Threshold Constraints on Symmetric Key Extraction from Rician Fading Estimates

Gill R. Tsouri and David M. Wagner
Communications Laboratory
Department of Electrical & Microelectronic Engineering
Rochester Institute of Technology

ABSTRACT

Symmetric key establishment using reciprocal quantization of channel estimates in wireless Rician fading environments is considered. The quantization bits from channel-phase and channel-amplitude are treated as the output of a random number generator. We determine threshold constraints on the required minimal distance of the legitimate communicating parties from a passive eavesdropper, and determine threshold constraints on maximal key establishing rates. The analysis makes use of widely accepted statistical test suites applied to the generated bit streams along with a lemma we define and prove. For distance analysis, the minimal required distance from the eavesdropper in order to maintain perfect secrecy during key establishment is derived. For key establishing rates, the maximal rates are derived while ensuring the generated bits streams pass the statistical test suites. The work results in generic and clear threshold requirements on distance and rates as function of the Rician factor and quantization bit for any transmission frequency. Clear thresholds are useful for systems operating in a-priori known or estimated propagation environments. In addition, we address the effect of imperfect channel reciprocity on key agreement. Results show practical systems can operate under reciprocal and secure conditions, and that channel-phase estimates perform better than channel-amplitude estimates.

Keywords – Wireless Physical Layer Security, Rician Fading, Symmetric Encryption Key.

Digital Object Indentifier 10.1109/TMC.2012.226

1. INTRODUCTION

The broadcast nature of wireless communication links exposes them to eavesdropping and other malicious attacks. Securing a wireless link is paramount in many applications and systems to protect privacy and block malicious attacks. In traditional symmetric encryption systems, a large pre-deployed secret key is shared by the two communicating parties. The same key is used to encrypt and decrypt information. A prominent example is the *Advanced Encryption Standard* (AES) [1], where a 128 bit key is typically used. Asymmetric encryption is based on public-key cryptography where the public key is not secret and is used to encrypt information. Decryption can only be performed using a private key which is secretly kept. A prominent example is the *Rivest-Shamir-Adleman* (RSA) [2] algorithm. Both types of encryption methods are based on security by complexity and provide adequate security to date. Symmetric methods are characterized by lower algorithmic complexity, while asymmetric methods are characterized by lower key management complexity.

To minimize complexity, one could use a simpler symmetric encryption method such as a stream cipher [3] coupled with periodic key establishing to compensate for its weak encryption strength. To this end, a method of securely establishing a symmetric encryption key is needed. A prominent method used in practice is the Diffie-Hellman algorithm [4] which reintroduces high algorithmic complexity.

Implementing these traditional cryptographic methods involves the use of considerable online computation power, memory space and communication overhead, and could prove impractical in resource-constrained devices such as implanted medical devices, compact mobile devices and wireless enabled bio-sensors. The costs associated with securing a wireless link in resource-constrained devices received considerable attention in the past – see [5] for example. A low-

complexity alternative for establishing a symmetric key is attractive provided that it is authenticated and secure from eavesdropping. Such an alternative would allow the use of low-complexity symmetric encryption coupled with frequent key establishment.

In recent years, there has been increased attention to the use of wireless physical layer security to establish *information theoretic security* as a low cost alternative to standard encryption methods based on *computational complexity*. Previous work on the secrecy capacity of wireless fading channels showed they have an intrinsic property of concealing information from an eavesdropper – see [6-12] for prominent examples. In addition, the literature depicts many attempts to practically use the secrecy-capacity to implement information theoretic security - see [13-28] and references therein for examples.

We focus our attention on low-complexity methods of symmetric key extraction based on reciprocal quantization of narrow-band channel estimates such as those reported in [15-21]. Narrow-band channel estimates are accessible via existing pilot and data signals carried over single-carrier transmission or *Orthogonal Frequency Division Multiplexing* (OFDM) subcarriers for example. In [15], knowledge of the channel-phase is used to encrypt data with some arbitrary quantization. In [16] reciprocal random fluctuations in the signal amplitudes are quantized to generate keys. In [17] key generating is simulated for ultra wideband channels, while in [18-21,28] the channel phase and/or amplitudes are directly quantized to generate secret key bits.

When considering security strength, two important aspects are of interest: the ability of an eavesdropper to deduce the key and the achievable key establishing rates. Most suggested practical methods did not consider the security strength of the generated key bits. In cases where security strength was assessed it was usually done using an information-theoretic approach by

evaluating the secrecy capacity and the mutual information between a passive eavesdropper with SNR disadvantage and the legitimate communicating parties – see [16,18,19,21] for examples.

Another issue of importance is the ability to authenticate a legitimate communicating party. In the framework of wireless physical layer security, we must assure that a legitimate communicating party is estimating the channel with a legitimate counterpart and not an adversary. It is common practice to treat the authentication problem separately.

The problem of authentication over the wireless channel received considerable attention in the past. Prominent examples include the work presented in [25-28]. In [25] the authors design a hypothesis test for authentication based on the ability to identify the channel response with specific parties. In [26] the authors consider a Rayleigh fading channel and propose a generalized likelihood test for testing the hypothesis that consecutive channel samples belong to the same legitimate party, while in [27] they use a related framework for effectively detecting a Sybil attack. In [28] a prototype system is evaluated where the wireless signal from a third party is used by two communicating parties in close proximity to extract authenticated secret bits. In this contribution, we assume a reliable authentication method is in place.

In most reported work on symmetric key establishment, it was assumed that the eavesdropper is sufficiently distanced from the intended receiver so that the channel from transmitter to receiver is independent of the channel from transmitter to eavesdropper. Under this assumption, channel estimates at the receiver are unique, and the eavesdropper is blocked access to them due to space selectivity of the wireless channel. This results in independent channels and therefore perfect secrecy for key establishment.

A mobile eavesdropper can make an attempt to near the intended receiver and compromise the basic assumption of independent channel estimates. In other words, the eavesdropper can

perform a *proximity attack* to reduce the space selectivity of the wireless channel. As a result, the eavesdropper would be able to gain knowledge of the channel estimates at the receiver based on its own channel estimates and thereby deduce the key with some certainty. In an extreme scenario, the eavesdropper could attach its antenna to that of the receiver to experience the same channel with the transmitter. This implies that an effective proximity attack would hinder any practical method based on channel randomness. The question is: what is the minimal required distance of an intended receiver from a potential eavesdropper to securely establish the key?

An analysis of security strength in the face of proximity attacks is crucial for evaluating the efficacy of encryption methods based on channel randomness and for promoting their possible acceptance as alternatives to traditional methods. There is limited reported work on the vulnerability of practical symmetric key establishment methods using channel randomness in the presence of a proximity attack. Information-theoretic analysis results in an assessment of the mutual information between the eavesdropper and the legitimate communicating parties. This is a soft estimate which is important for qualitatively assessing the secrecy of key exchange, but does not provide a clear and definite threshold on required distance from the eavesdropper. The most relevant work assessing the impact of a proximity attack was reported in [21,28].

In [21], a measurement campaign was conducted to evaluate the limits of key establishment based on reciprocal quantization of *Multiple Input Multiple Output* (MIMO) channels in the presence of a passive eavesdropper. Information theoretic analysis is used to find the percent of vulnerable secret bits out of the total number of generated bits as a function of the distance between eavesdropper and receiver. The difference in SNR of the channels to eavesdropper and receiver, the number of multipath components, presence of *Line of Sight* (LoS) and number of antenna being used are considered as system parameters and affect the ratio of vulnerable bits.

In [28] a prototype system for establishing authenticated keys is presented and evaluated. The legitimate parties are placed in close proximity and an adversary is assumed to be farther away. A third party transmits a pilot signal which is used by the legitimate parties to extract secret bits by quantizing channel-phase and channel-amplitude estimates. Since the legitimate parties are very close they extract the bits in agreement. An experimental setup was used to evaluate an eavesdropper's ability to deduce the key as a function of its distance from the legitimate parties. An experimental setup was used to gather data. Measurement results show that a distance of half a wavelength is required to have a bit mismatch of ~50% between the eavesdropper and the legitimate parties.

In contradistinction to past work, we present thresholds on the required distance from the eavesdropper guaranteeing complete secrecy of keys for any number of antennas and any SNR advantage at the eavesdropper. In addition, we use a Rician fading channel simulator instead of measurements to cover a wide variety of propagation scenarios.

Key establishing rates received considerable attention in the past. In general, the achievable key establishing rates depend on channel decorrelation in time (the channel coherence time). If bits are extracted from the channel too frequently, the channel would not decorrelate sufficiently and successive channel estimates and subsequent generated secret bits would be correlated. The strength of the key is diminished if successive secret bits are correlated.

Past reported work on achievable key refreshing rates applied an information-theoretic approach based on evaluating the secrecy capacity. Using this approach, the achievable key rates largely depend on channel conditions. For example, in a single antenna system, if the capacity of the channel from transmitter to eavesdropper is higher than that from transmitter to receiver, the secrecy capacity is zero and secure transmission is not possible. A more direct approach was

applied in [28], where the key rates were assessed by estimating the channel coherence time and expected bit error rates for the considered prototype system.

In this contribution, we treat the wireless fading channel as a source of randomness used to create a *Random Number Generator* (RNG) via quantization of its reciprocal estimates. This allows us to obtain clear thresholds on the required distance from an eavesdropper and maximal key establishing rates of practical low-complexity methods.

We investigate the Rician fading environment as it describes many practical fading scenarios via a single parameter (the Rician factor). For example, a Rician factor of 0 would model Rayleigh fading representing rich multipath scenarios, and a high Rician factor would model a strong LoS component likely to be present in vehicular and mobile access scenarios. Since we are interested in evaluating the security strength of the Rician channel regardless of a specific key distillation algorithm, we first assume perfect channel estimation and reciprocity.

We consider key establishing using reciprocal quantization of channel amplitude and phase, becasue this is the approach taken by most practical methods for low-complexity bit extraction. It should be noted that there are more elaborated methods of secret extraction from correlated channel estimates. These methods rely on decorrelation procedures and secret distilling which increase implementation complexity.

Evaluating the Rician fading channel as a source for generating encryption keys would have to rely on channel data obtained from experimental setups or a channel model implemented using a simulator. Experimental setups are important for evaluating specific systems and algorithms operating in practical scenarios and allow for assessing performance in specific propagation environments. A channel model is naturally limited in its description of the physical world, but offers the flexibility to control and sweep through many propagation scenarios. Since the focus

of this paper is on the Rician channel and not a specific system, we use a simulator to synthesize channel data for analysis. The Rician channel model assumes wide-sense stationary scattering from uncorrelated scatterers and is widely used to evaluate practical propagation environments.

Our analysis makes use of the Rician channel simulator reported in [29], the *National Institute of Science and Technology* (NIST) random number generator statistical test suite [30], and a supporting lemma we define and prove. The simulator in [29] offers high accuracy with regard to the random nature of the Rician factor and was successfully used in past work to synthesize Rician fading channels.

The NIST test suite [30] was used extensively to evaluate many cryptographic random number generators. Some past work made use of statistical tests to evaluate the generated key bits [22-24]. Tests were applied to bit streams gathered via experimental field trials using specific key distillation algorithms and for unknown Rician factors. We are unaware of a previous attempt to systematically evaluate the inherent security strength of fading channels as sources of RNGs.

For proximity attacks, we evaluate the minimum required distance between receiver (either one of the legitimate communicating parties) and eavesdropper so that perfect secrecy is maintained, regardless of a possible SNR advantage of the eavesdropper and the number of antennas being used. The analysis results in thresholds on the required distance to achieve perfect secrecy for key establishment as a function of the Rician factor and quantization bit. Such clear thresholds are useful for practical systems where the channel environment changes dynamically resulting in variable and unknown SNR advantage for the eavesdropper or when the number of antennas at the eavesdropper is unknown.

For key establishment rates, we treat the sequence of generated secret bits as the output of a RNG. Assuming the eavesdropper is sufficiently far from the communicating parties to render a

proximity attack ineffective, we are left with the need to validate the randomness of our channel-based RNG output. To this end, we use the NIST statistical test suite [30] in its entirety.

A common assumption in past work is that of perfect reciprocity. In this work, we first assume perfect reciprocity for evaluating key refreshing rates and proximity attacks, but then evaluate the effect of imperfect reciprocity on performance. In the framework of reciprocal quantization of channel estimation, imperfect reciprocity is the result of the communicating parties taking turns in estimating the channel over the same frequency. Taking turns cannot be avoided, since full-duplex communications is not a practical possibility in existing wireless transceivers.

The rest of the paper is organized as follows. In Section 2 we derive the analysis for proximity attacks, key establishment rates and the effect of imperfect reciprocity for a RNG based on reciprocal quantization of the Rician fading channel. In Sections 3 and 4 the analysis is applied to channel-phase and channel-amplitude. Generic results on threshold distances and rates are depicted in Section 5 along with practical examples. Section 6 concludes the work.

2. ANALYSIS

We consider the scenario depicted in Fig. 1, where two legitimate communicating parties (Alice and Bob) are establishing a key using reciprocal quantization of channel-phase or channel-amplitude. The eavesdropper (Eve) performs a proximity attack in attempt to decipher the key by approaching Bob or Alice during key establishment. Other than approaching one of the communicating parties, Eve is passive. Alice and Bob alternate roles as receiver and transmitter. We consider the distance of the eavesdropper from Alice.

We assume that some efficient method is used by Alice and Bob to accurately estimate the channel coefficient. Following the assumptions made in [12-18], we first assume that the channel is reciprocal for sufficient time so that Alice and Bob estimate the same value. We then assess

the impact of imperfect reciprocity by evaluating the probability for Bob and Alice to generate matching keys in practical scenarios.

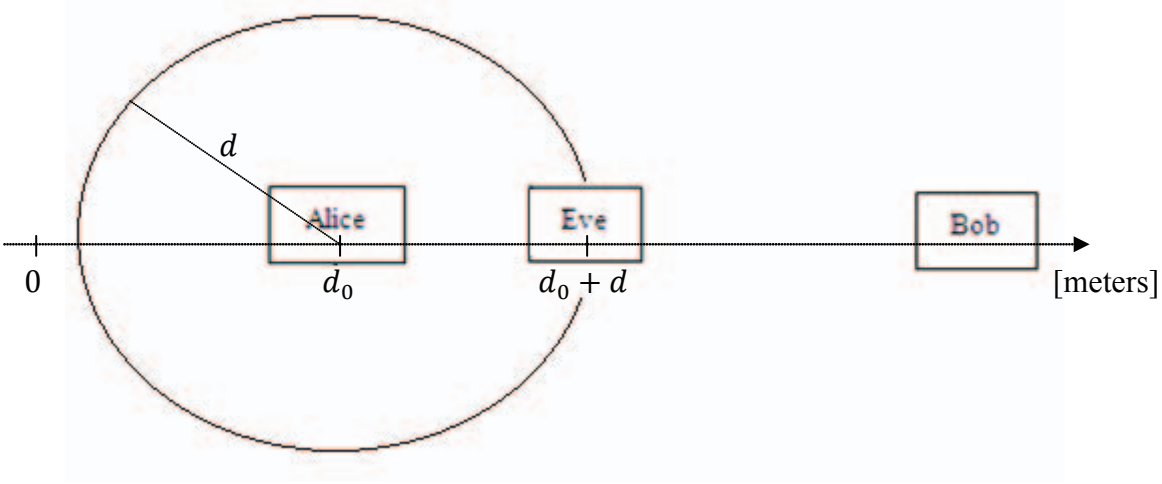

Fig. 1 – Key establishment in the presence of a mobile eavesdropper. Eve performs a proximity attack by decreasing its distance d from Alice to reduce space-selectivity of the fading channel.

The channel estimate is quantized to an arbitrary number of quantization bits which represent secret bits. The process is periodically repeated to generate the necessary amount of secret bits to form the encryption key. For the sake of analysis, we consider each bit of the quantization separately as if the key is generated by accumulating a single bit per quantized estimate. It should be noted that key establishment could fail due to quantization errors caused by receiver noise and estimation errors. The impact of such maladies depends on the quantization method and specific system at hand and is outside of the scope of the work presented in this paper.

We assume that the reciprocal bit extraction method being used is designed such that maximal key entropy is achieved, i.e., all possible keys are equally probable [31]. This means that the probability for any generated key bit to be zero or one is the same. This could translate to performing non-uniform quantization depending on the *Probability Density Function* (PDF) of the channel parameter being estimated. In addition, note that since Eve and Alice are in close

proximity they experience the same signal propagation environment. It follows that we may use the same channel model and Rician factor for both of them.

Since we require perfect secrecy during key establishment and key establishing rates which remain secure, we decouple analysis of proximity attacks and key establishing rates. In what follows, we assume a secure key establishing rate is used when performing analysis of proximity attacks, and that sufficient space separation between receiver and eavesdropper is in place when performing analysis of key establishing rates.

Although the analysis that follows focuses on channel-phase and channel-amplitude, it is readily applicable to quantization of other channel parameters.

2.1 Proximity Attacks

We use the time-based model given in [29] to describe the varying channel in space. This is justified due to the channel duality between space and time [32,33]. We use the following variable translation between space and time:

$$\frac{d}{\lambda} = f_D t \tag{1}$$

where d is distance in meters from an arbitrary reference point, λ is the wavelength associated with the frequency of operation, f_D is the Doppler shift, t is time and $\omega_D = 2\pi f_D$. This equivalency is also evident in [32] for the Rayleigh fading scenario. Further discussion on space-time duality in wireless channels can be found in [33].

Using the model in [29] and (1) we form the space-based model:

$$Z_c(d) = \frac{\frac{1}{\sqrt{N}}\sum_{n=1}^{N}\cos\left(\frac{2\pi d}{\lambda}\ cos(\alpha_n)\right) + \phi_n)}{\sqrt{1+K}} + \frac{\sqrt{K}\cos\left(\frac{2\pi d}{\lambda}\cos(\theta_0) + \phi_0\right)}{\sqrt{1+K}} \tag{2}$$

$$Z_s(d) = \frac{\frac{1}{\sqrt{N}}\sum_{n=1}^{N}\sin\left(\frac{2\pi d}{\lambda}\ cos(\alpha_n\right) + \phi_n)}{\sqrt{1+K}} + \frac{\sqrt{K}\sin\left(\frac{2\pi d}{\lambda}\cos(\theta_0) + \phi_0\right)}{\sqrt{1+K}} \tag{3}$$

where $Z_c(d)$ and $Z_s(d)$ represent the in-phase and quadrature components respectively at the Eve, K is the Rician Factor, N is the number of multipath components, θ_0 is the angle-of-arrival of the LoS, ϕ_0 is the initial phase of the LoS component, $\{\phi_n\}$ are the initial phases of the scattered components, and $\{\alpha_n\}$ are the angles-of-arrival of the scattered components.

The model in (2) and (3) allows for evaluating the correlation between any two points in space. Note that the conversion of the model from time to space forces us to assume the same Doppler shift (f_D) across the distance (d). In our case, this is not a problem because we consider close proximity (d is on the order of the wavelength), and it is safe to assume that the propagation conditions are the same across such short distances.

Alice and Eve obtain a channel estimate using the pilot signal from Bob. They then convert the channel estimate to a vector of B bits. We denote these vectors at Alice and Eve as $\boldsymbol{k^r} = [k_1^r, k_2^r, \dots, k_B^r]$ and $\boldsymbol{k^e} = [k_1^e, k_2^e, \dots, k_B^e]$ respectively. If $\boldsymbol{k^e}$ and $\boldsymbol{k^r}$ are independent the eavesdropper would not be able to deduce $\boldsymbol{k^r}$.

We define the following binary random variable:

$$\Delta e = k_i^r \oplus K_i^e \tag{4}$$

where $\oplus$ is the modulo 2 sum operation (exclusive or) and i is chosen out of $1, \dots B$ to reflect a specific bit in the quantized binary vector.

Lemma 1:

Let X and Y be discrete binary random variables each uniformly distributed and let $Z = X \oplus Y$. X and Y are independent if and only if Z is uniformly distributed. See Proof in Appendix A.

The quantized bits are binary random variables, each uniformly distributed. It follows from *Lemma 1* that if Δe is uniform, k_i^r and K_i^e are independent and Eve can gain no knowledge on the established key bit by observing its own channel estimates. To analyze proximity attacks, we

would apply the NIST monobit test [30] to assess the uniformity of Δe for various distances from Eve. No additional test is required.

Using the Rician channel model, we generate bit streams of single quantization bit positions for a given distance and calculate Δe. We then apply the NIST frequency monobit test to evaluate the uniformity of Δe. If the proportion pass-rate exceeds the threshold determined by the sequence length, the bit position of Δe is considered to be uniformly distributed. It follows that Eves observations are independent of those of Alice, and Eve can gain no knowledge of the generated key based on her channel estimates. This means that the space selectivity of the wireless channel, as determined by the distance between Eve and Alice, is sufficient to securely generate a key by quantizing the channel estimates.

2.2 Key Establishing Rates

A key is established between Alice and Bob by quantizing consecutive channel estimates obtained periodically from pilot signals. Hence, Alice and Bob sample the channel at an arbitrary sampling interval. Consecutive samples of a single bit from the quantized channel parameter comprise a random bit sequence which is the secret key. We apply the entire NIST test suite to the bit sequence per quantization bit as if it originated from a RNG. See Appendix B for a concise description of all the tests in the NIST statistical test suite. It is expected that if the sampling interval is too short, consecutive bits would be correlated and the bit sequence would fail the tests. We look for the minimum sampling interval for which the bit sequence passes all tests. The maximum key establishing rate is the reciprocal of the minimum sampling interval.

In order to formulate a testing strategy, we observe the channel in-phase and quadrature autocorrelation functions in the time-based Rician fading channel model in [29]:

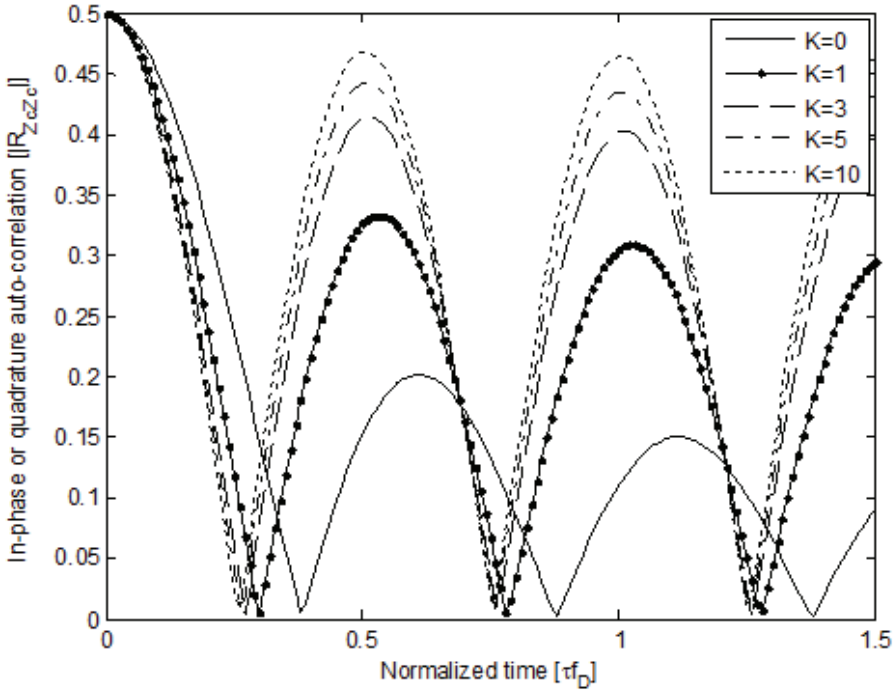

Fig. 2 – Rician channel decorrelation over time. A large Rician factor results in faster decorrelation but also higher correlation peaks.

$$R_{Z_cZ_c}(\tau) = R_{Z_sZ_s}(\tau) = \frac{J_0(\omega_d\tau) + Kcos(\omega_d\tau cos(\theta_0))}{2 + 2K} \quad (5)$$

where J_0 is the zero-order Bessel function of the first kind. We plot the absolute value of $R_{Z_cZ_c}(\tau)$ as a function of time normalized to the Doppler shift and $K \in [0, 1, 3, 5, 10]$ in Fig. 2. Note that as K increases the slope of $|R_{Z_cZ_c}(\tau)|$ increases as well. This means that the autocorrelation changes faster over time. It follows, that the channel decorrelates faster immediately after a peak value. This could compromise channel reciprocity as the channel might decorrelate while Alice and Bob are taking turns estimating the channel. Also note that the peak correlations are increased when K is increased. This implies key rates would decrease since Alice and Bob would have to wait longer for the channel to decorrelate across peaks.

The randomness of the channel for a particular sampling interval is related to the in-phase and quadrature components' autocorrelation value at that time. We observe that sampling at a zero

crossings in Fig. 2 would produce a channel estimate which is completely uncorrelated with the previous channel estimate. In an ideal setting, Alice and Bob would sample at this zero-crossing and achieve an extremely high key establishing rate. However, sampling precisely at the zero-crossing would require impractical precision, especially when considering imperfect reciprocity as the communicating parties take turns in sending pilots and sampling the channel over the same frequency. We assume the worst case of sampling on a peak corresponding to maximum correlation between consecutive channel estimates.

For a particular Rician factor, we must extract the sequence of sampling intervals corresponding to the extrema of $|R_{Z_c Z_c}(\tau)|$. To this end, a local extrema search is used for tested values of the Rician factor. The intervals corresponding to the extrema points are investigated.

For each sampling interval, a sequence of quantized channel estimates is generated using B bits per estimate. The quantized estimates are partitioned into separate sequences of random bits, where each sequence corresponds to a specific bit in the quantization bits vector $[k_1^r, k_2^r, \dots, k_B^r]$. Each sequence is evaluated using the entire NIST statistical tests suite. The smallest sampling interval, for which the sequence passes all NIST tests, corresponds to the smallest secure sampling interval. The inverse of this sampling period is the maximum key establishing rate for a specific quantized bit position and is denoted as $R_{b_{max}}$.

Recall that our analysis assumes quantized bits from the channel estimate are directly taken as secret bits. This approach has the lowest implementation complexity. It could still be possible to extract a secret bit at higher rates by using coding. This would increase system complexity.

2.3 Effect of Imperfect Reciprocity

The framework we established for analysis of key establishing rates is readily applicable to evaluate the effect of imperfect reciprocity. To obtain channel estimates assuming a practical

half-duplex system, Alice and Bob take turns transmitting pilot signals over the same frequency. Bob's channel estimates are obtained from a pilot signal sent by Alice and vice versa. The time that passes between channel estimates at Alice and Bob is a fundamental cause of imperfect reciprocity and is a system specific parameter. We wish to synthesis samples which reflect this time offset using the Rician fading channel simulator. To this end, we generate two channel instances with a timing offset equal to the time it takes a pilot signal to be sent and received. This is done by setting the sampling period in Section 2.2 to be the timing offset. This process is repeated multiple times to generate statistics on the matching between bits at Alice and Bob when these samples are quantized.

Imperfect reciprocity could also be caused by variations in transceiver hardware, interference and noise levels. In addition, in cases where Alice and Bob are very far apart compared to the wavelength of the pilot on the order of tens of meters, the propagation delay could become a major cause of imperfect reciprocity. It follows that establishing a symmetric key over a half-duplex channel inherently limits the distance between Alice and Bob.

Note that having some probability for bit mismatch does not mean system failure. Alice and Bob can send a challenge message to test key agreement. If they discover key establishing failed they only need to try again. The price is a reduction in the key establishment rate.

3. CHANNEL-PHASE QUANTIZATION

We now apply the analysis to key establishment based on reciprocal quantization of the channel-phase. Estimating a reciprocal channel-phase is not trivial. In a practical system, Alice and Bob would have to account for varying frequency drifts in their local oscillators. There are practical systems where reciprocal channel-phase was successfully estimated and used to extract key bits through quantization. A very recent example is the prototype system presented in [28] where the

differential phase was estimated across consecutive phase estimates. We assume Alice and Bob obtain accurate phase estimates which are then used to establish the key.

A graphical description of the quantization process is given in Fig. 3. A phase estimate $\emptyset$ assuming any value within $[-\pi, \pi)$ is mapped to a phase value belonging to a finite set of phases. Each such phase corresponds to a set of B bits. As B increases, the number of quantization levels increases and more bits are extracted per phase estimate.

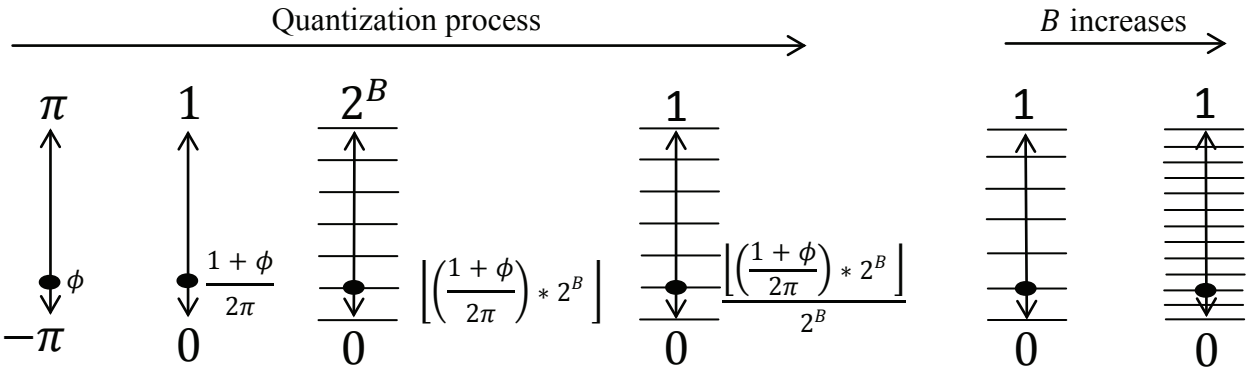

Fig. 3 – Process of quantizing a phase estimate.

3.1 Proximity Attacks

The channel-phase at the eavesdropper and receiver is given by

$$\theta_e = \arctan\left(\frac{Z_s(d)}{Z_c(d)}\right) \tag{6}$$

and

$$\theta_r = \arctan\left(\frac{Z_s(d_0)}{Z_c(d_0)}\right) \tag{7}$$

respectively. In order to generate the phase of a Rician fading channel, we first generate the received in-phase and quadrature components. Loosely stated, if the sign of Z_s and Z_c are

considered, full phase mapping is obtained and $\theta_e, \theta_r \in [-\pi, \pi)$. The phases are uniformly quantized to obtain $\boldsymbol{k^e}$ and $\boldsymbol{k^r}$.

Without loss of generality, we assume the eavesdropper and receiver are at a distance of d and d_0 respectively from some reference point placed on a straight line going through receiver and eavesdropper positions. Refer to Fig. 1 for a graphical description. We set the receiver to be at the reference position ($d_0 = 0$). For distances d and d_0, we used $N = 8$ multipath components to generate (2) and (3), from which (6) and (7) follow. Note that $N = 8$ was shown in [29] to be sufficiently high to accurately synthesize the Rician channel. The frequency monobit test requires a bit stream length of at least 100, and a significance level of $\alpha = 0.01$ requires $\frac{1}{\alpha} = 100$ bit streams. We generated 10^5 phases, which we then quantized to $B = 6$ bits. $B = 6$ was chosen after multiple observations showed this quantization is sufficient for passing the NIST tests. We formed Δe as in (4) and generated 1000 bit streams of sequence length 100 for each of the 6 bit-positions. Δe from each bit stream was then input to the NIST frequency monobit test.

For generality, we normalized the distance d by the carrier wavelength λ. We considered a normalized distance of $0 < d/\lambda \leq 1$, assuming the eavesdropper is always able to be within a wavelength of the receiver. We found the largest distance in this range for which the NIST monobit test failed. The distance up to the failing distance is the minimal required distance to securely generate the key and is noted d_{min}. If a distance of $d = \lambda$ failed the NIST test, we declare key generation as a failure. The aforementioned strategy was executed on each of the 6 quantized bit-positions with $K \in [0,1,3,5,10]$.

3.2 Key Establishing Rates

The channel-phase using the time model in [29] is given by

$$\theta_R(nT) = \arctan\left(\frac{Z_s(nT)}{Z_c(nT)}\right);\ n = 1,2,\dots,z \tag{8}$$

Eq. (8) generates a sequence of consecutive phases of length z. We generate m total number of such sequences. We first scale each phase θ_i from the range $[0,2\pi)$ to the range $[0,2^B)$

$$\theta_R'[n] = \theta_R(nT) * \frac{2^B}{2\pi} \tag{9}$$

and uniformly quantize these phases into B bits per phase,

$$\theta_R^Q = \lfloor \theta_R'[n] \rfloor, \tag{10}$$

where $\lfloor \cdot \rfloor$ denotes the floor operation. After quantizing, we have a matrix of bits of size m by z by B. We select a bit position $b \leq B$ and reshape the data into m bit streams of length z.

We ran a sweep of phase sampling period (T_s) values corresponding to the extrema in Fig. 2 using quantization of $B = 8$ bits, $N = 8$ multipath components, bit positions of $b \in [3,4,5,6,7,8]$ and Rician factors of $K \in [0,1,3,5,10]$. $B = 8$ was chosen after multiple observations showed this quantization is sufficient for passing the NIST tests. We then applied the NIST test suite with sequence length $z = 10^6$ so that we could execute all tests. We used a significance level of $\alpha = 0.01$, requiring $m = \frac{1}{\alpha} = 100$ sequences. Tab. 1 shows tests parameters. We determined $R_{b_{max}} = 1/T_s$ which simultaneously meets the randomness threshold for every test, across the aforementioned space of (K, b). For generality, we normalized time by the Doppler shift.

Tab. 1 – Parameters for NIST tests

Test	Parameter	Value
Block Frequency	block size	100000
	# blocks	10
Longest Run of Ones	block size	10000
	# blocks	75
Binary Matrix Rank	# matrix rows	32
	# matrix cols	32
Non-overlapping Template Matching	# blocks	8
	block size	125000
	template size	9
	template	000000001
Overlapping Template Matching	template size	9
	template	000000001
Maurer's "Universal Statistical"	block length	7
	# blocks	1280
Linear Complexity	block length	1000
	degrees of freedom	7
Serial	block length	3
Approximate Entropy	block length	2
Random Excursions	States	{-4..-1}{1..4}
Random Excursions Variant	states	{-9..-1}{1..9}

4. CHANNEL-AMPLITUDE QUANTIZATION

The channel-amplitude at the Eave and Alice is given by

$$A_e = \sqrt{Z_S^2(d) + Z_C^2(d)} \;\; ; \;\; A_r = \sqrt{Z_S^2(d_0) + Z_C^2(d_0)} \tag{11}$$

respectively. We applied the same analysis as applied to channel-phase in the previous section. A full description is omitted for brevity

Note that in practical systems, the mean of the amplitude estimates is sometimes estimated and removed. This is done for matching gain control between Alice and Bob and for making sure the full dynamic range for quantization is random. Subtracting a perfect estimation of the mean prior to quantization would shift the dynamic range of the quantized bits. In other words, MSBs after

subtracting the mean would mirror LSBs prior to subtracting the mean. The results would not change except for the bit notation.

5. RESULTS

5.1 Channel-Phase Quantization

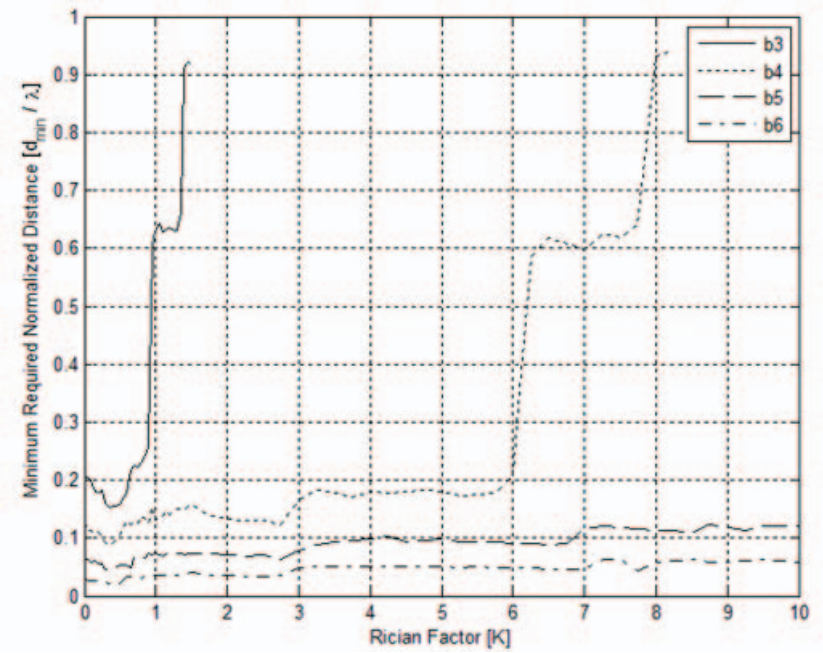

Fig. 4 – Minimum distance as a function of the Rician factor for various phase quantization bits. Note the staircase threshold behavior for required minimum distance from Eve.

Fig. 4 depicts the minimal required distance (d_{min}) to ensure perfect secrecy normalized by the transmission wavelength (λ) as a function of the Rician factor (K) for various quantization bits of the channel-phase. In the figure, b3 denotes *Most Significant Bit number 3* (MSB #3) and so on. For brevity we omit failed attempts ($d_{min} > \lambda$) from the graph. Bits b1 and b2 provided $d_{min} > \lambda$ for all values of K are therefore not represented in the figure. It is apparent that as K increases d_{min} increases as well. This is because a higher K results in less dominant multipath and hence less randomness of the channel. We observe that deeper quantization bits help decrease d_{min}. This is because deeper quantization bits are sensitive to smaller channel variations across space. As long as the quantization noise is tolerable, the loss of channel randomness due to high K can

be compensated by using a deeper quantization bit. Note the discrete levels of d_{min} for varying K. This is a manifestation of the hard-decision threshold output (pass or fail) of the NIST monobit test and is useful for determining clear requirements for d_{min} as a function of K.

The results in Fig. 4 determine how far a receiver must be from the eavesdropper to foil a proximity attack in practical systems. For example, transmission in the *Industrial Scientific Medical* (ISM) bands $2.45GHz$, $915MHz$ and $434MHz$ correspond to a wavelength of $12.2cm$, $32.7cm$ and $69.1cm$ respectively. Bit b3 of the phase quantization can be used for $K < 1$ if the receiver is at least $2.4cm$, $6.5cm$ and $13.8cm$ away from the eavesdropper for $2.45GHz$, $915MHz$ and $434MHz$ respectively. Such K values describe well a rich scattering environment with no dominant multipath component. If b4 is used, the same distances ensure security for $K < 6$. If bit b4 is used in a $2.45GHz$ IEEE 802.15.4 system (ZigBee, BlueTooth) and the channel is known to be Rician fading with $K \leq 8$ a distance of at least $7.3cm$ between receiver and eavesdropper is required. Such K values describe well a dominant multipath component such as present in vehicular communications. These distances seem reasonable for many practical systems. For quantization bits higher than five bits, the required distance is below $\lambda/10$, which corresponds to a minimal distance of $1.2cm$, $3.3cm$ and $6.9cm$ for $2.45GHz$, $915MHz$ and $434MHz$ respectively.

Fig. 5 depicts the maximal key refreshing rate ($R_{b_{max}}$) normalized to the Doppler shift (f_D) for which the generated bits are sufficiently random as a function of the quantization bit (b) of the channel-phase for various values of the Rician factor (K). Recall that $R_{b_{max}}$ corresponds to cases where the bit stream passes the entire NIST test suite. The value of K is noted above each bar in the figure. We note that $R_{b_{max}}$ varies inversely with K, since a higher K increases the ratio between LoS and scattered power resulting in reduced randomness. We also observe that

$R_{b_{max}}$ increases with a higher b, since a deeper quantization bit is more sensitive to small channel variations over time.

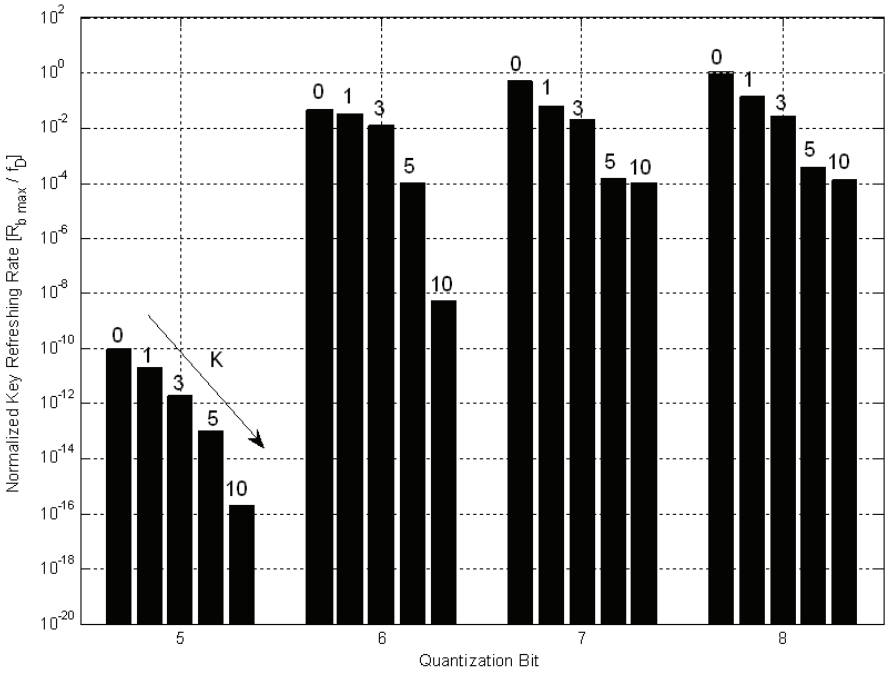

Fig. 5 – Maximum key rates as function of phase quantization bit for various Rician factors. Each bar column is determined by the minimum key rate obtained over all NIST tests. Note the reduction in key rate as the Rician factor is increased.

The results in Fig. 5 are useful for determining achievable key establishing rates in practical systems. For example, consider a stationary scenario with no LoS ($K = 0$, Rayleigh fading), where the dynamic environment corresponds to a low Doppler shift of $f_D = 5Hz$. In such a scenario, one may attain the following key refreshing rates: $6\,x\,10^{-2}\,\frac{bits}{sec} *\ 5 = 0.3\,\frac{bits}{sec}$ using bit b6 and $7\,x\,10^{-1}\,\frac{bits}{sec} * 5 = 3.5\,\frac{bits}{sec}$ using bit b7. This means that it would take $313sec$ to establish a 64 bit key using only bit b6, and $18sec$ to establish the same key using only bit b7. As another example, consider a mobile environment corresponding to $f_D = 200Hz$ with a LoS component corresponding to $K = 3$. In such a scenario, using only $MSB\ \#6$ to establish a 128 bit key would require $128/(10^{-2} * 200) = 64\ sec$.

5.2 Channel-Amplitude Quantization

Fig. 6 depicts d_{min}/λ as a function of K for various quantization bit of the channel-amplitude. The same trends are apparent with regard to quantization bit and K as observed for the channel-phase in Fig. 4. Note that the channel-amplitude is characterized by larger d_{min} compared to channel-phase. For example, b3 fails to provide adequate d_{min} for all tested values of K and so would be easily compromised with a proximity attack (unlike b3 of the channel-phase). As another example, if MSB#4 is used and the channel is known to be Rician fading with $3 \leq K \leq 4$ a normalized distance of at least $0.5/\lambda$ between receiver and eavesdropper is required as opposed to $0.2/\lambda$ when using the channel-phase (2.5 times closer), which is also valid for a wider range of $0 \leq K \leq 6$. This result is expected as the channel-phase decorrelates faster across distance compared to the channel-amplitude and has higher entropy.

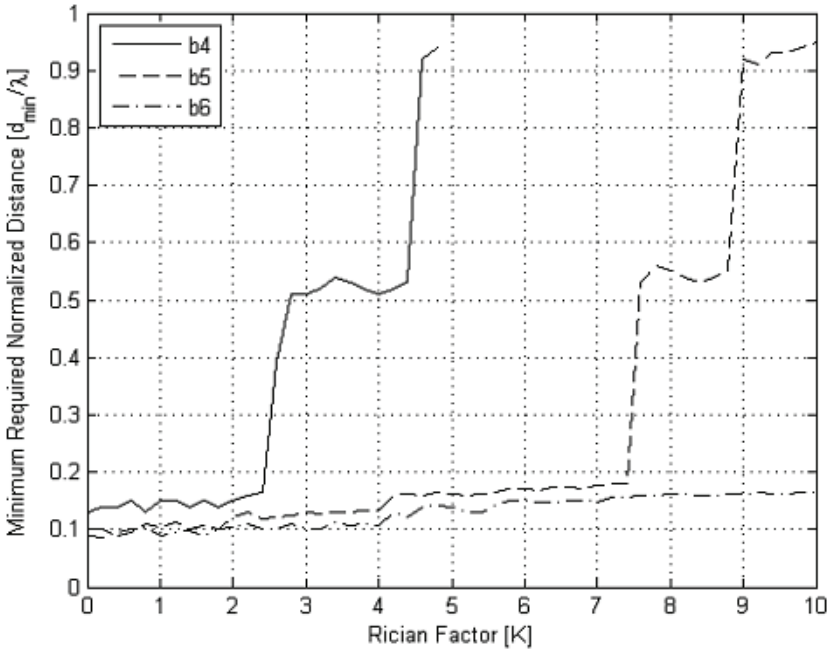

Fig. 6 – Minimum distance as function of the Rician factor for various quantized amplitude bits. Note the staircase threshold behavior for required minimum distance from Eve.

Fig. 7 depicts $R_{b_{max}}/f_D$ for which the generated bits are sufficiently random as a function of the quantization bit of the channel-amplitude for various values of K. The same trends are apparent with regard to quantization bit and K as observed for the channel-phase in Fig. 5. Note that the channel-amplitude provides lower key establishing rates compared to the channel-phases. For example, going back to the mobile environment corresponding to $f_D = 200Hz$, $K = 3$ and using MSB #6, establishing a 128 bit key would require a prohibitive amount of time as opposed to $64sec$ when using channel-phase. This is expected as the channel-phase decorrelates faster in time.

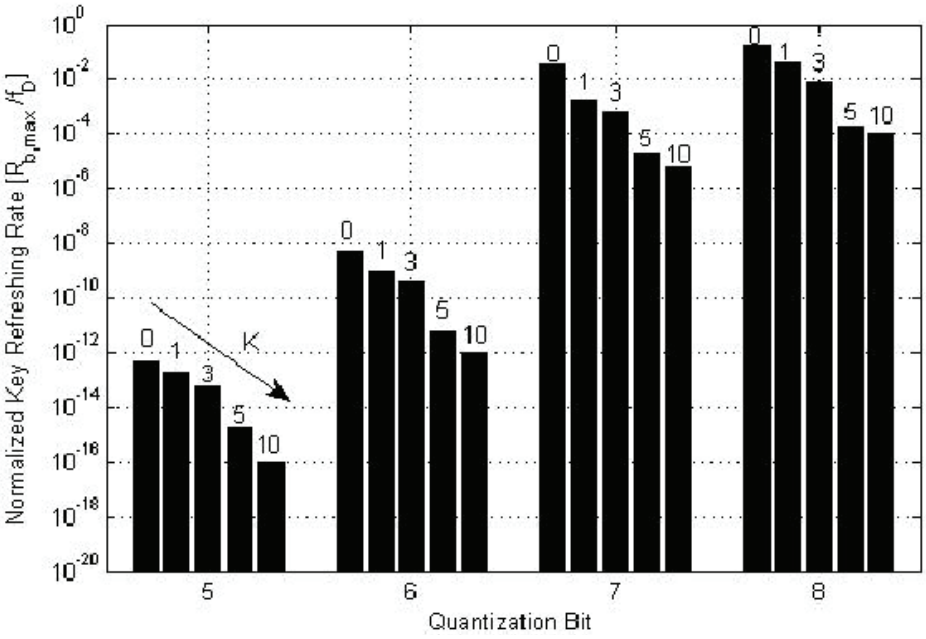

Fig. 7 – Maximum key rates as function of amplitude quantization for various Rician factors. Each bar column is determined by the minimum key rate obtained over all NIST tests. Note the reduction in key rate as the Rician factor is increased.

5.3 Imperfect Channel Reciprocity

Tab. 2 presents an assessment of the effect of imperfect channel reciprocity using the analysis presented in Section 2.3. As mentioned earlier, the timing offset between channel estimates at Alice and Bob is a system specific parameter. We set a timing offset of 1 msec corresponding to

the time it takes to transmit a short packet in a ZigBee transceiver operating in the ISM band of 2.4GHz. The time offset is the transmission time plus the signal propagation time which is negligible in comparison. The entries in Tab. 2 are the ratios of matching bits at Alice and Bob. Each ratio was calculated over a sample set of 10^4 channel estimates. It is evident that there are many entries reflecting near perfect agreement. For example, when $f_D = 5Hz$ and $K = 0$ less than a single bit is mismatched on average out of 1000 bits. This scenario models a pedestrian in a rich multipath environment. In general, we find that key agreement is decreased as f_D, K or quantization bit are increased. Recall that failure to agree on a secret key means Alice and Bob have to retry. The price would be a reduction in key establishing rate.

Tab. 2 – Bit matching probabilities for packet time of 1 msec for various Doppler shifts, Rician factors and quantized bit position. Each table entry lists probabilities for K=0,1,3,5,10 respectively. Many entries reflect near perfect agreement.

f_D [Hz]	b3	b4	b5	b6
5	0.9991, 0.9900, 0.9867, 0.9755, 0.9708	0.9978, 0.9811, 0.9679, 0.9547, 0.9421	0.9956, 0.9626, 0.9370, 0.9188, 0.8831	0.9910, 0.9266, 0.8825, 0.8495, 0.7834
20	0.994, 0.9683, 0.9451, 0.9047, 0.8761	0.9864, 0.9288, 0.8805, 0.8399, 0.7767	0.9759, 0.8582. 0.7732. 0.7282, 0.6333	0.9550, 0.7299, 0.6101, 0.5283, 0.4101
100	0.9385, 0.833, 0.7942, 0.621, 0.5606	0.8636, 0.6819, 0.5889, 0.4229, 0.3535	0.7391, 0.4982, 0.4022, 0.4042, 0.5307	0.5744, 0.4546, 0.5333, 0.4933, 0.5023

6. CONCLUSION

Symmetric key establishment using reciprocal quantization of channel estimates in wireless Rician fading channels was considered. Three aspects were addressed through generic analysis: impact of a proximity attack by a mobile eavesdropper, achievable key establishing rates and impact of imperfect reciprocity. Analysis made rigorous use of the NIST statistical test suite and a supporting lemma. The analysis was applied to channel-phase and channel-amplitude quantization and resulted in threshold conditions for maintaining secure key establishment. For

proximity attacks, the minimal required distance from the eavesdropper in order to maintain perfect secrecy during key establishment was evaluated as a function of the Rician factor and quantization bit. For key establishing rates, the maximal achievable rates were evaluated as a function of the Rician factor and quantization bit. In addition, the impact of imperfect reciprocity was assessed for practical scenarios. The analysis provided generic thresholds on required distances from an eavesdropper, achievable key refreshing rates and the impact of imperfect reciprocity for a wide variety of propagation scenarios. Results demonstrated that reciprocal quantization of Rician fading channel estimates can provide a secure key in reasonable time in practical scenarios. Channel-phase estimates were shown to provide better results than channel-amplitude estimates. Although the analysis focused on channel-phase and channel-amplitude it is readily applicable to quantization of other channel parameters.

REFERENCES

[1] J. Daemen, V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*, Springer-Verlag, 2002.

[2] R. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, 1978.

[3] M. Robshaw, O. Billet (Eds.), *New Stream Cipher Designs – the eSTREAM Finalists*, Springer, 2008.

[4] W. Diffie, M. Hellman, "New directions in cryptography," IEEE *Transactions on Information Theory*, vol.22, no.6, pp. 644- 654, Nov 1976.

[5] N. R. Potlapally, S. Ravi, A. Raghunath and N. K. Jha, "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols", *IEEE Transactions on Mobile Computing*, vol. 5, no. 2, pp. 128-143, Feb. 2006.

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

[7] D. K. Petraki, M. P. Anastasopoulus and S. Papavassiliou, "Secrecy Capacity for Satellite Networks under Rain Fading", *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 5, pp. 777-782, Sep. 2011.

[8] A. Mukherjee and A. L. Swindlehurst, “Robust Beamforming for Security in MIMO Wiretap Channels With Imperfect CSI”, *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 351-361, January 2011.

[9] P. K. Gopala, L. Lai and H. El Gamal, “On the Secrecy Capacity of Fading Channels”, *IEEE Transactions on Information Theory*, vol. 54, issue 10, pp. 4687-4698, Oct. 2008.

[10] F. He, H. Man and W. Wang, “Maximal Ratio Diversity Combining Enhanced Security”, *IEEE Communications Letters*, vol. 15, no. 5, pp. 509-511, March 2011.

[11] L. Dong, Z. Han, A. P. Petropulu, H. V. Poor, “Improving Wireless Physical Layer Security via Cooperating Relays”, *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875-1888, March 2010.

[12] M. Kobayashi, M. Debbah, and S. Shamai, “Secured Communication over Frequency-Selective Fading Channels: A Practical Vandermonde Precoding”, *Eurasip Journal on Wireless Communications & Networking – Special Issue on Physical Layer Security*, 2009.

[13] G. R. Tsouri and D. Wulich, “Securing OFDM over Wireless Time-Varying Channels using Sub-Carrier Over-Loading with Joint Signal Constellations”, *Eurasip Journal on Wireless Communications & Networking – Special Issue on Physical Layer Security*, 2009.

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

[15] H. Koorapaty, A. Hassan, and S. Chennakeshu, “Secure Information Transmission for Mobile Radio”, *IEEE Communication Letters*, vol. 4, issue 2, pp. 52-55, Feb. 2000.

[16] Y. Liang, H. V. Poor and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Transactions on Information Theory – Special Issue on Information Theoretic Security*, 54(6), pp. 2470-2492, Jun. 2008.

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

[18] C. Chen and M. A. Jensen, “Secret Key Establishment Using Temporally and Spatially Correlated Wireless Channel Coefficients”, *IEEE Transactions on Mobile Computing*, vol. 10, no. 2, pp. 205-215, Feb. 2011.

[19] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, “Information-theoretically secret key generation for fading wireless channels,” *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 240–254, Jun. 2010.

[20] G. R. Tsouri and J. Wilczewski, "Reliable Symmetric Key Generation for Body Area Networks using Wireless Physical Layer Security in the Presence of an On-Body Eavesdropper ", *4th International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL)*, Oct. 2011.

[21] J. W. Wallace, R. K. Sharma, “Automatic Secret Keys from Reciprocal MIMO Wireless Channels: Measurements and Analysis”, *IEEE Transactions on Information Forensics and Security*, Sept. 2010.

[22] S. Mathur, W. Trappe, N. Mandayan, C. Ye and A. Reznik, "Raio-Telepathy: Extracting Secret Key from an Unauthenticated Wireless Channel", *Proceedings of the 14th ACM international conference on Mobile computing and networking*, Sep. 2008.

[23] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments", *Proceedings of the 15th ACM annual international conference on Mobile computing and networking*, Sep. 2009.

[24] Neal Patwari, Jessica Croft, Suman Jana, Sneha Kumar Kasera, "High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17-30, Jan. 2010.

[25] Liang Xiao, Larry Greenstein, Narayan B. Mandayam and Wade Trappe, "Using the Physical Layer for Wireless Authentication in Time-Variant Channels," *IEEE Transactions on Wireless Communications*, vol. 7, No. 7, pp. 2571-2579, July 2008

[26] L. Xiao, L. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-selective Rayleigh channels," *IEEE Transactions on Wireless Communications*, vol. 8, No. 12, pp. 5948-5956, December 2009

[27] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Channel-based detection of Sybil attacks in wireless networks," *IEEE Transactions on Information Forensics & Security*, vol. 4, No. 3, pp. 492-503, September, 2009

[28] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam. "Proximate: proximity-based secure pairing using ambient wireless signals," in *Proceedings of the 9th international conference on Mobile systems, applications, and services*, pages 211–224. ACM, 2011.

[29] C. Xiao, Y.R. Zheng, N.C. Beaulieu, "Novel Sum-of-Sinusoids Simulation Models for Rayleigh and Rician Fading Channels," *IEEE Transactions on Wireless Communications*, vol. 5, pp. 3667-3679, Dec. 2006.

[30] A. Rukhin, J. Soto, J, Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," *NIST*, Aug. 2008.

[31] C. E. Shannon, "Communication theory of secrecy systems," *Bell Systems Technical Journal*, vol. 28, pp. 656–715, 1949.

[32] A. Goldsmith, *Wireless Communications*, University Press, 2005.

[33] G. D. Durgin, *Space-Time Wireless Channels*, Prentice Hall, 2002.

Bios:

Gill R. Tsouri received the B.Sc., M.Sc., and Ph.D. degrees in electrical and computer engineering from Ben-Gurion University, Beer-Sheva, Israel, in 2000, 2004, and 2008, respectively. From 1999 to 2003, he was with Yitran Communications, where he developed power-line communications. In 2008, he joined Rochester Institute of Technology, Rochester, NY, where he established the Communications Research Laboratory (CommLab). His current research interests include wireless physical layer security, body area networks, and biomedical signal processing.

David M. Wagner received the B.Sc. and M.Sc. degrees in electrical engineering from Rochester Institute of Technology, Rochester, NY, in 2010. Since then, he has been with the Advanced Development Group at Harris Corporation - RF Communications in Rochester, NY, where he works on embedded communication systems for software defined radios.