, it was assumed that Alice and Bob exchange their probes at a faster rate. However, a decorrelation between $\hat{H}_{BA}$ and $\hat{H}_{AB}$ could result from the asymmetric additive noise, as will be discussed later.

Quantization: After Alice and Bob collect their estimations of the channel coefficients, they use a two-level quantizer to detect excursions that exceed a threshold, $\pm q$. We define an excursion as a channel estimate in $\hat{H}_{BA}$ or $\hat{H}_{AB}$ that exceeds the threshold $\pm q$. This quantization approach was originally proposed in [20] and was also adopted in [21] and [48]. The quantizer threshold depends on the channel statistics (i.e, mean μ_H and standard deviation σ_H of the channel estimates) as follows:

$$\pm q_A = \mu_{\hat{h}_{BA}(i)} \pm \xi\, \sigma_{\hat{h}_{BA}(i)} \tag{19a}$$
$$\pm q_B = \mu_{\hat{h}_{AB}(i)} \pm \xi\, \sigma_{\hat{h}_{AB}(i)} \tag{19b}$$

where $\pm q_A$ and $\pm q_B$ are the quantizer threshold levels at Alice and Bob, respectively, $i = 1, 2, ..., E$, and ξ is a tuning parameter that takes any value between $\{0.1 - 0.8\}$. A high ξ gives a strict quantizer that results in a smaller key size, but at the same time, reduces the chance of Eve having similar excursions, and vice versa.

Once Alice and Bob determine such a threshold, Alice searches $\hat{H}_{BA}$ to obtain the locations of existing excursions, and put them in a vector L_A. To increase the probability of having identical sequences of bits, later, generated at the two parties, Alice considers the location of an excursion only if that excursion occurs S_m successive times. S_m is a tuning parameter that takes integer values between $\{2 - 5\}$, and has two main benefits: 1) it functions analogous to repetition codes (i.e., sending a message repeatedly to reduce the error probability through majority decoding [79]), and 2) it guarantees that only one key bit is generated from a subset of successive channel estimates that exceed $\pm q$. Accordingly, Alice searches $\hat{H}_{BA}$ to find subsets with exactly S_m successive similar excursions, where an entire subset is used to generate only one key bit. While the LCR quantizer reported in [20] enables Alice to adopt subsets that have S_m or more successive excursions, ours enforces Alice to search $\hat{H}_{BA}$ and find subsets that have exactly S_m successive excursions. Our use of a more realistic fading model justifies this modification. Furthermore, in [20], it was assumed that the fading process $h(t)$ is a Gaussian random variable, which does not accurately model the correlation between successive estimates in realistic scenarios. However, in a more realistic fading model where temporal variation between these estimates exists, decorrelation between different subsets of channel estimates exist and is dictated by the channel coherence time T_c. For example, a channel with $f_m = 100\ Hz$ has a coherence time T_c of 4.23×10^{-3} seconds. Therefore, within one T_c period and a probing rate of $1 Kprobe/s$, Alice and Bob have enough window to exchange two probes each, as shown in Fig. 6. As such, every two successive channel estimates have a high correlation in this window. Therefore, setting $S_m = 2$ is more practical than $S_m \geq 2$.

Excursions-to-Bits Extraction: Alice sends Bob a vector L_A, which has the excursions locations, over the

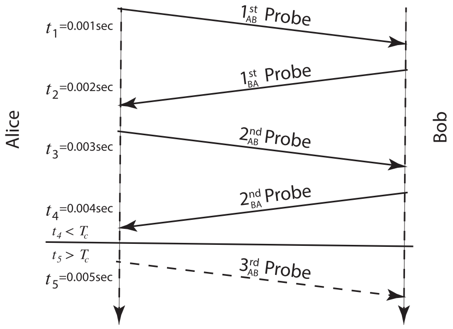


FIGURE 6. Probes exchange between Alice and Bob in a channel with coherence time of 4.23 *ms* and probing rate of 1*Kprobe*/*s*.

public channel. In the same way, Bob determines the locations of the excursions, at his side, from $\hat{H}_{AB}$ and compares his excursions locations against Alice's L_A. Bob indicates the matching indices in a new updated vector L_B and sends it back to Alice. Eve's observations of $L_{A,B}$ will not provide any useful information about $\hat{H}_{BA,AB}$, as $L_{A,B}$ only have the excursions locations. A pseudocode for the LCR quantizer is given as follows:

```
Algorithm 1 Alice LCR Quantizer
  $count = 1$
  while $count \leq length(\hat{H}_{BA}) - S_m + 1$ do
    if $\varphi[\hat{H}_{BA}(count : count + S_m - 1)] \geq +q_A$ or $\leq -q_A$ then
      $L_A = [L_A \quad save_{index}]$
      $count = count + S_m$
    else
      $L_A = [L_A \quad return_{null}]$
      $count = count + 1$
    end if
  end while
  Send $L_A$ to Bob
```

```
Algorithm 2 Bob LCR Quantizer
  $count = 1$
  while $count \leq length(\hat{H}_{AB}) - S_m + 1$ do
    if $\varphi[\hat{H}_{AB}(count : count + S_m - 1)] \geq +q_B$ or $\leq -q_B$ then
      $L_B = [L_B \quad save_{index}]$
      $count = count + S_m$
    else
      $L_B = [L_B \quad return_{null}]$
      $count = count + 1$
    end if
  end while
  Compare $L_B$ with $L_A$, Send $L_B$ to Alice
```

Finally, given the vector L_B at both sides, and based on the threshold ±q, a binary 1 is generated if the value of an excursion is greater than $+q$; whereas a binary 0 is generated if the value of an excursion is less than $-q$. In other words:

$$\varphi[h(i)] = \begin{cases} 0 & \text{for } h(i) \leq -q \\ 1 & \text{for } h(i) \geq +q \end{cases}, i=1, 2..., length(L_B) \quad (20)$$

C. SIMULATION RESULTS

Simulations are performed based on the system model shown in Fig. 3, where the effect of asymmetric AWGN (i.e., non-reciprocity) on the KGR is demonstrated. The design parameters are subdivided into two main categories: 1) channel parameters; specifically, the fading parameter m, maximum Doppler frequency f_m, number of paths N, and the variance (i.e., power) of the additive noise σ^2, 2) LCR quantizer parameters; specifically, the tuning parameter ξ (that controls ±q), and S_m. Simulations are performed in five different scenarios, and the KGR is measured over a period of 50 *sec*. Simulation parameters for all scenarios are summarized in Table 2. It is worth mentioning that the number of paths N and the rate at which Alice and Bob probe each other are fixed at 100 and 1*Kprobe*/*sec*, respectively.

TABLE 2. Simulation parameters.

	Channel			LCR Quantizer	
	m	$f_m(Hz)$	$SNR(dB)$	ξ	S_m
Fig.7	4	200	10	0.5, 0.6, 0.7, 0.8	2
Fig.8	1,2,3,4,5	100	10	0.8	2
Fig.9	4	100	10	0.8	2, 3, 4, 5
Fig.10	4	100, 150, 200	10	0.8	2
Fig.11	4	100	0, 3, 5, 10	0.8	2

As mentioned earlier, reciprocity degrades when there is a difference between σ^2_{AB} and σ^2_{BA} and/or a high fading gain. To validate the former effect on the KGR, the variance of the AWGN in the forward channel (i.e., σ^2_{AB}) is set to 1; whereas the variance of the reverse channel (i.e., σ^2_{BA}) is changed by varying σ_{BA} in the range $\{1-5\}$. f_m, m, and the signal-to-noise ratio (SNR) are set to 200 *Hz*, 4, and 10 *dB*, respectively. Such values are chosen under the assumption that two vehicular nodes are communicating at 2.4 *GHz* carrier frequency. The LCR quantizer parameters are set to $\xi = 0.5, 0.6, 0.7, 0.8$ and $S_m = 2$.

Fig. 7 shows that a larger difference between σ^2_{AB} and σ^2_{BA} induces a noticeable decrease in the KGR due to the decrease in reciprocity degree. Specifically, each unit increase in σ_{BA} reduces the KGR by 14%. Furthermore, it can be seen that smaller key sizes are obtained for higher ξ values as fewer excursions are considered due to the larger ±q magnitudes.

KGR analysis under different fading gains is illustrated by varying m in the range $\{1 - 5\}$, while fixing f_m to 100 *Hz* and *SNR* to 10 *dB*. The LCR quantizer parameters are set to $\xi = 0.8$ and $S_m = 2$. Fig. 8 shows that higher values of m (i.e., less fading severity) result in a higher KGR. This can be attributed to the fact that higher m values result in a better channel reciprocity degree R.

It is paramount to point out that a simple two-level quantizer design could result in a high mismatch rate (i.e., Alice

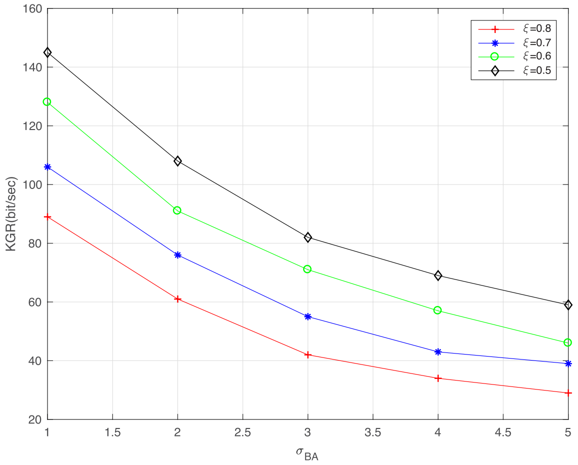


FIGURE 7. ***KGR* vs σ_{BA} for $\xi = 0.5, 0.6, 0.7,$ and 0.8.**

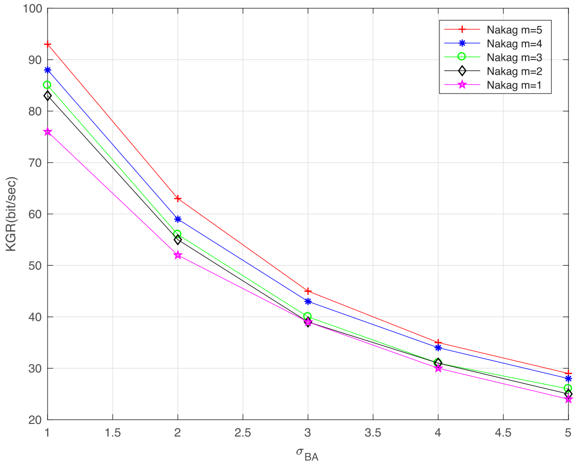


FIGURE 8. ***KGR* vs σ_{BA} for *m*=1, 2, 3, 4 and 5.**

and Bob may agree on index values with excursions lying in opposite directions). Such a mismatch is overcome by using key distillation and privacy amplification techniques [80], [81] which are beyond the scope of this paper. Nonetheless, as discussed in Section IV.B, the mismatch rate can be reduced by considering S_m successive (rather than single) excursions. However, S_m can be increased to a certain limit as having similar excursions will also become less frequent due to the temporal variation between successive estimations. With a probing rate of $1Kprobe/s$ and a channel coherence time T_c of $4.23ms$, Alice and Bob have enough window to exchange two probes each. In this case, higher S_m values (i.e., $S_m > 2$), as shown in Fig. 9, result in a lower KGR.

Fig. 10 shows the effect of the Doppler frequency f_m on the KGR. Higher f_m values (i.e., increased nodes' velocity) increases the KGR as the likelihood of having more excursions increases. However, as predicted by (12c), the KGR is capped by f_m (simulation parameters are set to $m = 4$, $SNR = 10\ dB$, $\xi = 0.8$, and $S_m = 2$). Finally, Fig. 11 shows a proportional relation between the SNR and the KGR, as higher SNR values impose low noise power (i.e. higher reciprocity).

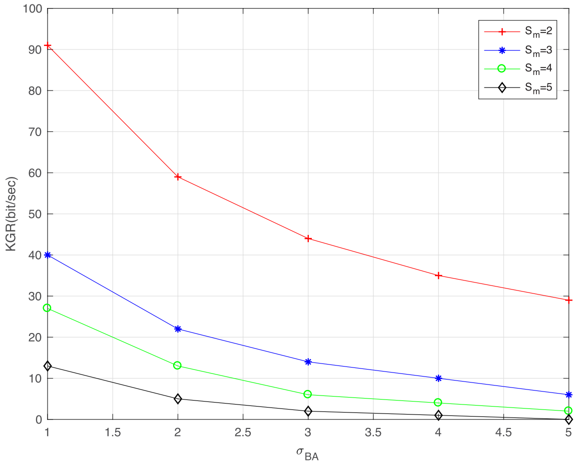


FIGURE 9. ***KGR* vs σ_{BA} for $S_m = 2, 3, 4,$ and 5.**

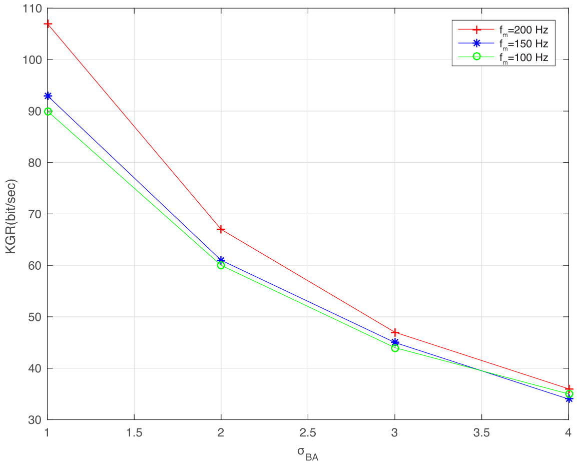


FIGURE 10. ***KGR* vs σ_{BA} for $f_m = 100, 150,$ and 200 *Hz*.**

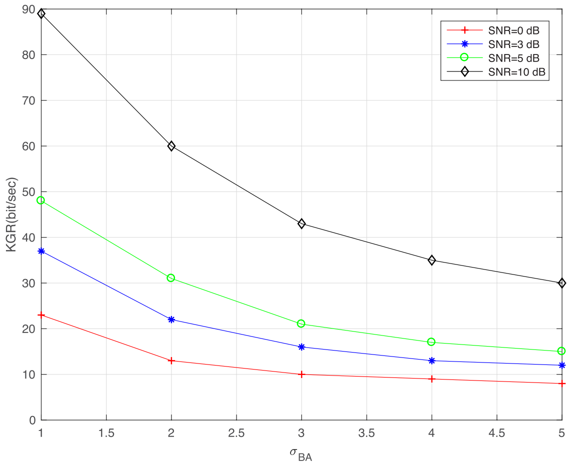


FIGURE 11. ***KGR* vs σ_{BA} for *SNR* = 0, 3, 5, and 10*dB*.**

V. CONCLUSION

We derived and validated a PLS scheme to assess the maximum achievable KGR under practical assumptions.

A theoretical bound on the KGR in a setup that utilizes level crossings to generate secret keys is derived and validated by simulations. Our derivation can characterize the effect of non-perfect reciprocity due to asymmetric AWGN on the KGR. Unlike many previous works that used the mutual information as a bound, the LCR in a fading environment characterized by Nakagami-m fading model is adopted, where reciprocity is not assumed. Since Nakagami-m fading model demonstrates better approximations to realistic wireless channels as well as the universality it offers in characterizing these channels, based on fading severity, the proposed analytical and simulation frameworks enable a practical PLS scheme. To facilitate the analysis of non-perfect reciprocity of the channel on the KGR, secret keys between two nodes communicating over a wireless channel that incurs multipath and asymmetric AWGN are extracted. The Nakagami-m fading process is generated using the sum-of-sinusoids approach to provide a flexibility in characterizing various fading conditions, through varying the number of paths as well as the maximum Doppler frequency. Analytical and simulation results show that differences in noise power between the forward/reverse channels decreases the KGR as channel reciprocity is not maintained. While, higher m values (i.e., less fading severity) result in a higher KGR as channel reciprocity is improved.

APPENDIX A

TABLE 3. Symbols & notations ■■ Sec. III ■□ Sec. III, IV □□ Sec. IV.

	Symbol	Notation
■■	u	Input signal to the channel (e.g. probe signal)
■■	x	Faded signal
■■	n	Additive white Gaussian noise (AWGN)
■■	σ^2	Noise variance
■■	h	Channel impulse response
■■	y	Received signal
■■	$f_Y(y\|u)$	Conditional PDF of y given the observation of u
■■	$p(u)$	Probability of the occurrence of u
■■	$U(.)$	Unit step function
■■	$Q(.)$	Tail of the Gaussian distribution
■■	$\Gamma(.)$	Gamma function
■■	Ω	Average power
■■	$D_{-v}(z)$	Parabolic cylinder function of order v and argument z
■■	R	Reciprocity degree
■■	LCR	Level Crossing Rate
■□	m	Nakagami parameter
■□	f_m	Doppler Shift
■□	KGR	Key Generation Rate
■□	n_{ij}	AWGN between $node_i$ and $node_j$
■□	σ_{ij}^2	Noise variance between $node_i$ and $node_j$
■□	u_{ij}	Signal (e.g. Probe) sent from $node_i$ to $node_j$
■□	y_{ij}	Received signal sent from $node_i$ to $node_j$
■□	h_{ij}	Channel response between $node_i$ and $node_j$
□□	$\hat{h}_{ij}$	Estimated noisy channel response between $node_i$ and $node_j$
□□	$\hat{H}_{ij}$	A vector of the channel estimates between $node_i$ and $node_j$
□□	R_{Nak}	Nakagami fading envelope
□□	R_{Ray}	Rayleigh fading envelope
□□	R_{Ric}	Rician fading envelope
□□	$G(t)$	Rayleigh fading envelope in complex form
□□	$Z(t)$	Rician fading envelope in complex form
□□	k	Rician factor: Ratio of the specular to scattered power
□□	ξ, S_m	Protocol tuning parameters
□□	$\pm q_i$	Quantization threshold at $node_i$
□□	L_i	Vector of excursions indices extracted at $node_i$
□□	T_c	Channel coherence time

APPENDIX B

Considering the LHS of (8):

$$\frac{(2\alpha_{BA})^{-m}}{\sigma_{BA}} e^{-\frac{y_{AB}^2}{2\sigma_{BA}^2}} \left[e^{\frac{(y_{AB}/\sigma_{BA}^2)^2}{8\alpha_{BA}}} D_{-2m}\left[\frac{-\frac{u_{BA}y_{AB}}{\sigma_{BA}^2}}{\sqrt{2\alpha_{BA}}}\right]\right]$$
$$= \frac{(2\alpha_{BA})^{-m}}{\sigma_{BA}} e^{\frac{1-4\sigma_{BA}^2\alpha_{BA}}{8\sigma_{BA}^4\alpha_{BA}} y_{AB}^2} D_{-2m}\left[\frac{-\frac{u_{BA}y_{AB}}{\sigma_{BA}^2}}{\sqrt{2\alpha_{BA}}}\right]$$
$$= \frac{(\frac{\beta_{BA}}{\sigma_{BA}^2})^{-m}}{\sigma_{BA}} e^{\frac{1-2\beta_{BA}}{4\sigma_{BA}^2\beta_{BA}} y_{AB}^2} D_{-2m}\left[\frac{-\frac{u_{BA}y_{AB}}{\sigma_{BA}}}{\sqrt{\beta_{BA}}}\right] \qquad \text{(B-I)}$$

where $\beta_{ij} = 2m\sigma_{ij} + 1$. Furthermore, we also have the following approximation:

$$D_v(z) = 2^{v/2} e^{-z^2/4} U\left(-\frac{1}{2}v, \frac{1}{2}, z^2\right) \qquad \text{(B-II)}$$

$U(a, b, z)$ is defined as the confluent hypergeometric function of the first kind:

$$U(a, b, z) = \sum_{k=0}^{\infty} \frac{(a)_k}{(b)_k} \frac{z^k}{k!} \qquad \text{(B-III)}$$

where $(n)_k$ is the Pochhammer symbol. Considering the first two terms of (B.III) and (B.II) in (B.I) yields to:

$$LHS = 2^{-m} \frac{(\frac{\beta_{BA}}{\sigma_{BA}^2})^{-m}}{\sigma_{BA}} e^{\frac{1-2\beta_{BA}-u_{BA}^2}{4\sigma_{BA}^2\beta_{BA}} y_{AB}^2} \left(1 + \frac{2mu_{BA}^2\, y_{AB}^2}{\sigma_{BA}^2\beta_{BA}}\right)$$

Utilizing the approximation $1 + x = e^x$ leads to:

$$LHS = 2^{-m} \frac{(\frac{\beta_{BA}}{\sigma_{BA}^2})^{-m}}{\sigma_{BA}} e^{\frac{1-2\beta_{BA}-u_{BA}^2}{4\sigma_{BA}^2\beta_{BA}} y_{AB}^2} e^{\frac{2mu_{BA}^2\, y_{BA}^2}{\sigma_{BA}^2\beta_{BA}}}$$
$$= 2^{-m} \frac{(\frac{\beta_{BA}}{\sigma_{BA}^2})^{-m}}{\sigma_{BA}} e^{\frac{1-2\beta_{BA}+(8m-1)u_{BA}^2}{4\sigma_{BA}^2\beta_{BA}} y_{AB}^2}$$
$$= 2^{-m} \frac{(\frac{\beta_{BA}}{\sigma_{BA}^2})^{-m}}{\sigma_{BA}}$$
$$+ \left[2^{-m} \frac{1-2\beta_{BA}+(8m-1)u_{BA}^2}{4\sigma_{BA}^2\beta_{BA}} \frac{(\frac{\beta_{BA}}{\sigma_{BA}^2})^{-m}}{\sigma_{BA}} y_{AB}^2\right]$$

Finally, applying reciprocity condition to (8), i.e., LHS = RHS to (8) we obtain:

$$\frac{(\frac{\beta_{AB}}{\sigma_{AB}^2})^{-m}}{\sigma_{AB}} + \frac{(\frac{\beta_{AB}}{\sigma_{AB}^2})^{-m}}{\sigma_{AB}} \frac{1-2\beta_{AB}+(8m-1)u_{AB}^2}{4\sigma_{AB}^2\beta_{AB}} y_{BA}^2$$
$$= \frac{(\frac{\beta_{BA}}{\sigma_{BA}^2})^{-m}}{\sigma_{BA}} + \frac{(\frac{\beta_{BA}}{\sigma_{BA}^2})^{-m}}{\sigma_{BA}} \frac{1-2\beta_{BA}+(8m-1)u_{BA}^2}{4\sigma_{BA}^2\beta_{BA}} y_{AB}^2$$

Thus, for $f_Y(y_{AB}|u_{BA}) = f_Y(y_{BA}|u_{AB})$:

$$\frac{(\beta_{AB}/\sigma_{AB}^2)^{-m}}{\sigma_{AB}} = \frac{(\beta_{BA}/\sigma_{BA}^2)^{-m}}{\sigma_{BA}}$$
$$\frac{1-2\beta_{AB}+(8m-1)u_{AB}^2}{4\sigma_{AB}^2\beta_{AB}} = \frac{1-2\beta_{BA}+(8m-1)u_{BA}^2}{4\sigma_{BA}^2\beta_{BA}}$$

Q.E.D

ACKNOWLEDGMENT

The authors would like to thank the Higher Committee for Education Development (HCED) in Iraq for funding Abdulsahib Albehadili's research. The authors also would like to thank the Paul A. Hotmer Family Cybersecurity and Teaming Research (CSTAR) Laboratory as well as the department of EECS at the University of Toledo for provding all the necessary resources to support this research.

REFERENCES

[1] Q. Zhang, P. Wang, D. S. Reeves, and P. Ning, "Defending against Sybil attacks in sensor networks," in *Proc. s25th IEEE Int. Conf. Distrib. Comput. Syst. Workshops*, Jun. 2005, pp. 185–191.

[2] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2418–2434, Jun. 2010.

[3] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis & defenses," in *Proc. 3rd Int. Symp. Inf. Process. Sensor Netw. (IPSN)*, New York, NY, USA, 2004, pp. 259–268.

[4] Data Encryption Standard, *Federal Information Processing Standards Publication 46*, National Bureau of Standards, U.S. Department of Commerce, 1977.

[5] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[6] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, no. 1, pp. 78–88, Jan. 1983. [Online]. Available: http://doi.acm.org/10.1145/1008908.1008920

[7] L. Greenemeier, *Election Fix? Switzerland Tests Quantum Cryptography*. Scientific American, 2007.

[8] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, no. 1, pp. 3–28, Jan. 1992.

[9] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[10] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[11] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[12] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, Sep. 2013.

[13] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[14] T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Netw.*, vol. 21, no. 6, pp. 1835–1846, Mar. 2015.

[15] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[16] 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.

[17] U. M. Maurer and S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 499–514, Mar. 1999.

[18] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[19] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2007, pp. 401–410.

[20] 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 Int. Conf. Mobile Comput. Netw. (MobiCom)*, New York, NY, USA, 2008, pp. 128–139.

[21] 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 Security*, vol. 5, no. 2, pp. 240–254, Jun. 2010.

[22] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

[23] A. Agrawal, Z. Rezki, A. J. Khisti, and M. S. Alouini, "Noncoherent capacity of secret-key agreement with public discussion," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 565–574, Sep. 2011.

[24] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1578–1588, Sep. 2012.

[25] A. Khisti, "Interactive secret key generation over reciprocal fading channels," in *Proc. IEEE 50th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2012, pp. 1374–1381.

[26] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2578–2588, Jun. 2016.

[27] H. Liu, J. Yang, Y. Wang, and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *Proc. 31st IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Orlando, FL, USA, Mar. 2012, pp. 927–935.

[28] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1666–1674, Oct. 2012.

[29] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, "Cryptographic key agreement for mobile radio," *Digit. Signal Process.*, vol. 6, no. 4, pp. 207–212, 1996.

[30] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, Mar. 2010, pp. 1–9.

[31] X. Zhu, F. Xu, E. Novak, C. C. Tan, Q. Li, and G. Chen, "Extracting secret key from wireless link dynamics in vehicular environments," in *Proc. 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Turin, Italy, Apr. 2013, pp. 2283–2291.

[32] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *Proc. 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Turin, Italy, Apr. 2013, pp. 3048–3056.

[33] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Comput.*, vol. 9, no. 1, pp. 17–30, Jan. 2010.

[34] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. 15th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, New York, NY, USA, 2009, pp. 321–332.

[35] S. N. Premnath *et al.*, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 917–930, May 2013.

[36] H. Zhou, L. M. Huie, and L. Lai, "Secret key generation in the two-way relay channel with active attackers," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 3, pp. 476–488, Mar. 2014.

[37] L. Tang and Z. Hongbo, "Analysis and simulation of Nakagami fading channel with MATLAB," in *Proc. IEEE Asia–Pacific Conf. Environ. Electromagn. (CEEM)*, Nov. 2003, pp. 490–494.

[38] L. Xiao, Q. Yan, W. Lou, G. Chen, and Y. T. Hou, "Proximity-based security techniques for mobile users in wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2089–2100, Dec. 2013.

[39] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10037–10047, Dec. 2016.

[40] X. Wan, L. Xiao, Q. Li, and Z. Han, "FHY-layer authentication with multiple landmarks with reduced communication overhead," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[41] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.

[42] D. R. Hardoon, S. Szedmak, and J. Shawe-Taylor, "Canonical correlation analysis: An overview with application to learning methods," *Neural Comput.*, vol. 16, no. 12, pp. 2639–2664, 2004.

[43] P. Elias, "The efficient construction of an unbiased random sequence," *Ann. Math. Stat.*, vol. 3, no. 3, pp. 865–870, 1972.

[44] 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, no. 11, pp. 3776–3784, Nov. 2005.

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

[46] R. Mehmood, J. W. Wallace, and M. A. Jensen, "Key establishment employing reconfigurable antennas: Impact of antenna complexity," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6300–6310, Nov. 2014.

[47] T. Castel, P. Van Torre, and H. Rogier, "RSS-based secret key generation for indoor and outdoor WBANs using on-body sensor nodes," in *Proc. Int. Conf. Military Commun. Inf. Syst. (ICMCIS)*, 2016, pp. 1–5.

[48] M. Yuliana, Wirawan, and Suwadi, "Performance evaluation of the key extraction schemes in wireless indoor environment," in *Proc. Int. Conf. Signals Syst. (ICSigSys)*, May 2017, pp. 138–144.

[49] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, and Y. Ding, "Experimental study on channel reciprocity in wireless key generation," in *Proc. 17th IEEE Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Edinburgh, U.K., Jul. 2016, pp. 1–5.

[50] J. Zhang, R. Woods, A. Marshall, and T. Q. Duong, "An effective key generation system using improved channel reciprocity," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Apr. 2015, pp. 1727–1731.

[51] S. Gopinath, R. Guillaume, P. Duplys, and A. Czylwik, "Reciprocity enhancement and decorrelation schemes for PHY-based key generation," in *Proc. Globecom Workshops*, Austin, TX, USA, Dec. 2014, pp. 1367–1372.

[52] A. Ambekar, M. Hassan, and H. D. Schotten, "Improving channel reciprocity for effective key management systems," in *Proc. Int. Symp. Signals, Syst., Electron. (ISSSE)*, Potsdam, Germany, Oct. 2012, pp. 1–4.

[53] T. K. Sarkar, Z. Ji, K. Kim, A. Medouri, and M. Salazar-Palma, "A survey of various propagation models for mobile communication," *IEEE Antennas Propag. Mag.*, vol. 45, no. 3, pp. 51–82, Jun. 2003.

[54] M. Nakagami, "The *m*-distribution—A general formula of intensity distribution of rapid fading," in *Statistical Methods in Radio Wave Propagation*. Amsterdam, The Netherlands: Elsevier, 1960, pp. 3–36.

[55] T. Aulin, "Characteristics of a digital mobile radio channel," *IEEE Trans. Veh. Technol.*, vol. VT-30, no. 2, pp. 45–53, May 1981.

[56] L. Rubio, N. Cardona, S. Flores, J. Reig, and L. Juan-Llacer, "The use of semi-deterministic propagation models for the prediction of the short-term fading statistics in mobile channels," in *Proc. IEEE VTS 50th Veh. Technol. Conf. Gateway, 21st Century Commun. Village (VTC-Fall)*, vol. 3. Sep. 1999, pp. 1460–1464.

[57] H. Suzuki, "A statistical model for urban radio propogation," *IEEE Trans. Commun.*, vol. 25, no. 7, pp. 673–680, Jul. 1977.

[58] A. U. Sheikh, M. Abdi, and M. Handforth, "Indoor mobile radio channel at 946 MHz: Measurements and modeling," in *Proc. IEEE Veh. Technol. Conf. (VTC)*, Secaucus, NJ, USA, May 1993, pp. 73–76.

[59] T. Zwick, C. Fischer, D. Didascalou, and W. Wiesbeck, "A stochastic spatial channel model based on wave-propagation modeling," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 1, pp. 6–15, Jan. 2000.

[60] J. J. Olmos, A. Gelonch, F. J. Casadevall, and G. Femenias, "Design and implementation of a wide-band real-time mobile channel emulator," *IEEE Trans. Veh. Technol.*, vol. 48, no. 3, pp. 746–764, May 1999.

[61] D. P. Agrawal and Q.-A. Zeng, *Introduction to Wireless and Mobile Systems*. Boston, MA, USA: Cengage Learning, 2015.

[62] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. San Francisco, CA, USA: Academic, 2014.

[63] R. Niu, B. Chen, and P. K. Varshney, "Fusion of decisions transmitted over Rayleigh fading channels in wireless sensor networks," *IEEE Trans. Signal Process.*, vol. 54, no. 3, pp. 1018–1027, Mar. 2006.

[64] L. Cheng, B. E. Henty, D. D. Stancil, F. Bai, and P. Mudalige, "Mobile vehicle-to-vehicle narrow-band channel measurement and characterization of the 5.9 GHz dedicated short range communication (DSRC) frequency band," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1501–1516, Oct. 2007.

[65] M. D. Yacoub, J. E. V. Bautista, and L. G. D. R. Guedes, "On higher order statistics of the Nakagami-*m* distribution," *IEEE Trans. Veh. Technol.*, vol. 48, no. 3, pp. 790–794, May 1999.

[66] C. S. Patel, G. L. Stuber, and T. G. Pratt, "Simulation of Rayleigh-faded mobile-to-mobile communication channels," *IEEE Trans. Commun.*, vol. 53, no. 11, pp. 1876–1884, Nov. 2005.

[67] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proc. Int. Symp. Inf. Theory (ISIT)*, Seattle, WA, USA, Jul. 2006, pp. 2593–2597.

[68] A. Khisti. (2012). "Secret-key agreement capacity over reciprocal fading channels: A separation approach." [Online]. Available: https://arxiv.org/abs/1211.1660

[69] M. A. Tope and J. C. McEachen, "Unconditionally secure communications over fading channels," in *Proc. MILCOM Proc. Commun. Netw.-Centric Operat., Creating Inf. Force*, vol. 1. 2001, pp. 54–58.

[70] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[71] B. Sklar, *Digital Communications*, vol. 2. Upper Saddle River, NJ, USA: Prentice-Hall, 2001.

[72] M. Viswanathan, *Simulation of Digital Communication Systems Using MATLAB*. Los Gatos, CA, USA: Smashwords, 2013.

[73] M. Pätzold, M. Patzold, and M. Paetzold, *Mobile Fading Channels*, vol. 14. Hoboken, NJ, USA: Wiley, 2002.

[74] Y. R. Zheng and C. Xiao, "Simulation models with correct statistical properties for Rayleigh fading channels," *IEEE Trans. Commun.*, vol. 51, no. 6, pp. 920–928, Jun. 2003.

[75] C. Xiao, Y. R. Zheng, and N. C. Beaulieu, "Novel sum-of-sinusoids simulation models for Rayleigh and Rician fading channels," *IEEE Trans. Wireless Commun.*, vol. 5, no. 12, pp. 3667–3679, Dec. 2006.

[76] C. Xiao, Y. R. Zheng, and N. C. Beaulieu, "Statistical simulation models for Rayleigh and Rician fading," in *Proc. IEEE Int. Conf. Commun. (ICC)*, vol. 5. May 2003, pp. 3524–3529.

[77] J. C. S. Filho, M. D. Yacoub, and G. Fraidenraich, "A simple accurate method for generating autocorrelated Nakagami-*m* envelope sequences," *IEEE Commun. Lett.*, vol. 11, no. 3, pp. 231–233, Mar. 2007.

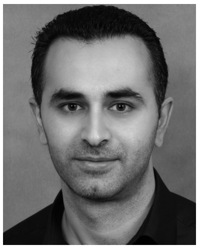
[78] J. K. Tugnait, L. Tong, and Z. Ding, "Single-user channel estimation and equalization," *IEEE Signal Process. Mag.*, vol. 17, no. 3, pp. 17–28, May 2000.

[79] S. Lin and D. J. Costello, *Error Control Coding*. Delhi, India: Pearson, 2004.

[80] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Advances in Cryptology—EUROCRYPT*, T. Helleseth, Ed. Berlin, Germany: Springer, 1994, pp. 410–423.

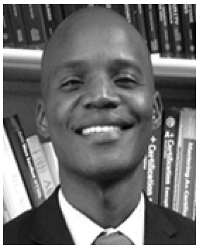
[81] R. Impagliazzo, L. A. Levin, and M. Luby, "Pseudo-random generation from one-way functions," in *Proc. 21st Annu. ACM Symp. Theory Comput. (STOC)*, New York, NY, USA, 1989, pp. 12–24.

ABDULSAHIB ALBEHADILI received the bachelor's degree (Hons.) in communication engineering from Al-Furat Al-Awsat Technical University, Iraq, and the master's degree (Hons.) in wireless communications from Brunel University, London, U.K. He is currently pursuing the Ph.D. degree with the School of Electrical Engineering and Computer Science, The University of Toledo, Toledo, OH, USA. He has the NSF Innovation Corps Program certificate. He is currently the Entrepreneurial Leader of the Physical Layer Security Team, NSF iCorp Project, The University of Toledo. His current research interests include physical-layer security, probabilistic approaches for communications, and channel coding, ranging from theory to design and implementation using software-defined radio. He has collaborated actively with researchers from other universities, mainly on Physical Layer Security research and partially on the implementation and analysis of Polar Codes.



KHAIR AL SHAMAILEH (S'15–M'16) received the B.Sc. degree in telecommunications and electronics engineering and the M.Sc. degree in wireless communications engineering from the Jordan University of Science and Technology, Jordan, in 2009 and 2011, respectively, and the Ph.D. degree in engineering science with an emphasis on electrical engineering from The University of Toledo, Toledo, OH, USA, in 2015. He is currently an Assistant Professor with the Electrical and Computer Engineering Department, Purdue University Northwest, Hammond Campus. His interests include planar antenna design, microwave modeling, multi-/wideband passive and active RF/microwave components design, optimization techniques, wireless security and encryption, localization algorithms in wireless networks, mobile communications, and coding theory.

AHMAD JAVAID received the B.Tech. degree (Hons.) in computer engineering from Aligarh Muslim University, India, in 2008, and the Ph.D. degree from The University of Toledo in 2015. He was a Scientist Fellow with the Ministry of Science and Technology, Government of India, for two years. He joined the EECS Department as an Assistant Professor in 2015, where he is currently the Founding Director of the Paul A. Hotmer Cybersecurity and Teaming Research (CSTAR) Lab, The University of Toledo. During his time at The University of Toledo, he has participated in several collaborative research proposals that have led to a cumulative sum of $4.3 million in funding of which roughly $800K has been allocated specifically to him. These projects have been funded by various agencies including the National Science Foundation, the Air Force Research Laboratory, and the State of Ohio. He also played a critical role in the cultivation of a private gift to support the CSTAR lab for cyber security research. He has authored over 30 peer-reviewed journal and conference papers. His research expertise is in the area of cyber security of drone networks, smartphones, wireless sensor networks, and other systems. He is also conducting extensive research on human–machine teams and the applications of AI and machine learning to attack detection and mitigation. He was a recipient of the prestigious University Fellowship Award. He has also served as a reviewer for several high impact journals and as a member of the technical program committee for several conferences.



JARED OLUOCH received the M.Sc. degree in management information systems from the University of Nebraska, Omaha, in 2009, and the Ph.D. degree in computer science and informatics from Oakland University, Rochester, MI, USA, in 2015. He is currently an Assistant Professor of computer science and engineering technology with the Department of Engineering Technology, The University of Toledo. His research interests include trust and reputation management for vehicular ad hoc networks, information security, localization for wireless sensor networks, and physical-layer security.

VIJAY DEVABHAKTUNI (S'97–M'03–SM'09) received the B.Eng. degree in EEE and the M.Sc. degree in physics from BITS, Pilani, in 1996, and the Ph.D. in electronics from Carleton University, Canada, in 2003. From 2003 to 2004, he held the Natural Sciences and Engineering Research Council of the Canada Post-Doctoral Fellowship and spent the tenure researching with the University of Calgary. In 2005, he taught with Penn State Erie Behrend. From 2005 to 2008, he held the internationally prestigious Canada Research Chair in computer-aided high-frequency modeling and design with Concordia University, Montreal, Canada. In 2008, he joined the EECS Department, The University of Toledo, as an Associate Professor. Since 2012, he has been the Director of the College of Engineering for Interdisciplinary Research Initiatives, and has been recently promoted to a Full Professor. He has co-authored around 190 peer-reviewed papers and is advising 13 M.S./Ph.D. students. His interests are applied electromagnetics, biomedical applications of wireless networks, computer aided design, device modeling, image processing, infrastructure monitoring, neural networks, optimization methods, power theft modeling and education, RF/microwave optimization, and virtual reality. In these areas, he secured external funding close to 5 *million* (sponsoring agencies include AFOSR, CFI, ODOT, NASA, NSERC, NSF, and industry). He is a Registered Member of the Association of Professional Engineers, Geologists, and Geophysicists of Alberta. He was a recipient of the Carleton University senate medal for outstanding scholastic accomplishments at the Ph.D. level. He was also a recipient of several teaching excellence awards in Canada and USA. He serves as the Associate Editor of the *International Journal of RF and Microwave Computer-Aided Engineering*.