IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 8, 2021, accepted January 25, 2021, date of publication January 29, 2021, date of current version February 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3055561

On Quantization for Secret Key Generation From Wireless Channel Samples

MUHAMMAD ADIL, SHURJEEL WYNE, (Senior Member, IEEE), AND SYED JUNAID NAWAZ, (Senior Member, IEEE)
Department of Electrical and Computer Engineering, COMSATS University Islamabad (CUI), Islamabad 45550, Pakistan

Corresponding author: Muhammad Adil (adil34700@gmail.com)

The work of Muhammad Adil was supported by Higher Education Commission (HEC) Pakistan under Indigenous Ph.D. Fellowship Program.

ABSTRACT Physical layer security (PLS) techniques hold promise for augmenting secure communications in the 5th generation of mobile wireless networks. Secret key generation (SKG) is a PLS technique which exploits the wireless propagation channel's randomness to generate symmetric key bits for information encryption and decryption. This work proposes symmetric key generation based on non-uniform quantization of the received signal strength (RSS) samples of a Nakagami-m fading channel. The proposed strategy for non-uniform quantization for SKG aims to set quantization thresholds for maximal key randomness and high values of key generation rate (KGR) and key agreement probability (KAP). Finally, a framework is proposed to use single node RSS measurements, readily available in the literature, to generate RSS samples at the other link end. This framework facilitates the testing of new SKG algorithms that require simultaneous RSS measurements by the legitimate nodes, which are not readily available in the open literature. The effectiveness of the proposed SKG scheme is validated through Monte Carlo methods and the National Institute of Standards and Technology (NIST) test suite for assessing the randomness of the generated key sequence.

INDEX TERMS Nakagami-m, non-uniform quantization, PLS, secret key generation.

I. INTRODUCTION

The commercial deployment of the 5th generation (5G) of wireless networks has recently begun. Along with an evolution of existing communication technologies, 5G has revealed various new technology revolutions which extend the support to ultra-reliable-low-latency-communications (URLLC), massive-machine-type-communications (mMTC), and enhanced mobile broadband services [1]. In massively connected wireless networks of the future, the provision of security and privacy to the network users is expected to be one of the major challenges.

Information security for legitimately communicating nodes requires that they communicate successfully without leaking information to an unintended recipient. Wireless communications is inherently broadcast in nature, which makes the transmitted information susceptible to eavesdropping, i.e., a wireless device with a tuned receive and malicious intent may also receive and decode the information. Traditionally, information security has been ensured through computational security methods implemented at higher layers of the protocol stack. Such methods are based on public-key cryptography, wherein a public key is freely shared over the network to encrypt the information and a private key is retained only by the intended receiver to decrypt the encrypted message [2]. These traditional methods assume that the eavesdropping device has a limited computational ability and so it cannot decipher the secret information within reasonable time. These traditional methods also require a supporting infrastructure to distribute the secret encryption key between the legitimate users. However, with ever increasing computational capabilities that follow the Moore's law, and the advent of new technologies such as quantum computing, the assumption of the eavesdropper's limited computational ability is being challenged. Furthermore, in many emerging wireless communication scenarios such as vehicular communications and the internet-of-things [3]–[5], the infrastructure needed for secret key distribution among legitimate users does not scale with the number of users. To solve these problems, implementing information security at the physical layer emerges as a natural solution by exploiting the wireless channel's randomness for secret key generation (SKG) [6], [7].

The associate editor coordinating the review of this manuscript and approving it for publication was Jiayi Zhang.

A. PHYSICAL LAYER SECURITY: MOTIVATION AND BACKGROUND

The idea of augmenting secure communications through physical layer security (PLS) techniques has received significant attention in recent literature due to its practical significance [8]. Secure communication based on information-theoretic principles provides robust security such that the eavesdropper (Eve) cannot decipher the encrypted information, despite possessing unlimited computational power, unless it gains additional knowledge to break the encryption [3]. The fundamental idea underlying information-theoretic security is to secure the communication link at the physical layer by exploiting the difference in the random variations of the main and the eavesdropper channels. The information-theoretic security can be provided through key-less mechanisms [3], [9], [10] or using a secret key-based approach [3]. The key-less security techniques allow a theoretical analysis of the secrecy capacity, i.e., the maximum rate of secret communications. However, this method requires the restrictive condition of the availability of eavesdropper's (Eve) channel knowledge at the legitimate nodes [10]. On the other hand, the key-based PLS techniques do not require such knowledge. In the key-based information-theoretic model the legitimate nodes, traditionally refereed to as Alice and Bob, have access to a shared symmetric secret key generated from the main channel between them, which remains unknown to Eve. Recently, several algorithms exploiting the wireless channel for SKG are proposed for different communication scenarios such as body area networks (BANs) [11], internet of things (IoT) [3], vehicle-to-vehicle (V2V) communications [12], and energy harvesting systems [13]. In [14], space-time signal processing techniques were proposed for achieving secure communications in multiple-input multiple-output (MIMO) systems.

B. SECRET KEY GENERATION (SKG)

In recent years, there has been growing interest in extracting key bits from random wireless channels by exploiting channel reciprocity between the legitimate nodes. Specifically, in a time-division duplex (TDD) system, the wireless propagation channel between Alice and Bob is reciprocal, i.e., it is identical irrespective of whether the communication is from Alice-to-Bob or from Bob-to-Alice [15]. The secret key for encrypting the message needs to be derived from some random source. The random time-variability of the main channel between the two legitimate nodes can serve as a common source of randomness to extract identical keys, independently at both legitimate nodes. If the eavesdropper has a channel to the legitimate transmitter that is sufficiently decorrelated from the main channel, then Eve cannot extract the same key bits as Alice and Bob even if it has knowledge of the key generation algorithm used by Alice and Bob. For a sufficient time-rate of variations of the main channel, key bits can be extracted at an arbitrary rate. However, due to factors such as different hardware and noise conditions at the legitimate nodes, perfect reciprocity cannot be achieved practically, which makes the generation of symmetric key bits a challenging task.

The Nakagami-m fading model offers the advantage of modeling diverse fading conditions with an appropriate choice of its fading severity parameter m. For example, setting $m = 1$ represents Rayleigh fading conditions, i.e., both real and imaginary parts of the received complex signal envelope are zero-mean Gaussian distributed (there is no dominant multipath component). Theoretical bounds on secret key rate for single-input single-output (SISO) complex Gaussian channels were investigated in [16], [17]. The authors introduced secret key capacity as the supremum of the achievable SKG characterizing a theoretical upper bound on the secret key rate per channel sample. In [18], this concept was further investigated for MIMO channels. The rate of secret key extraction for practical SKG methods depends on the design of the algorithm and the underlying channel conditions.

Exploiting the main channel's reciprocity, some channel parameter such as its amplitude, power, or phase observed in the time, frequency, or angular domains can be used to generate symmetric secret keys independently at both legitimate nodes. In [19], the carrier frequency offset (CFO) in combination with the channel estimation of the orthogonal frequency division multiplexing (OFDM) carriers was used to generate key bits for message encryption. In [20], key bits were generated by exploiting the eigenvalue reciprocity between the channel covariance matrices of the uplink and the downlink. In [15], practical methods of key bit generation from RSS measurements were investigated and the trade-off between the key generation rate (KGR) and the key agreement probability (KAP) was analyzed. KAP is inverse interpretation of bit miss-match probability (BMP). In [16], the channel impulse response (CIR) was exploited for key bit generation and some measurement-based results were also reported. In [21], secret key bit generation in an indoor Gaussian channel was investigated. The authors showed that their proposed scheme was efficient in terms of randomness and BMP but the KGR was observed not to be very promising. In [22], the authors proposed a beamforming technique to artificially induce variations in the wireless channel for efficient key bit generation from the channel samples. In [23], an RSS-based algorithm for SKG was proposed for home devices employing a self-adaptive quantization strategy. In [24], the acknowledgment (ACK) and negative-acknowledgment (NACK) messages of the automatic repeat request (ARQ) protocol were exploited for SKG. In [25], phase shifting, and correction techniques were employed to increase the KGR and reduce BMP of the proposed SKG scheme. The work in [26] proposed SKG from the deep fading envelope of the wireless channel. A high improbability of deep fade mismatch between the legitimate users and strong independence of deep fades between the eavesdropper and the legitimate users were assumed.

From the foregoing survey, it is evident that several parameters of the wireless propagation channel can be exploited for key bit generation. However, each has its own merits and demerits. For example, acquisition of the full channel state information in the form of instantaneous channel impulse response is a computationally intensive task, which cannot be carried out by energy-constrained sensor nodes. Also, this information is not provided by most commercial network interface cards meaning that dedicated hardware must be designed for such key generation schemes. Furthermore, the channel phase information is susceptible to CFO, noise and receiver clock-drift, which complicates the reliable extraction of identical keys at the legitimate nodes. On the other hand, measurement of the wireless channel's RSS variations is a more straightforward task and this information is readily provided by most network interface cards. Therefore, RSS-based key generation schemes have been extensively studied in the literature. In [27], an RSS-based key bit generation scheme was proposed for on-body sensors deployed on two individuals, in an industrial environment. In [26], theoretical bounds on secret key extraction from the deep fades of the RSS were investigated. This key extraction algorithm generates secret keys with low BMP and the KGR is also low. An analytical expression for secret key capacity under Nakagami-m fading was derived in [28], where the authors also demonstrated the impact of non-reciprocity on the correlation of the uplink and downlink channels. The authors also proposed a two-level quantizer to validate their derivation. In [29], key bits were extracted from a time-static channel by randomizing the phase coefficients. In [30], the secret key capacity was investigated in the presence of multiple eavesdroppers.

The performance of SKG methods is conventionally measured by metrics such as KGR, i.e., number of key-bits generated per channel sample (with a high value desirable), BMP, i.e., probability of mismatch between key-bits generated at the legitimate nodes (with a small value desirable), and randomness of the generated key sequence (with maximal randomness desirable) as quantified by the NIST test suite [31]). These performance metrics largely depend on a number of parameters that include the considered quantization scheme and key extraction algorithm. The so-called level crossing algorithms form a widely used set of practical key generation algorithms [15], [32]. In [32], a SKG algorithm was proposed by quantizing the channel amplitude samples. The measured amplitude range was divided into multiple quantization intervals with the boundary between two intervals straddled by a guard strip. A sample excursion was then defined as a sequence of consecutive RSS samples lying within the same quantization interval. Then only the matching excursions at the legitimate nodes were used for SKG. More specifically, only the central sample of each pair of matching excursions was used for SKG. This algorithm extracts secret key bits with minimal BMP and desirable randomness properties but the KGR is rather low. In [15], an adaptive SKG algorithm (ASBG) was proposed, which has an increased KGR relative to those of the techniques proposed by [32] and [26]. However, this increase in KGR is achieved at the cost of increased BMP. In [33], a technique for reducing the BMP was proposed by exploiting Gray-codes and multilevel quantization. However, the proposed algorithm requires increased hardware complexity and is difficult to implement practically. In [27], a modification to the algorithm of [32] was proposed through the introduction of multi-dimensional mapping of samples. This modified algorithm offers a significant relative increase in the KGR without any loss in the BMP but the randomness properties of the extracted keys were not investigated.

C. QUANTIZATION SCHEMES FOR SKG

The essential steps for SKG comprise channel probing to collect the RSS samples, pre-processing (i.e., smoothing, filtering, etc. of the collected samples), sample quantization, sample encoding (assigning binary sequences to each quantization level), information reconciliation (e.g., coding to reduce BMP), and privacy amplification to minimize information leakage to the eavesdropper during the information reconciliation process. The legitimate nodes Alice/Bob communicate over the public channel to share algorithm related information for some of the aforementioned key generation steps such as information reconciliation. While this information exchange is not completely protected from the eavesdropper, the legitimate nodes can still extract a secret key at a positive rate. The legitimate nodes may incorporate channel estimation techniques prior to SKG to estimate algorithm parameters such as the channel correlation and the Nakagami shape parameter m [34]. Among the aforementioned steps, the quantization step is of prime significance in influencing the efficacy of SKG techniques. This subsection reviews some notable quantization strategies along with their characteristics and significance in terms of KGR, BMP, and randomness properties.

Quantizers used for SKG are broadly classified into *lossy quantizers* and *lossless quantizers* [15]. A lossless quantizer utilizes every channel sample for key bit generation with primary focus on KGR enhancement, while lossy quantizers leave some channel samples unutilized when generating the key bits with prime emphasis on enhancing the tradeoff between KGR and BMP. Both categories of quantizers can be employed with uniform quantization strategy (UQS) or non-uniform quantization strategy (NUQS). In UQS, the entire amplitude range of the channel samples is divided into uniformly spaced quantization intervals, while in NUQS, the sample range is divided into non-uniform quantization intervals. However, multilevel UQS is only suited for channel samples with uniform distribution where the probability of the RSS samples lying in any quantization interval is equal. Given the statistical knowledge of channel samples and the same number of quantization intervals, the NUQS can achieve a smaller quantization error than UQS on average to obtain a higher quantization signal-to-noise ratio (SNR).

In [35], a 2-level uniform quantization was proposed for secure communications for log-normal distributed channel samples. In [32], another 2-level uniform quantization-based method was proposed. In order to reduce the BMP, guard-strips were centered on each boundary between adjacent quantization intervals such that the samples falling in any guard strip were not considered for generation of secret key bits. Also, a constraint on the minimum excursion length was set for it to be considered for SKG. This key generation based on the UQS was observed to exhibit promising BMP and key randomness properties at the cost of reduced KGR. In [15], a similar 2-level uniform quantizer was proposed to improve the KGR by relaxing the strictness on the definition of excursion by incorporating an adaptive thresholding mechanism into the method of [32]. A gain in KGR was achieved at the cost of increased BMP and some reduction in the key randomness properties. In [27], another similar 2-level uniform quantizer was proposed as an extension of the method in [32] by introducing vector quantization. This aimed at increasing the KGR relative to that of the method of [32], while maintaining similar BMP performance and key randomness properties. However, the effectiveness of the method of [27] is restricted to channels that exhibit a sample distribution symmetric about its mean. In [36], UQS was used for SKG in IoT networks. In [37], a multi-level UQS was suggested as an extension of the 2-level UQS proposed in [32] with an aim to increase the KGR. In [38], a Lloyd–Max based quantizer coupled with RSS pre-processing based on a sliding window averaging approach was considered. The prime focus of this work was to reduce the BMP. In [39], a SKG scheme based on channel phase information was proposed and a two-layer secure quantizer design was suggested. Nevertheless, there exists a significant scope to investigate NUQS for SKG in channels exhibiting non-symmetric distribution of the measured samples used for SKG.

D. CONTRIBUTIONS AND ORGANIZATION

The proposed work builds on prior RSS-based SKG methods with consideration of the actual underlying probability density function (PDF) of the channel RSS samples in order to achieve a robust performance in terms of KGR, BMP, and key randomness properties. The proposed work considers Nakagami-m fading channel amplitude to derive analytical expressions for channel metrics relevant to the key extraction process. The choice of the Nakagami-m distribution for channel envelopes, and Gamma-distributed RSS, is motivated by the fact that several works have found the Nakagami-m distribution to accurately model the fading of wireless channel amplitude gain in various practical communication scenarios, refer [28], [40] and references therein. The main contributions of this work are listed as follows:

- A novel framework is proposed for generating dual-node correlated RSS measurements from single-node RSS measurements at one of the legitimate nodes, to facilitate testing of new SKG algorithms.
- A NUQS for SKG is proposed for Nakagami-m fading channels. Closed-form analytical expressions to determine the quantization-interval widths are derived to ensure an identical probability of occurrence of RSS samples in all quantization intervals. Moreover, analytical expression to determine the width of the guard-strips is also derived as a function of the correlation coefficient between the channel observations made at both the link-ends.
- Based on the proposed NUQS, an SKG algorithm is proposed which exhibits robust performance in terms of KGR, BMP (or KAP), and key randomness properties.
- A comprehensive comparative performance analysis of the proposed method is conducted in terms of KGR, BMP, and key randomness. Moreover, the effect of the RSS correlation is also investigated to develop more insight into the proposed SKG algorithm.

Table 1 presents a brief summary of some notable RSS-based SKG schemes and also shows the proposed work in that context.

TABLE 1. Summary of recent work on wireless channel-based SKG.

Research Publication and Year	Channel Model	Channel Parameter	Quantization	Approach
[22], 2005	Measurement Based	RSS	2-Level UQS	Measurement
[26], 2007	Rayleigh	CIR	2-Level UQS	Analytical
[16], 2010	Rayleigh	CIR	Multi-Level UQS	Analytical, Measurement
[15], 2014	Measurement Based	RSS	Multi-Level UQS	Measurement
[27], 2017	Measurement Based	RSS	2-Level UQS	Measurement
[38], 2019	Measurement Based	RSS	2-Level UQS	Measurement
[39], 2019	Simulation Based	Phase	Multi-Level UQS	Analytical
Proposed Work	**Nakagami-m**	**RSS**	**Multi -Level NUQS**	**Analytical**

This work is organised as follows. In Section I, the physical layer security paradigm and secret key extraction from wireless channel samples is introduced. Section II describes the considered system model and proposes a technique for generating correlated RSS samples from single-node RSS measurements to emulate dual node measurements for testing new SKG techniques. Section III presents the proposed analytical framework for non-uniform quantization of RSS for effective SKG. Section IV describes the algorithmic details of SKG from the wireless channel variations and describes the key aspects of the proposed SKG scheme. Section V evaluates the performance of the proposed quantization strategy in comparison with other SKG algorithms proposed in the literature. Finally, Section VI concludes this work.

II. SYSTEM MODEL

We consider a secure communication scenario in which Alice and Bob are two legitimate nodes that want to communicate in the presence of a passive eavesdropper node Eve, refer Fig. 1. The envelope of the main channel from Alice-to-Bob (A2B) is denoted h_{ab}, whereas h_{ba} denotes the envelope

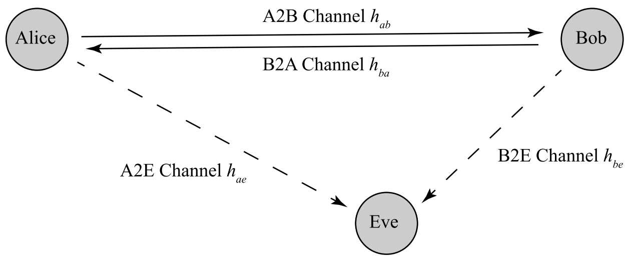


FIGURE 1. **System model.**

of the reciprocal channel from Bob-to-Alice (B2A). The eavesdropping channels from Alice-to-Eve (A2E) and from Bob-to-Eve (B2E) are denoted as h_{ae} and h_{be}, respectively. All coefficients h_{ij} $ij \in (ab, ba, ae, be)$ are assumed to be Nakagami-m fading. Alice and Bob aim to exploit the random channel's small-scale RSS variations to generate encryption keys for secure communication. The collected channel samples are normalized, prior to secret key extraction, to remove distance-dependent pathloss and large-scale-fading effects. Eve is considered to be at a sufficient spatial separation from Alice and Bob to experience independent fading [41], [42].[1]

Each cycle for collecting RSS samples begins with Bob transmitting a probe signal to Alice, who stores the measured RSS values. Then Alice transmits a probe signal to Bob who stores his measured RSS values. Each cycle must be completed within one channel coherence time interval T_c so that essentially the same channel is measured. Multiple RSS collection cycles are repeated until the desired number of secret key bits is generated. Although h_{ba} and h_{ab} are reciprocal channels in theory, their measurements by Alice and Bob, respectively, differ due to practical limitations such as simplex transceivers, hardware tolerances, and noise [15]. In the open literature there is a scarcity of data-sets that include simultaneous RSS measurements by two nodes of their common channel. Also, the few data-sets that are available comprise only a limited number of measurement samples [15]. This coupled with the measurement complexity of collecting multiple RSS sample pairs, each within the coherence time of the time-varying channel between two nodes, hinders the testing of novel key extraction algorithms. This issue is addressed in the following section where we propose a novel framework to use available RSS measurements at one link-end to generate RSS samples for the other link-end.

A. FRAMEWORK FOR DUAL-NODE RSS DATA SET GENERATION

Without loss of generality assume that h_{ba} is the true channel estimate while h_{ab} is its correlated noisy version. Then h_{ab} may be related with h_{ba} through a Gauss Markov model expressed as [43]

$$h_{ab} = \hat{\rho} h_{ba} + \sqrt{1 - \hat{\rho}^2}\varepsilon, \tag{1}$$

where $\hat{\rho} \in [0, 1]$ is the correlation coefficient between h_{ab} and h_{ba}, and $\varepsilon \sim \mathcal{N}(0, 1)$ represents the Gaussian-distributed channel-independent measurement error at Bob. Then the signal received at Bob can be written as

$$y_{ab} = \sqrt{P_T} h_{ab} d^{-\alpha/2} x + n_{ab}, \tag{2}$$

where x is the transmitted symbol with unit mean-squared value, P_T is the transmit power identically at Alice and Bob, d is the separation distance between Alice and Bob, α is the path-loss exponent, and $n_{ab} \sim \mathcal{N}(0, \sigma^2)$ represents the Gaussian-distributed thermal noise at Bob. The signal received at Alice can then be expressed as [44]

$$y_{ba} = \sqrt{P_T} h_{ba} d^{-\alpha/2} x + n_{ba}, \tag{3}$$

where $n_{ba} \sim \mathcal{N}(0, \sigma^2)$ represents the Gaussian-distributed thermal noise at Alice. It follows that the received SNR at Bob can be written as

$$\gamma_{ab} = \frac{P_T |h_{ab}|^2 d^{-\alpha}}{\sigma^2}, \tag{4}$$

and the received SNR at Alice can be expressed as

$$\gamma_{ba} = \frac{P_T |h_{ba}|^2 d^{-\alpha}}{\sigma^2}. \tag{5}$$

Note that for a fixed noise variance, the SNR variations are equivalent to variations of the absolute-squared channel amplitude, i.e., the RSS variations. The PDF of the Nakagami-m distributed channel envelopes h_{ij} can be expressed as [45]

$$p(h_{ij}) = \frac{2m^m h_{ij}^{2m-1}}{\Omega^m \Gamma(m)} e^{-\frac{m h_{ij}^2}{\Omega}}, \tag{6}$$

where $m \in [1/2, \infty)$ is the Nakagami fading parameter, $\Omega = E[h_{ij}^2]$, and $\Gamma(.)$ is the gamma function [46]. Then the squared envelope, which corresponds to the RSS, follows a gamma distribution expressed as [45]

$$p(\gamma_{ij}) = \frac{m^m \gamma_{ij}^{m-1}}{\overline{\gamma}_{ij}^m \Gamma(m)} e^{-\frac{m\gamma_{ij}}{\overline{\gamma}_{ij}}}, \tag{7}$$

where $\overline{\gamma}_{ij}$ is the mean SNR. The joint distribution of the correlated variables γ_{ab} and γ_{ba} can be expressed as [47]

$$p(\gamma_{ab}, \gamma_{ba}) = \frac{e^{-\frac{mA}{(1-\rho)}} (\frac{B}{\rho})^{\frac{m-1}{2}} I_{m-1}\left(\frac{2m\sqrt{B\rho}}{(1-\rho)}\right)}{m^{-(m+1)} \overline{\gamma}_{ab} \overline{\gamma}_{ba} (1-\rho) \Gamma(m)}, \tag{8}$$

where $A = \left(\frac{\gamma_{ab}}{\overline{\gamma}_{ab}} + \frac{\gamma_{ba}}{\overline{\gamma}_{ba}}\right)$, $B = \left(\frac{\gamma_{ab}\gamma_{ba}}{\overline{\gamma}_{ab}\overline{\gamma}_{ba}}\right)$, $\rho \in [0, 1]$ is the correlation coefficient between γ_{ab} and γ_{ba} (γ_{ab} and γ_{ba} correspond to the amplitude squares of h_{ab} and h_{ba} respectively), and $I_{m-1}(.)$ is the modified Bessel function of order $m - 1$. Furthermore, $\overline{\gamma}_{ab} = \overline{\gamma}_{ba} = \overline{\gamma}$ is the mean RSS value at Alice and Bob as the main channel's statistics remain unchanged when measured at either legitimate node. Finally, dividing (8)

[1] Based on the angular-spread of the arriving multipath, the small-scale fading can decorrelate on the order of a carrier wavelength distance. Therefore, the assumption of decorrelated eavesdropper channels can be justified for large as well as for small spatial separation of the eavesdropper.

by the marginal PDF of γ_{ba} gives the conditional PDF of γ_{ab} expressed as

$$p(\gamma_{ab}|\gamma_{ba}) = \frac{m\rho(\frac{\overline{\gamma}_{ba}}{\gamma_{ba}})^m e^{\frac{m(\overline{\gamma}_{ba}\gamma_{ab}+\overline{\gamma}_{ab}\rho\gamma_{ba})}{\overline{\gamma}_{ab}\overline{\gamma}_{ba}(\rho-1)}} I_{m-1}\left(-\frac{2m\sqrt{B\rho}}{\rho-1}\right)}{\left(\frac{B}{\rho}\right)^{-\frac{m+1}{2}}(1-\rho)\gamma_{ab}}. \tag{9}$$

Then by integrating (9) and after some mathematical manipulation, the conditional cumulative distribution function (CDF) is obtained as,

$$F(\gamma_{ab}|\gamma_{ba}) = 1 - Q_m\left(\sqrt{\frac{2m\rho\gamma_{ba}}{\overline{\gamma}_{ba}(1-\rho)}}, \sqrt{\frac{2m\gamma_{ab}}{\overline{\gamma}_{ab}(1-\rho)}}\right), \tag{10}$$

where $Q_m(.,.)$ is the Marcum-Q function of order m [48]. The RSS samples (γ_{ba} or γ_{ab}) observed at Alice/Bob node are recorded in $\mathcal{V}^{\text{Alice/Bob}}$, where the total number of samples are N. Finally, given the RSS values for Alice, the correlated RSS samples for Bob can be generated by using (10) and the inverse CDF method. This procedure is summarized in Algorithm 1. The operator ← represents assignment operation, function rand(1) represents generating a random number from uniform distribution in the range [0, 1], and the function solve(., .) represents solving the expression (equality) provided as the first input argument for the variable provided as the second input argument.

Algorithm 1 Proposed Algorithm to Generate RSS at Bob

```
Input: $\mathcal{V}^{\text{Alice}}, m, \rho, \overline{\gamma}$
Output: $\mathcal{V}^{\text{Bob}}$
for $i = 1$ to $N$ do
    $r \leftarrow \text{rand}(1)$
    $\mathcal{V}^{\text{Bob}}(i) \leftarrow \text{solve}\left(r = 1 - Q_m\left(\sqrt{\frac{2m\rho\ \mathcal{V}^{\text{Bob}}(i)}{\overline{\gamma}(1-\rho)}}, \sqrt{\frac{2m\hat{\gamma}_{ab}}{\overline{\gamma}(1-\rho)}}\right), \hat{\gamma}_{ab}\right)$
end for
```

III. PROPOSED NON UNIFORM QUANTIZATION STRATEGY (NUQS)

Optimal quantizer design is of central importance to secret key extraction with desirable characteristics such as maximal randomness, minimal bit mismatch probability, and maximal KGR. Most quantizer designs in the literature focus on improving KGR or BMP [15], [27] but a lesser emphasis has been given to analyzing the randomness characteristics of the considered SKG techniques. In this section a quantizer design is proposed that aims at maximizing the randomness of the generated key sequence, in addition to achieving minimal BMP and maximal KGR. Conventionally, the mean of the channel samples, collected at the legitimate nodes, is used for quantizer design with the quantization range uniformly distributed around the sample mean [15], [27]. However, if the distribution of the channel samples is known then a more robust quantizer can be designed that will alleviate the need to collect sufficient number of channel samples and run-time calculation of quantizer design parameters to begin the SKG process.

For the considered scenario of independent and quasi-static Nakagami-m fading links, the RSS (squared amplitude) values follow the Gamma distribution [45]. To increase the uncertainty of the secret keys extracted at the legitimate nodes, the quantizer must have two characteristics: (i) the RSS sample should equally-likely fall in any of the M quantization intervals, and (ii) the algorithm should also be symmetrically applied across all quantization intervals, essentially generating an equal proportion of 0's and 1's (RSS samples or excursions has to be treated in a uniform manner in all the M quantization intervals so that equal proportions of 0's and 1's are generated). We propose an M-level non uniform quantization strategy (M-NUQS) for the Gamma distributed RSS to satisfy the first requirement stated above. Fig. 2 provides an overview of the M-NUQS scheme. The PDF of the Gamma distributed RSS values is shown at the left edge of the figure, whereas the RSS profile at a legitimate node (say Alice) is shown on the right. The PDF support is divided into M non-uniform quantization intervals (gray horizontal strips) with widths d_{qi}, $i \in 1, \ldots, M$ such that there is a uniform probability of the RSS falling in each interval, i.e., equal area regions enclosed by the Gamma PDF. Also shown in the same figure, there are $M-1$ guard strips (blue horizontal strips) of width z each that are centered on one of the $M-1$ quantization boundaries. The i^{th} guard strip is bounded by a lower threshold q_i^-, and an upper threshold q_i^+, $i \in 1, \cdots, M-1$.

Given M, z, and the RSS PDF, the proposed M-NUQS scheme places the $M-1$ guard strips in the RSS range such that the resulting M quantization intervals have equal areas under the PDF. This task is equivalent to finding for the bounding thresholds of i^{th} guard strip ($i \in 1, \cdots, M-1$), i.e., determining the lower and upper thresholds q_i^- and q_i^+, respectively.

The area under the PDF curve for each quantization interval can be computed by integrating the PDF over the limits of each quantization interval (i.e., determined by bounding thresholds of guard strips q_i^+ and q_i^-). Since upper threshold of each guard strip can be written in terms of its lower bounding threshold given strip width z as

$$q_i^+ = q_i^- + z, \quad 1 \leq i \leq M-1, \tag{11}$$

the limits of integration operator applied for each quantization interval can be written in terms of z and lower boundary thresholds of guard strips (bounding the quantization interval). By observing Fig. 2, the 1st quantization interval has limits from $q_0^+ = 0$ to q_1^-, the 2nd quantization interval has limits $q_1^+ = q_1^- + z$ to q_2^-, and so on until the Mth quantization interval having limits $q_{M-1}^+ = q_{M-1}^- + z$ and ∞. This leaves the M areas as functions of z and $M-1$ lower thresholds as

$$\int_{q_0^+}^{q_1^-} p(\gamma)d\gamma = \int_{q_1^-+z}^{q_2^-} p(\gamma)d\gamma = \cdots = \int_{q_{M-1}^-+z}^{\infty} p(\gamma)d\gamma. \tag{12}$$

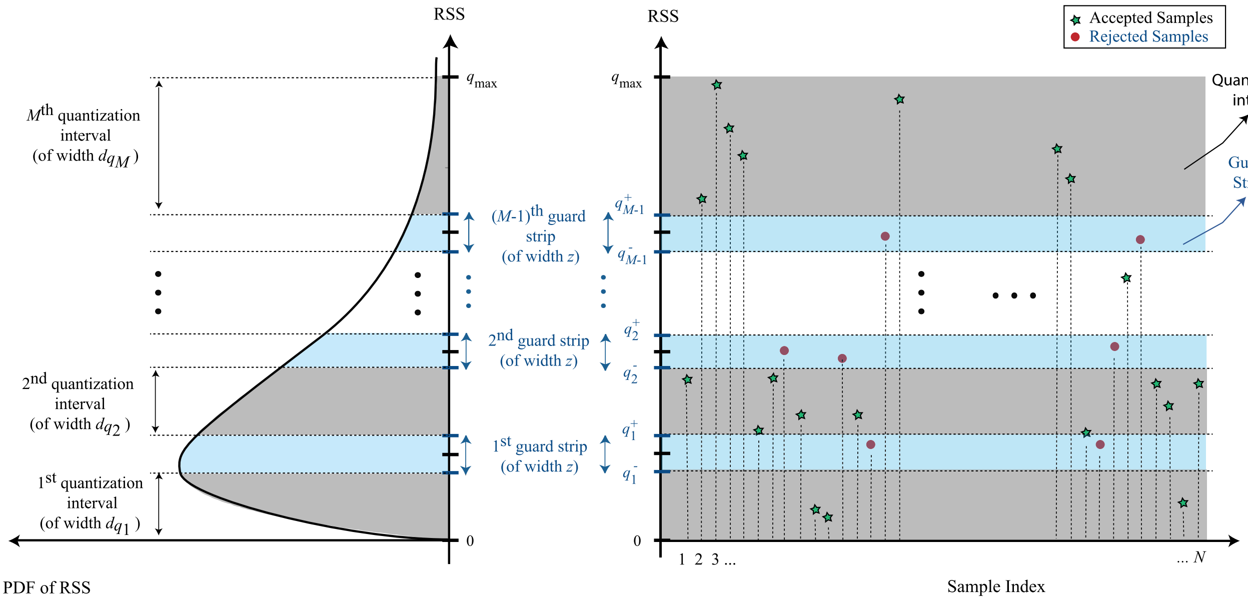

RSS
$q_{\max}$
M^{th} quantization interval (of width dq_M)
$(M\text{-}1)^{\text{th}}$ guard strip (of width z)
2^{nd} guard strip (of width z)
1^{st} guard strip (of width z)
2^{nd} quantization interval (of width dq_2)
1^{st} quantization interval (of width dq_1)
0
PDF of RSS
RSS
$q_{\max}$
$q^+_{M\text{-}1}$
$q^-_{M\text{-}1}$
q_2^+
q_2^-
q_1^+
q_1^-
0
Accepted Samples
Rejected Samples
Quantization interval
Guard Strip
1 2 3 ...
... N
Sample Index

FIGURE 2. RSS profile and its Gamma PDF used by proposed M-NUQS. The nonuniform widths $dq_1, \cdots, dq_M$ of M quantization intervals are determined from the PDF of RSS, whereas the identical width z of $M-1$ guard strips is determined from the MSE between RSS observations at the legitimate nodes.

Since there are a total of M regions in the PDF each representing equal area, therefore, after equating the expressions of any of the two regions and solving the relationship can determine the corresponding bounding thresholds. By equating 2 expressions out of M total expressions, a total of ${}^{M}C_2$ combinations can be formed, i.e., ${}^{M}C_2 = \frac{M!}{2!(M-2)!}$ equations. Given the value of z, the $M-1$ lower boundary thresholds (excluding q_0^+ being known, as equal to 0) can be computed by manipulating $M-1$ equations. The corresponding upper thresholds can then be computed by using the relationship provided in (11).

An RSS sample falling inside any guard strip is rejected and the probability of the rejection event can be expressed as

$$\mathcal{P}^{s^M}_{Rej.} = \sum_{i=1}^{M-1} \int_{q_i^-}^{q_i^+} p(\gamma)d\gamma. \tag{13}$$

On the other hand, an RSS sample falling inside one of the M quantization intervals is accepted for SKG and the probability of sample acceptance event can be expressed as

$$\mathcal{P}^{s^M}_{Acp.} = \sum_{i=0}^{M-1} \int_{q_i^+}^{q_{i+1}^-} p(\gamma)d\gamma. \tag{14}$$

It is pertinent to mention that $\mathcal{P}^{s^M}_{Rej.} + \mathcal{P}^{s^M}_{Acp.} = 1$.

Considering 2-NUQS as a toy example for the considered Nakagami-m fading scenario, we start by solving

$$\int_{q_0^+}^{q_1^-} p(\gamma)d\gamma = \int_{q_1^-+z}^{\infty} p(\gamma)d\gamma, \tag{15}$$

and after some further manipulations obtain the relation

$$\Gamma(m) - \Gamma\left(m, \frac{mq_1^-}{\overline{\gamma}}\right) = \Gamma\left(m, \frac{m(q_1^- + z)}{\overline{\gamma}}\right), \tag{16}$$

where $\Gamma(x, y)$ is the upper incomplete gamma function [46]. Eq. (16) can be solved numerically for the computation of the lower threshold q_1^-. The upper threshold is then simply calculated as

$$q_1^+ = q_1^- + z. \tag{17}$$

Thus given M, z and the Nakagami-m PDF, the desired lower threshold q_1^- and upper threshold q_1^+ for 2-NUQS can be obtained. The sample rejection probability for the 2-NUQS case can be given as be given by (13),

$$\mathcal{P}^{s^2}_{Rej.} = \int_{q_1^-}^{q_1^+} p(\gamma)d\gamma. \tag{18}$$

The guard strip's width z has a direct influence on the KGR and BMP of the extracted keys. In the preceding discussion z was treated as a given. We now propose a strategy to determine z as a function of the mean squared error (MSE) between the RSS sequences measured at the legitimate nodes. Specifically, z can be computed as

$$z = k\delta = kE[(\gamma_{ab} - \gamma_{ba})^2], \tag{19}$$

where δ is the MSE between the correlated RSS of Alice and Bob, and the parameter k is the constant of proportionality for setting the guard strips width proportional to the MSE and ensuring appropriate mapping of the MSE range over the RSS range. For example, for the worst scenario represented by maximum possible MSE of $\delta_{\max}$, the width of $M-1$ guard strips (differentiating M quantization intervals) together must not exceed the entire RSS range (i.e., $q_{\max} - 0 = q_{\max}$, as illustrated in Fig. 2). This consideration suggests the range of constant scaling parameter as, $0 \leq k \leq q_{\max}/\left(\delta_{\max}(M-1)\right)$. Also, this range can be determined in terms of σ as, $0 \leq k \leq q_{\max}/\left(2\sigma^2(M-1)\right)$.

By expanding the expectation term and using the properties of expectation operation [49], (19) reduces to

$$z = k(E[\gamma_{ab}^2] + E[\gamma_{ba}^2] - 2E[\gamma_{ab}\gamma_{ba}]), \tag{20}$$

and using the fact that the RSS distribution is same at the legitimate nodes we obtain

$$z = k(2E[\gamma_{ab}^2] - 2E[\gamma_{ab}\gamma_{ba}]). \tag{21}$$

Then using $E[XY] = \text{cov}(X, Y) + E[X]E[Y]$ as in [49], where the function cov(., .) represents the covariance of two input random variables, into (21) and applying mathematical simplification operations, we get

$$z = k\left\{2E[\gamma_{ab}^2] - 2(\text{cov}(\gamma_{ab}, \gamma_{ba}) + E[\gamma_{ab}]E[\gamma_{ba}])\right\}. \tag{22}$$

Since $\text{cov}(X, Y) = \rho\sigma_X\sigma_Y$ [49], where ρ is correlation coefficient between X and Y and σ_X, σ_Y are the respective standard deviations, we further obtain

$$z = k\left\{2E[\gamma_{ab}^2] - 2(\rho\sigma_{\gamma_{ab}}\sigma_{\gamma_{ba}} + E[\gamma_{ab}]E[\gamma_{ba}])\right\}. \tag{23}$$

Finally, using the fact that $E[\gamma_{ab}] = E[\gamma_{ba}] = \overline{\gamma}$ and $\sigma_{\gamma_{ab}} = \sigma_{\gamma_{ba}} = \sigma$, z can be expressed as

$$z = 2k(\overline{\gamma^2} - \overline{\gamma}^2 - \rho\sigma^2) = 2k\sigma^2(1-\rho). \tag{24}$$

By choosing z according to the above relationship, Alice and Bob can take advantage of a larger number of RSS samples while maintaining minimal BMP.

IV. SECRET KEY GENERATION (SKG) AND EVALUATION PARAMETERS UNDER THE PROPOSED *M*-NUQS

Given that the legitimate nodes have designed their M-level quantizers according to the proposed M-NUQS scheme, the next step is to apply a suitable algorithm to generate secret keys from the measured RSS samples. The Algorithm 2 provided herein describes the SKG steps of [32] after incorporating the proposed M-NUQS scheme.

Starting with defining the basic parameters, the algorithm consists of measurement/generation of samples, NUQS, SKG, and key reconciliation steps. A sample excursion length is defined as the number of consecutive RSS samples that fall within a certain quantization interval. L represents the minimum excursion length to be considered for SKG, i.e., only the excursions with length $\geq L$ are considered for the SKG. The probability that an L-samples excursion falls in different quantization intervals when observed at Alice and Bob reduces with an increase in the excursion length L, i.e., the chances of two consecutive samples falling in different quantization intervals at two different ends is less compared to a single-sample falling in different quantization intervals. An illustration of the basic flow of primary steps involved in the SKG algorithm is provided in Fig. 3, where a minimum excursion length of $L = 3$ is considered.

For each admissible excursion, the index of the central sample can be calculated as,

$$l_j^{\text{Alice/Bob}} = \lceil \frac{i_j^{\text{end}} + i_j^{\text{start}}}{2} \rceil, \tag{25}$$

Algorithm 2 Mathur-NUQS: An Example Secret Key Generation Algorithm Combined With Proposed NUQS

Parameters Definition:

- Define M, L, k, and z.
- Compute/estimate m and ρ.

Measure/Generate Samples:

- Measure RSS profile at Alice/Bob (i.e., $\mathcal{V}^{\text{Alice/Bob}}$), or generate the RSS profile by exploiting the proposed correlation based method in Algorithm 1.

***M*-NUQS:**

- Compute the bounding thresholds of guard strips and quantization intervals (i.e., q_i^- and q_i^+) by using (11) and (12).
- Assign unique binary codes to each quantization interval (i.e., Gray coding).

SKG (i.e., $\mathcal{H}(.)$):

- Compute excursions with minimum length L at Alice/Bob from $\mathcal{V}^{\text{Alice/Bob}}$.
- Determine the central sample index $l_j^{\text{Alice/Bob}}$ of each excursion (j), as defined by (25).
- Record the indices in $\Omega^{\text{Alice/Bob}}$, as defined in (26).
- **Indices Exchange and Key Reconciliation:**
  - Alice sends Ω^{Alice} to Bob.
  - Bob compares Ω^{Alice} with Ω^{Bob} and determines the common set of indices in Υ.
  - Bob sends Υ to Alice.
  - Alice reconciles generated secret key by using Υ.
- Draw sample-values for the indices reconciled in Υ from $\mathcal{V}^{\text{Alice/Bob}}$.
- Map the samples (Υ) to the predefined (non-uniform) quantization intervals.
- Generate secret key bits by concatenating the Gray codes associated to each interval, in $\mathcal{K}_{\text{bits}}^{\text{Alice/Bob}}$, as defined in (27).

where i_j^{start} and i_j^{end} represent the index of first and last sample in j^{th} excursion, respectively, and the operator $\lceil . \rceil$ represents the mapping of input real number to the least integer value greater than or equal to the input real number (i.e., ceiling operation). The indices of the samples positioned at the central location of each considered excursion (j) can be recorded independently at Alice and Bob. Concatenating these indices in a vector, it can be represented as

$$\Omega^{\text{Alice/Bob}} = \left[l_1^{\text{Alice/Bob}}, l_2^{\text{Alice/Bob}}, \cdots, l_J^{\text{Alice/Bob}}\right]^{\text{T}}, \tag{26}$$

where J represents the total number of determined excursions (i.e., $\Omega^{Alice/Bob}$ is a $J \times 1$ dimensional vector). The number of excursions (J) observed at at Alice and Bob may be different before the conduction of information exchange/reconciliation. Next, the sample values for the selected samples can be recorded and transformed to a binary

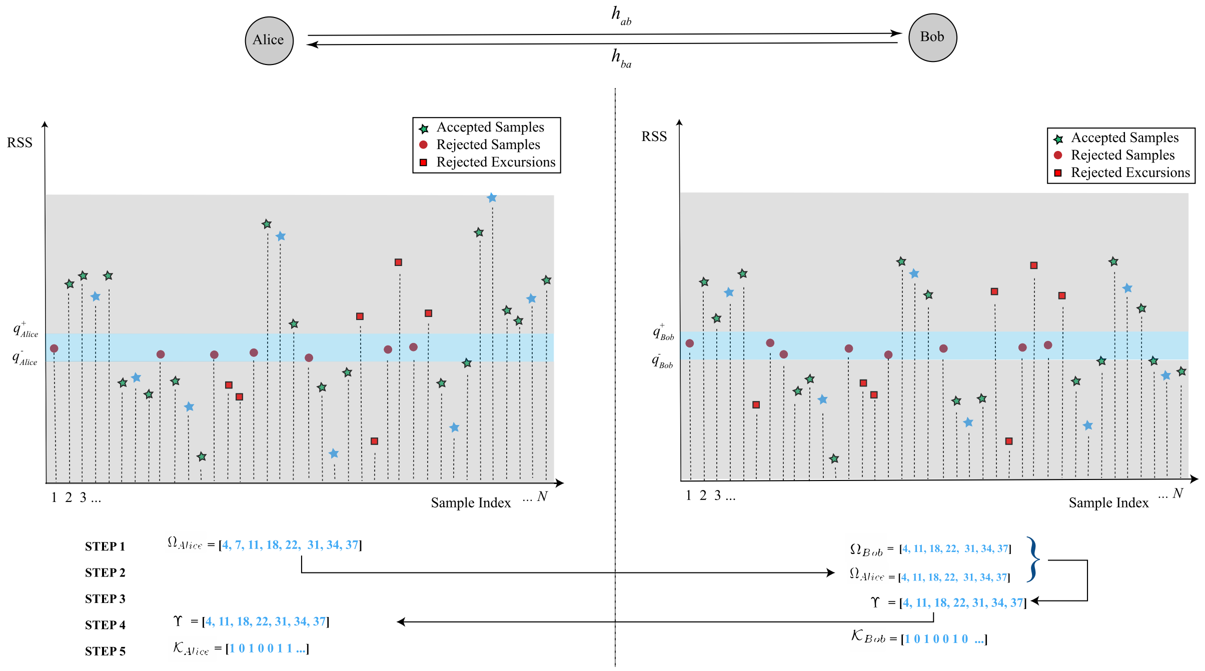

Alice
h_{ab}
h_{ba}
Bob
RSS
Accepted Samples
Rejected Samples
Rejected Excursions
q^{+}_{Alice}
q^{-}_{Alice}
1 2 3 ...
Sample Index
... N
RSS
Accepted Samples
Rejected Samples
Rejected Excursions
q^{+}_{Bob}
q^{-}_{Bob}
1 2 3 ...
Sample Index
... N
STEP 1
STEP 2
STEP 3
STEP 4
STEP 5
Ω_{Alice} = [4, 7, 11, 18, 22, 31, 34, 37]
Ω_{Bob} = [4, 11, 18, 22, 31, 34, 37]
Ω_{Alice} = [4, 11, 18, 22, 31, 34, 37]
Υ = [4, 11, 18, 22, 31, 34, 37]
Υ = [4, 11, 18, 22, 31, 34, 37]
$\mathcal{K}_{Alice}$ = [1 0 1 0 0 1 1 ...]
$\mathcal{K}_{Bob}$ = [1 0 1 0 0 1 0 ...]

FIGURE 3. **Proposed *M*-NUQS scheme with *M* = 2. The samples with green and blue star-shaped markers are the accepted samples, red circle-shaped markers are the rejected samples (falling in guard strip), and red square-shaped markers are the samples exhibiting insufficient excursion length (i.e, excursion length < *L*). From the set of accepted samples, the blue-colored star-shaped markers represent the central samples of admissible excursions, which are utilized for SKG.**

stream, as

$$\mathcal{K}^{\text{Alice/Bob}}_{\text{bits}} = \mathcal{H}\left(\Omega^{\text{Alice/Bob}}\right), \tag{27}$$

where the function $\mathcal{H}(.)$ represents the SKG operation from the provided list of indices as the input argument. Through exchanging the indices of excursions between the legitimate nodes (instead of exchanging sample values to maintain secrecy) which are determined independently at both the nodes, a reconciled common set of excursions is agreed (i.e., Υ). Next, the SKG follows drawing of sample-values for the provided reconciled indices-set Υ from the RSS profile ($\mathcal{V}^{\text{Alice/Bob}}$) and then transforming them to a binary stream through their mapping according to the predefined binary codes associated with the quantization intervals. In this work, Gray coding is used for assigning binary codes to each quantization interval. Finally, secret key bits at Alice and Bob can be generated as represented by $\mathcal{K}^{\text{Alice/Bob}}_{\text{bits}}$.

Two notable SKG algorithms proposed in [32] and [27] combined with the proposed M-NUQS are named as, Mathur-NUQS and Li-NUQS, respectively. The performance of the herein considered SKG schemes is quantified on the basis of KGR ($\mathcal{K}_{\mathcal{G}}$), key agreement probability (KAP) ($\mathcal{K}_{\mathcal{A}}$), and key randomness properties. The definition of these quantifiers is discussed as follows.

If the generated secret key bits and total available RSS samples are represented by $\mathcal{N}_k$ and $\mathcal{N}_c$, then the KGR (i.e., bit generated per sample) is defined by,

$$\mathcal{K}_{\mathcal{G}} = \frac{\mathcal{N}_k}{\mathcal{N}_c}. \tag{28}$$

If the number of different bits generated by Alice and Bob is represented by $\mathcal{N}_m$, the BMP can be expressed as follows,

$$\mathcal{P} = \frac{\mathcal{N}_m}{\mathcal{N}_k}. \tag{29}$$

The Key Agreement Probability $\mathcal{K}_{\mathcal{A}}$ can be defined as a function of BMP, as

$$\mathcal{K}_{\mathcal{A}} = 1 - \mathcal{P}. \tag{30}$$

The randomness properties of the generated secret key can be quantified by employing NIST test suite, which consists of 16 different tests. For each test, there is an associated null hypothesis H_0 which asserts that the observed sequence is random and an alternate hypothesis H_a which asserts that the sequence is not random. From these statistics, the value of P parameter is computed which represents the probability that a perfectly random source has generated a sequence less random than the given criteria, and this parameter summarizes the strength of the evidence against null hypothesis [31]. Each test evaluates the key randomness properties as represented by the P-value, where a high P-value represents high key randomness properties. The NIST tests considered in this study are frequency test, block frequency test, runs test, longest run of ones test, cumulative sum forward test, cumulative sum reversed test, Maurer test, discrete Fourier transform (spectral) test, and approximate entropy test.

V. SIMULATION RESULTS

This section is dedicated to a discussion of simulation results obtained after applying the proposed NUQS scheme to the

RSS samples. We consider a simulation scenario where Alice and Bob are the legitimate nodes. Assuming the channel between the legitimate node is Nakagami-m fading channel, 10^5 channel samples are generated. Different channel conditions are studied in terms of setting different values for Nakagami shape parameter m for the legitimate node (say Alice). The RSS variations are induced by the absolute square of these channel envelopes. We assume that the legitimate nodes have prior available knowledge of m, ρ, and L. Alice calculates the thresholds for $M-1$ guard-strips by numerically solving (12) and (11). Using the algorithm given in Algorithm 1, a correlated RSS data-set for Bob is generated by setting a certain values of ρ. Similar to Alice, Bob can determine the guard-strips by solving (12) and (11), where Alice and Bob share the accurate information of m, ρ, and L. Alice and Bob compute guard strip thresholds independently, where their thresholds might be slightly different as their RSS values are not same but only correlated. Once Alice and Bob have the RSS data set generated or probed, and determined the guard-strips thresholds, they independently apply Algorithm 2 to generate secret key bits. Both the UQS and NUQS schemes are applied to the same data sets for conducting a comparative study.

In order to highlight the effectiveness of the proposed NUQS, a thorough comparative analysis with different UQS schemes is conducted. Even though the proposed scheme is build on same basic flow of steps suggested in [27], it demonstrates subtle differences showing a profound impact on the characteristics of the generated key bits. First, using Algorithm 1, correlated channel samples are generated for the other side of the channel from the available samples of one side. Second, using the proposed analytical framework, the threshold values for quantization and guard strips are determined. Third, using Algorithm 2, secret key at both sides of the channel (between legitimate nodes) is extracted. Finally, performance tradeoff between KGR, KAP/BMP, and randomness characteristics of the generated keys is thoroughly analyzed. One of the striking characteristic of the proposed SKG method is the promising randomness properties of the generated key. As there is no single recognized quantifier of gauging all the aspects of a key's randomness properties, therefore, multiple tests suggested in the NIST test suite are performed for the considered SKG methods and the value of P is determined. Since the prime focus of the proposed NUQS is to enhance the randomness properties of the generated keys, we start the discussion by conducting a comparative analysis of the proposed NUQS with some notable UQSs in the existing literature in terms of investigating the impact of different important parameters over the value of P.

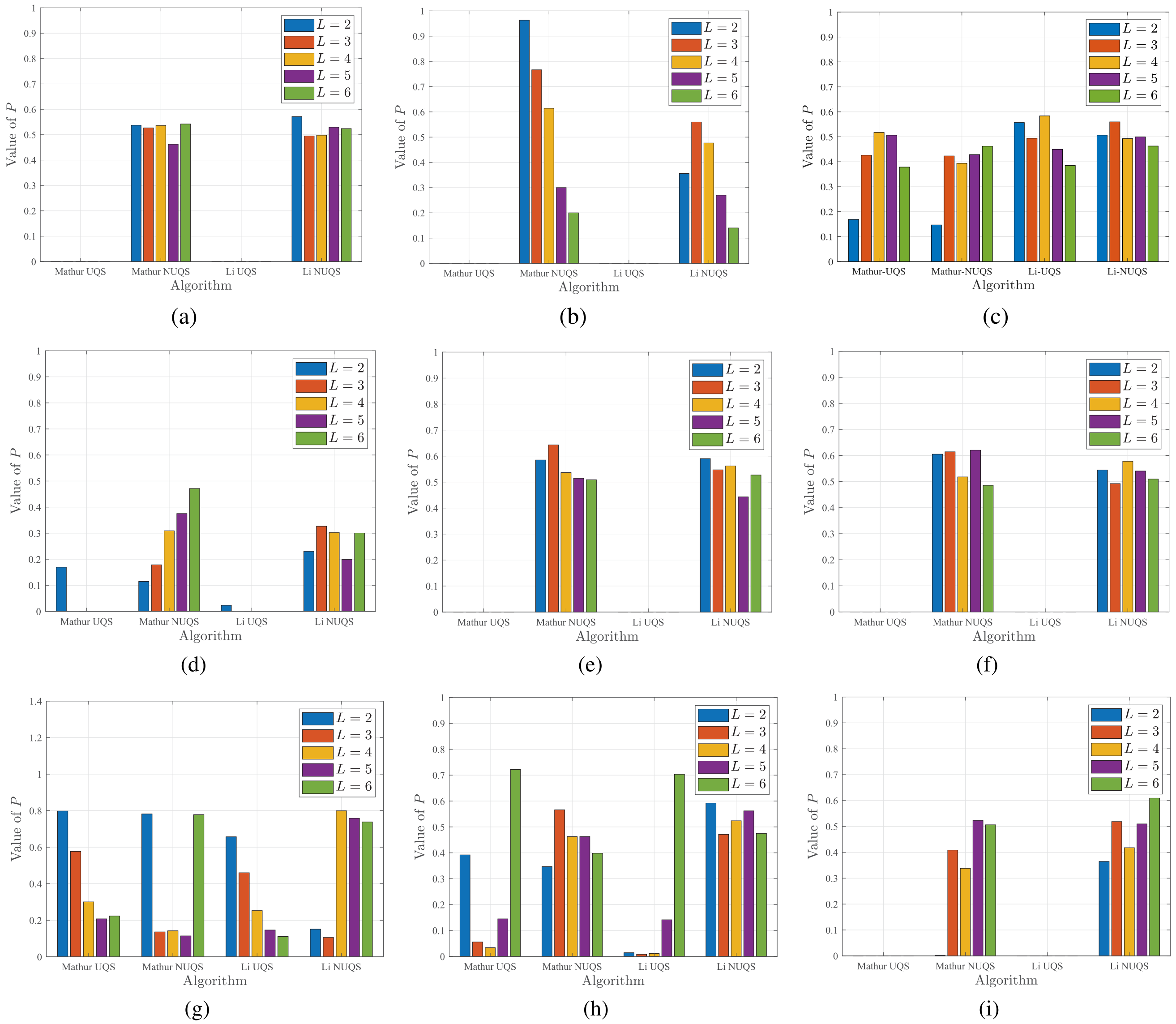
Fig. 4 (a) to (i) display the obtained results of 9 different tests suggested under the NIST framework for studying the randomness properties of the generated keys. Two different notable key generation algorithms with UQS and the proposed NUQS are compared. The results are shown for four different methods namely Mathur-UQS [32], proposed Mathur-NUQS (i.e., extensions of SKG algorithm by Mathur *et al.* in [32] by employing the proposed NUQS), Li-UQS [27], and Li-NUQS (i.e., extension of SKG method proposed by Li *et al.* in [27] by employing the proposed NUQS). From the results it can be observed that by employing NUQS, promising randomness properties can be achieved.

Fig. 4 (a) depicts the results of the frequency test. The frequency test counts the number of 1's and 0's in a given sequence and the calculated corresponding value of P indicates the degree of randomness of the sequence, where $P \geq 0.01$ is usually regarded as the case exhibiting reasonable key randomness properties. For a sequence to be truly random, passing this first test (i.e., frequency test) is critical and a prerequisite for all the subsequent tests [31]. The quantized and encoded samples based key extraction methods are likely to pass the frequency test if the quantization and guard strips' threshold values are set such that an equal number of considered samples (i.e., after rejecting the samples falling in guard strips) fall under each quantization interval. Moreover, the binary codes associated to each quantization interval must also ensure an even distribution of 1's and 0's. From the results obtained for the frequency test, it is clearly evident that NUQS outperforms UQS for both the considered SKG algorithms for all excursion lengths (i.e., tested for up to excursion length of $L = 6$). This is because when considering a UQS for a non-uniformly distributed sample-set, the number of samples falling in each quantization interval may be significantly different. The observed significantly large value of P for the proposed NUQS compared to the conventional UQS is because of the fact that under Nakagami-m fading conditions the RSS samples follow a non-uniform distribution, i.e., Gamma distribution. It is also pertinent to mention that the demonstrated gain in randomness proprieties of the generated keys is achieved without any loss in KGR, as shown in Fig. 6.

Fig. 4 (b) indicates the obtained results for block frequency test. Block frequency test is defined by performing frequency tests independently over each sub-block of a large sequence. The results suggest that UQS for both the considered SKG algorithms (i.e., Mathur-UQS and Li-UQS) exhibit the value of P as equal to 0, which indicates that UQS for Gamma distributed RSS samples fails the block frequency test. Whereas, in contrast, the NUQS for both the considered algorithms (i.e., Mathur-NUQS and Li-NUQS) exhibit promising results.

Another notable test for investigating the randomness properties of sequences is the runs test. A run is defined as an occurrence of consecutive 0's or 1's in a sequence. In 4 (c), it can be observed that all the considered schemes exhibit a comparable performance for the runs test.

The longest run of ones test checks whether the given sequence contains the longest run of 1's as per a given random sequence of similar size. Fig. 4 (d) shows the results of longest run of ones test. UQS for both the algorithms (i.e., Mathur-UQS and Li-UQS) fail in this test for most of the settings of excursion length L, except the marginal

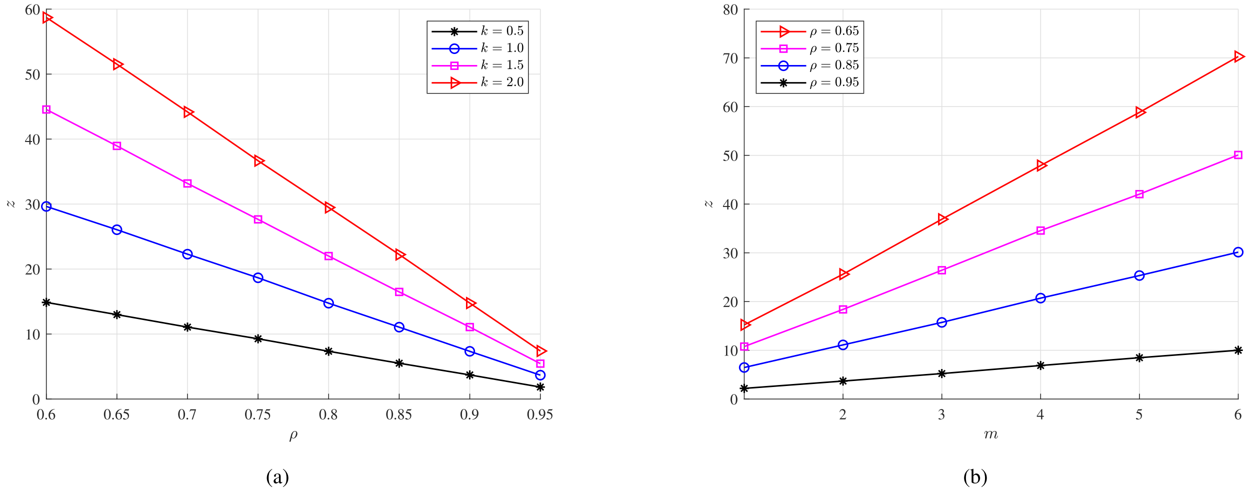


(a) (b) (c) (d) (e) (f) (g) (h) (i)

FIGURE 4. **Performance comparison of NUQS and UQS for producing desirable randomness characteristics in generated secret keys. The randomness tests used from NIST test suite include: (a) Frequency Test. (b) Block Frequency Test. (c) Run Test. (d) Longest Run of Ones. (e) Cumulative Sum Forward. (f) Cumulative Sum Reverse. (g) Maurer Test. (h) Discrete Fourier Transform Test. and (i) Approximate Entropy Test.**

qualification for L =1 (a single sample is defined as an excursion). The proposed NUQS (for both, Mathur-NUQS and Li-NUQS) passes this test for all values of L upto 6, and exhibit good randomness characteristics. The results of forward and reverse commutative sum test are shown in Fig. 4 (e) and Fig. 4 (f). Since the count of 0's and 1's is again important, the proposed NUQS for both the algorithms (i.e., Mathur-NUQS and Li-NUQS) pass both the tests. However, the UQS with both the algorithms (i.e., Mathur-UQS and Li-UQS) fail to qualify these tests. In cumulative sum forward test, for $L = 1$, Mathur-UQS has comparable performance with Mathur-NUQS; while for all the other values of L, Mathur-NUQS performs superior than Mathur-UQS. Moreover, the performance of Li-NUQS is observed superior than Li-UQS for all settings of L.

For the Maurer and discrete fourier transform (spectral) tests, the proposed NUQS is seen to exhibit comparable or superior performance than that by UQS, see Fig. 4 (g) and 4 (h). This establishes that the proposed NUQS scheme suggests an optimal placements of quantization and guard strips bounding thresholds and assure good randomness properties of the generated keys. Fig. 4 (i) shows the comparative results for approximate entropy test. The approximate entropy test is of high significance in measuring the randomness properties of a given sequence. It can be examined from Fig. 4 (h) that both the algorithms for UQS (i.e., Mathur-UQS and Li-UQS) fail in this test for all the settings of excursion length L. Whereas, the proposed NUQS for both the algorithms (i.e., Mathur-NUQS and Li-NUQS) are observed to pass the test with a significantly high value



(a)

(b)

FIGURE 5. Impact of system parameters on guard strip width, z. (a) Effect of correlation coefficient for $m = 2$, (b) Effect of Nakagami fading severity parameter for $k = 1$.

of P. This again establishes that the proposed NUQS ensures superior randomness properties of the generated secret key.

Along with the high significance of key good randomness behaviour, the key generation and agreement rate (i.e., $\mathcal{K}_\mathcal{G}$ and $\mathcal{K}_\mathcal{A}$, respectively) are also equally important. In general, $\mathcal{K}_\mathcal{G}$ is a function of guard strip interval (i.e., z) and it is highly influenced by the quantization strategy. The KAP ($\mathcal{K}_\mathcal{A}$) is a function of both guard strip interval z and excursion length L. Moreover, another important parameter to be investigated is the correlation coefficient, ρ, for the two way channels between the legitimate nodes. In Fig. 5 (a), the impact of variations in ρ on MSE and correspondingly on guard strip interval z for different values of k is plotted. In setting the guard strip interval z proportional to MSE (function of ρ), the parameter k represents the constant of proportionality. With an increase in the value of ρ, the guard strip interval z deceases almost linearly and the slope of the line is determined by k. Also in Fig. 5 (a), it can be observed that for a small values of ρ, the resultant value of z is very large, which corresponds to the scenarios where a large number of samples fall in the guard strip (thus rejected). For reciprocal channels, however, the value of ρ is practically expected to be high, and thus the corresponding guard strip interval will be generally a small interval. In Fig. 5 (b), the behaviour of MSE against an increase in the value of Nakagami shape parameter m is plotted. Interestingly, as the value of m increases, the value of z increases almost linearly, however, the slope of the line is influenced by ρ – higher the value of ρ the smaller is the slope of the line for z along m.

The KGR $\mathcal{K}_\mathcal{G}$ is a function of the parameters k, ρ, L, and m. For studying the KGR performance of the proposed NUQS, we consider the practical case of reciprocal channel exhibiting a high value of correlation coefficient. Fig. 6 depicts the behaviour of $\mathcal{K}_\mathcal{G}$ against different values of excursion length L for the other important parameters set as, $\rho = 0.95$, $m = 2$, and $k = 1$. With an increase in L, the KGR $\mathcal{K}_\mathcal{G}$ reduce for both the algorithms with NUQS and UQS. As the value of L increases (e.g., approaches to 6), $\mathcal{K}_\mathcal{G}$ reduces (i.e., approaches to 0), which implies that the occurrence of 6 consecutive samples lying within a certain quantization interval is highly unlikely considering the behaviour of random variations in the channel statistics. Another important point to be noted, as also mentioned before, is that the KGR performance achieved by UQS is maintained by NUQS, while the key randomness properties demonstrated by NUQS are significantly superior than those demonstrated by UQS.

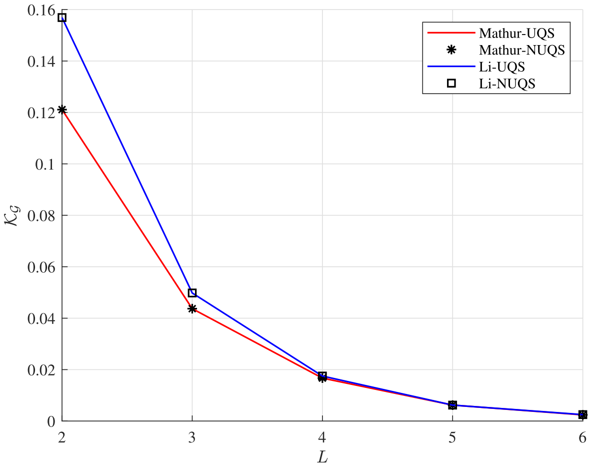
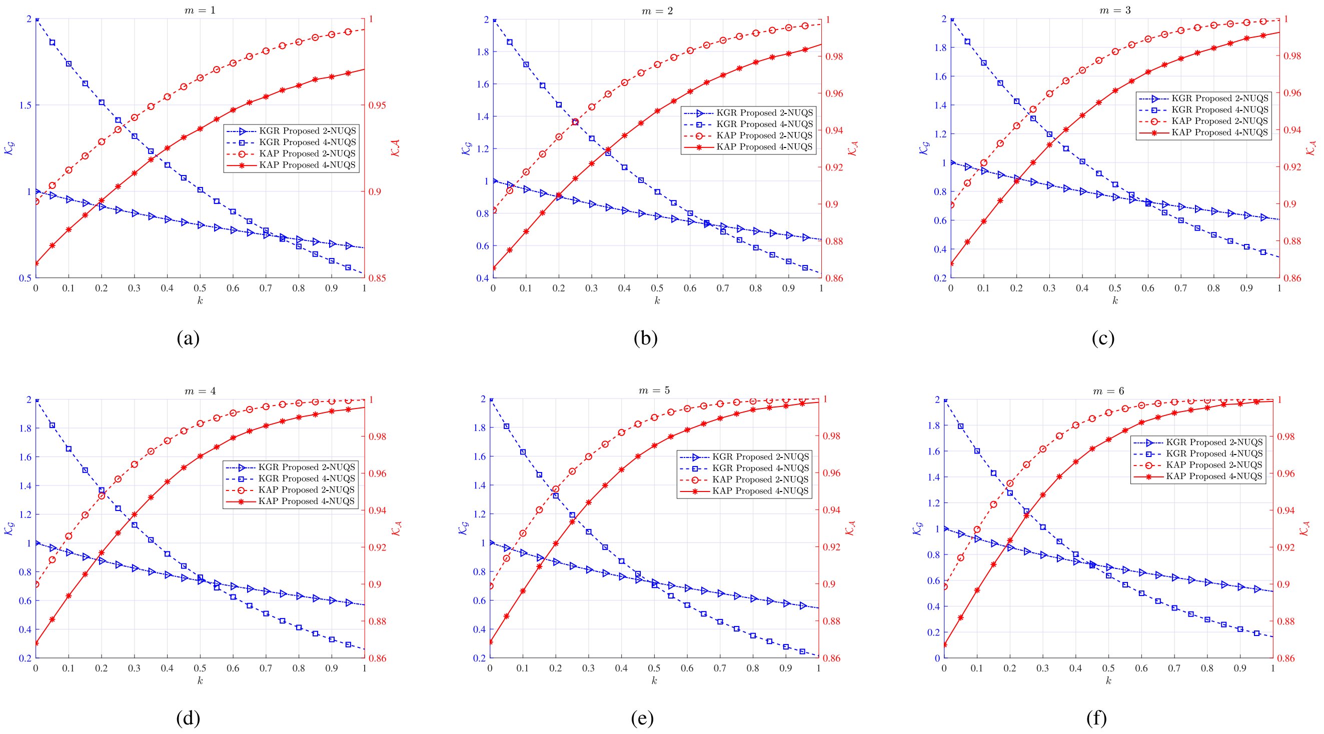


FIGURE 6. Effect of excursion length L on key generation rate of UQS and NUQS. Other parameter values are $M = 2$, $\rho = 0.95$, $m = 1$, and $k = 1$.

Fig. 7 (a)–(f) show the impact of variations in k on $\mathcal{K}_\mathcal{G}$ and $\mathcal{K}_\mathcal{A}$ for 2- and 4-level NUQS, named as 2-NUQS and 4-NUQS, respectively. Moreover, the impact of different changes in channel conditions, as represented by Nakagami shape parameter m, is also demonstrated. For $k = 0$, representing the case of no guard strips, the rate of key generation is high (ideal) as no samples are being rejected, while the



(a) (b) (c)

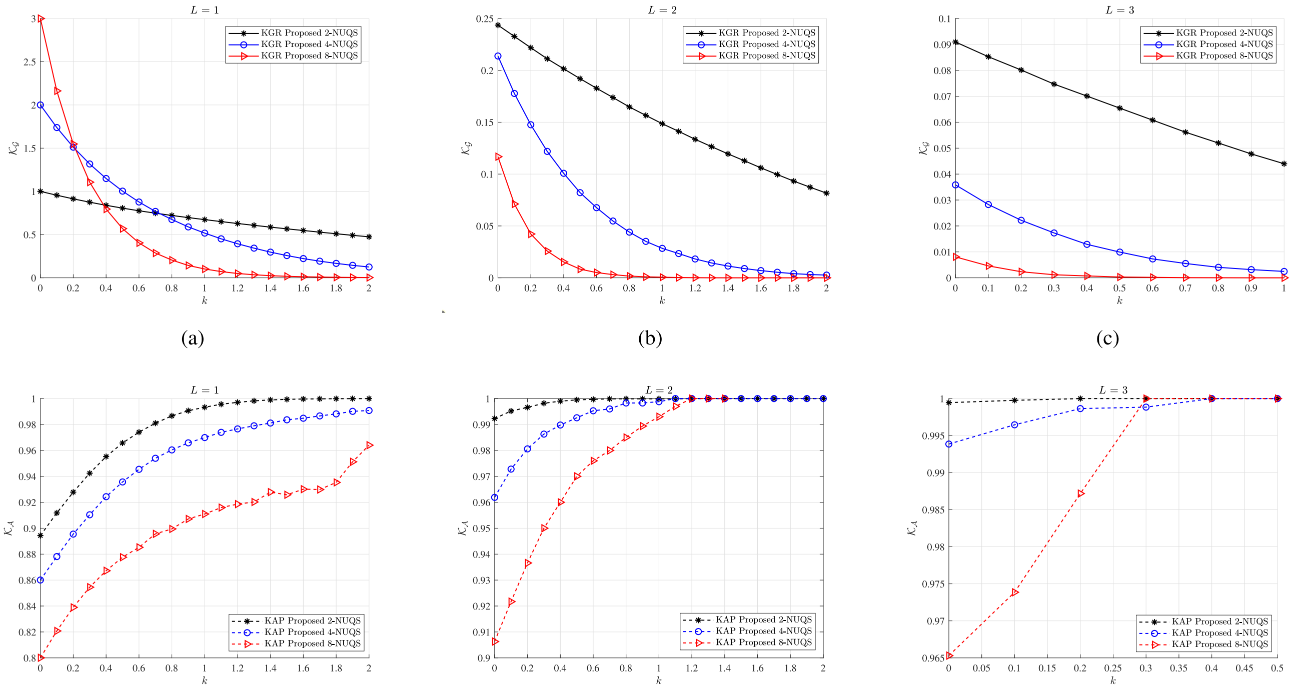
(d) (e) (f)

FIGURE 7. Impact of Nakagami fading severity parameter *m* on key generation rate and key agreement probability of NUQS. (a) *m* = 1. (b) *m* = 2. (c) *m* = 3. (d) *m* = 4. (e) *m* = 5. (f) *m* = 6. Other parameter values are $\rho = 0.9$, and $L = 1$.

rate of key agreement is low (worst) as the impact of difference in the channels (observed at two sides of the link) is not being countered. The behaviour of decrease in $\mathcal{K}_{\mathcal{G}}$ and increase in $\mathcal{K}_{\mathcal{A}}$ along with an increase in k is observed as different for different quantization levels setting. Along with an increase in guard strip interval (influenced by an increase in k), the matching probability between the keys generated at both the link-ends can be enhanced while it employs a cost of decrease in KGR. This analysis endorses our proposal of setting the guard strips interval as proportional to the correlation (or MSE) between the channel observations made independently on both the link-ends.

From Fig. 7 (a)–(f), the performance trade off between KGR and KAP for NUQS of different quantization levels can also be analyzed. It can be observed that increasing the levels of quantization does not necessarily ensure an improvement in the rate of key generation. This is because the KGR is also a function of various other discussed parameters along with the number of quantization levels being considered, e.g., the nature of key extraction algorithm (excursion length), channel conditions, etc. Increasing the number of quantization levels allows the assignment of multiple bits per quantization level, which increases the KGR. However, on the other hand, increasing the number of quantization levels also increases the number of guard strips, which leads to more number of samples being rejected (falling in guard strip) and causes a decrease in KGR. Therefore, the best choice for the number of quantization levels to be considered depends on the performance trade off between KGR, KAP, and key randomness properties under certain noise and channel conditions. For investigating different channel conditions, by comparing the Fig. 7 (a)–(f), the impact of Nakagami shape parameter m on $\mathcal{K}_{\mathcal{G}}$ and $\mathcal{K}_{\mathcal{A}}$ can also be observed. The key matching performance improves with an increase in the value of m for high-level NUQS. This indicates that for channel conditions represented by small values of m, higher level quantization is not a suitable choice in terms of keys agreement performance.

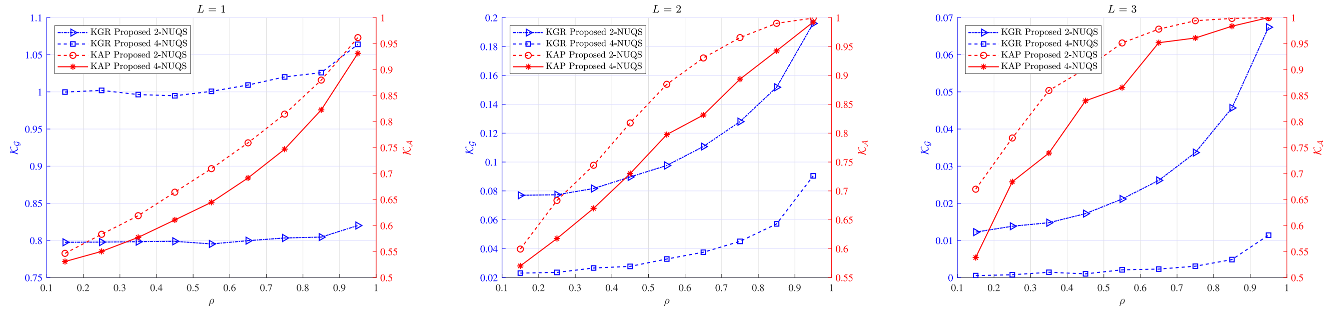
Excursion length is one of the prime influencing factors on KGR, KAP, and key randomness properties. The impact of change in excursion length L on $\mathcal{K}_{\mathcal{G}}$ and $\mathcal{K}_{\mathcal{A}}$ can be observed by comparing the Figures 8 (a) – (c) and Figures 8 (d) – (f), respectively. The results are shown for different settings of quantization intervals and guard strips. For large values of excursion length, the KGR is observed to decrease, where the rate of decrease is higher for multi-level quantization strategies compared to 2-level quantization strategy. This is because, in a rapidly varying RSS profile, it is less likely to have large number of consecutive samples (i.e., large valued excursion length) falling within a quantization interval. However, on the other hand, the increase in excursion length improves the key agreement rate. Furthermore, in Fig. 9 (a), (b), and (c), the impact of change in correlation coefficient ρ on $\mathcal{K}_{\mathcal{G}}$ and $\mathcal{K}_{\mathcal{A}}$ is shown for the excursion length of $L = 1$, 2, and 3, respectively. It is interesting to note that for $L = 1$, the $\mathcal{K}_{\mathcal{G}}$ for both 2-, 4-, and 8-level NUQS increase only marginally with an increase in ρ, whereas the plot of



(a) (b) (c)

(d) (e) (f)

FIGURE 8. Impact of excursion length L on the key generation rate of NUQS. (a) $L = 1$. (b) $L = 2$. (c) $L = 3$, and the key agreement probability of NUQS. (d) $L = 1$. (e) $L = 2$, and (f) $L = 3$. Other parameter values are $\rho = 0.95$, and $m = 1$.



(a) (b) (c)

FIGURE 9. Effect of correlation coefficient ρ on the key generation rate and key agreement probability of NUQS for different excursion lengths L. (a) $L = 1$. (b) $L = 2$. (c) $L = 3$. Other parameter values are $m = 1$ and $z = 1$.

$\mathcal{K}_\mathcal{A}$ is being drastically influenced. This is because that each sample is being considered an excursion and only factor that cause increase in $\mathcal{K}_\mathcal{G}$ is reduction in the number of rejected samples. The higher values of ρ represent the cases when the channel observation made at Alice and Bob are similar to each other and the significance of guard strip becomes marginal. However, the increase is KGR and KAP performance is more apparent for higher values of L. This indicates that setting a high value for L is more suitable for the scenarios when the value of correlation coefficient ρ is higher.

The combined effect of number of quantization levels M and excursion length L on both $\mathcal{K}_\mathcal{G}$ and $\mathcal{K}_\mathcal{A}$ is shown in Fig. 10. For excursion length of $L = 1$, i.e., each RSS sample is being utilized for key generation, $\mathcal{K}_\mathcal{G}$ is observed to increase with an increase in M over its entire range. However, for $L > 1$, the $\mathcal{K}_\mathcal{G}$ is observed to initially increases with an increase in M up to a certain point, and a converse behaviour beyond that point is observed. Despite an increase in the number of bits associated to each sample along with an increase in the quantization levels, the increase in the number of guard strips required for high level quantization schemes also reduce, which eventually cause the reduction in KGR beyond a certain point. Another contributing factor to this behaviour is the rapid random fluctuations encountered in the channel profile, which makes it is less likely for a longer excursion to hold in a high level quantization strategy.

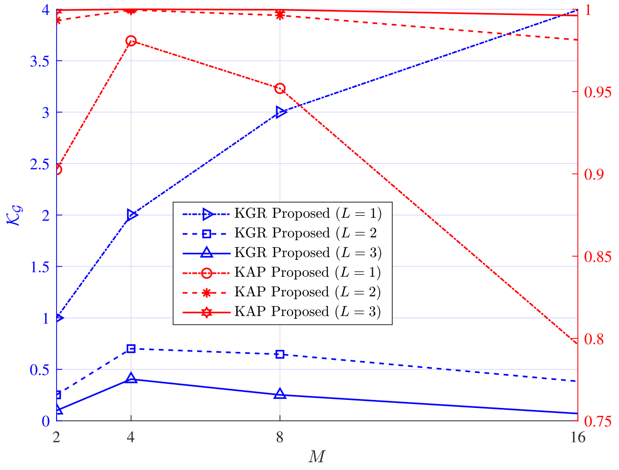


FIGURE 10. Effect of number of quantization intervals M on $\mathcal{K}_{\mathcal{G}}$ and $\mathcal{K}_{\mathcal{A}}$. Other parameter values are $m = 2$ and $\rho = 0.95$.

Novel analytical results often need to be compared with appropriate measurements or simulations to establish their validity. The unavailability of suitable data-sets in the open literature, which include simultaneous RSS measurements, necessitate the need for conducting such measurement campaigns to investigate the efficacy of new SKG algorithms. To this end, our proposed analytical framework for generation of RSS samples can also be used as a reference model.

VI. CONCLUSION

In this paper, first, a framework for generating correlated RSS samples for one link-end from the available samples observed at the other link-end of a reciprocal wireless channel has been proposed. Considering the practical limitations on the designing of measurement setups for simultaneously (or within a coherence time slot) sensing the channel samples at both link-ends, the proposed framework can assist in designing and testing of SKG algorithms as well as providing a reference for conducting such measurement campaigns in the future. Secondly, a multi-level non-uniform quantization strategy has been proposed for secret key generation under Nakagami-m fading conditions. Moreover, exploiting the proposed non-uniform quantization strategy, an extension of two notable level-crossing based key generation algorithms has been proposed, viz: Mahatur-NUQS and Li-NUQS. Comprehensive performance analysis of the proposed methods has been conducted, where the effect of different fading conditions, noise conditions, quantization levels setting, and other parameters (transmitters/receiver side) on the KGR, KAP, and key randomness properties (quantified through NIST tests) have been evaluated. A thorough comparative analysis of the proposed non-uniform quantization strategy with the conventional uniform quantization strategy for secret key generation with both the considered algorithms has also been conducted. It has been established that the proposed non-uniform strategy provides superior key randomness properties than those provided by conventional uniform quantization strategy with the assurance of maintaining the same KGR and KAP. Moreover, various other useful conclusions have also been drawn; e.g., the optimal choice of quantization levels and values of other notable parameters to be made under given fading and noise conditions as defined by the Nakagami shape parameter and correlation coefficient (between two-way reciprocal channels), respectively, etc.

REFERENCES

[1] S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary, and M. Asaduzzaman, "Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future," *IEEE Access*, vol. 7, pp. 46317–46350, 2019.

[2] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. New York, NY, USA: Springer-Verlag, 2010.

[3] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the Internet of Things: Authentication and key generation," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 92–98, Oct. 2019.

[4] P. Hao and X. Wang, "Integrating PHY security into NDN-IoT networks by exploiting MEC: Authentication efficiency, robustness, and accuracy enhancement," *IEEE Trans. Signal Inf. Process. over Netw.*, vol. 5, no. 4, pp. 792–806, Dec. 2019.

[5] C. Liu, J. Lee, and T. Q. S. Quek, "Safeguarding UAV communications against full-duplex active eavesdropper," *IEEE Trans. Wireless Commun.*, vol. 18, no. 6, pp. 2919–2931, Jun. 2019.

[6] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[7] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682–3722, 4th Quart., 2019.

[8] 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.

[9] F. Jameel, S. Wyne, and I. Krikidis, "Secrecy outage for wireless sensor networks," *IEEE Commun. Lett.*, vol. 21, no. 7, pp. 1565–1568, Jul. 2017.

[10] F. Jameel, S. Wyne, S. Junaid Nawaz, J. Ahmed, and K. Cumanan, "On the secrecy performance of SWIPT receiver architectures with multiple eavesdroppers," *Wireless Commun. Mobile Comput.*, vol. 2018, Jun. 2018, Art. no. 8747420.

[11] Z. Li, H. Fang, and H. Wang, "Integrated node authentication and key distribution method for body area network," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2019, pp. 557–561.

[12] E. Talavera, A. Diaz Alvarez, and J. E. Naranjo, "A review of security aspects in vehicular ad-hoc networks," *IEEE Access*, vol. 7, pp. 41981–41988, 2019.

[13] F. Jameel, S. Wyne, and Z. Ding, "Secure communications in three-step two-way energy harvesting DF relaying," *IEEE Commun. Lett.*, vol. 22, no. 2, pp. 308–311, Feb. 2018.

[14] A. O. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[15] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 917–930, May 2013.

[16] 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.

[17] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, 2013.

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

[19] M. Jacovic, M. Kraus, G. Mainland, and K. R. Dandekar, "Evaluation of physical layer secret key generation for IoT devices," in *Proc. IEEE 20th Wireless Microw. Technol. Conf. (WAMICON)*, Apr. 2019, pp. 1–6.

[20] B. Liu, A. Hu, and G. Li, "Secret key generation scheme based on the channel covariance matrix eigenvalues in FDD systems," *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1493–1496, Sep. 2019.

[21] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 2593–2597.

[22] 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.

[23] H. Zhao, Y. Zhang, X. Huang, and Y. Xiang, "An adaptive secret key establishment scheme in smart home environments," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.

[24] Y. Abdallah, M. Abdel Latif, M. Youssef, A. Sultan, and H. El Gamal, "Keys through ARQ: Theory and practice," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 737–751, Sep. 2011.

[25] Y. El Hajj Shehadeh, O. Alfandi, K. Tout, and D. Hogrefe, "Intelligent mechanisms for key generation from multipath wireless channels," in *Proc. Wireless Telecommun. Symp. (WTS)*, Apr. 2011, pp. 1–6.

[26] 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.*, 2007, pp. 401–410.

[27] X. Li, J. Liu, Q. Yao, and J. Ma, "Efficient and consistent key extraction based on received signal strength for vehicular ad hoc networks," *IEEE Access*, vol. 5, pp. 5281–5291, 2017.

[28] A. Albehadili, K. Al Shamaileh, A. Javaid, J. Oluoch, and V. Devabhaktuni, "An upper bound on PHY-layer key generation for secure communications over a Nakagami-m fading channel with asymmetric additive noise," *IEEE Access*, vol. 6, pp. 28137–28149, 2018.

[29] 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.

[30] M. Z. I. Sarkar, T. Ratnarajah, and M. Sellathurai, "Secrecy capacity of Nakagami-m fading wireless channels in the presence of multiple eavesdroppers," in *Proc. Asilomar Conf. Signals, Syst. Comput.*, 2009, pp. 829–833.

[31] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz-allen and Hamilton, Mclean, VA, USA, Tech. Rep. 800-22 Rev 1a, 2001.

[32] 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.*, 2008, pp. 128–139.

[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] M. McGuire, "Channel estimation for secret key generation," in *Proc. IEEE 28th Int. Conf. Adv. Inf. Netw. Appl.*, May 2014, pp. 490–496.

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

[36] M. Yuliana, Wirawan, and Suwadi, "An efficient key generation for the Internet of Things based synchronized quantization," *Sensors*, vol. 19, no. 12, p. 2674, Jun. 2019.

[37] B. Han, S. Peng, C. Wu, X. Wang, and B. Wang, "LoRa-based physical layer key generation for secure V2 V/V2I communications," *Sensors*, vol. 20, no. 3, p. 682, Jan. 2020.

[38] A. Soni, R. Upadhyay, and A. Kumar, "Wireless physical layer key generation with improved bit disagreement for the Internet of Things using moving window averaging," *Phys. Commun.*, vol. 33, pp. 249–258, 2019.

[39] H. Jin, K. Huang, S. Xiao, Y. Lou, X. Xu, and Y. Chen, "A two-layer secure quantization algorithm for secret key generation with correlated eavesdropping channel," *IEEE Access*, vol. 7, pp. 26480–26487, 2019.

[40] A. Raza, S. Junaid Nawaz, S. Wyne, A. Ahmed, M. A. Javed, and M. N. Patwary, "Spatial modeling of interference in inter-vehicular communications for 3-D volumetric wireless networks," *IEEE Access*, vol. 8, pp. 108281–108299, 2020.

[41] F. P. Fontæn and P. M. Espiæeira, *Modelling the Wireless Propagation Channel: A Simulation Approach With MATLAB*. Hoboken, NJ, USA: Wiley, 2008.

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

[43] X. Liu, "Outage probability of secrecy capacity over correlated log-normal fading channels," *IEEE Commun. Lett.*, vol. 17, no. 2, pp. 289–292, Feb. 2013.

[44] J. Hu, Y. Cai, N. Yang, X. Zhou, and W. Yang, "Artificial-Noise-Aided secure transmission scheme with limited training and feedback overhead," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 193–205, Jan. 2017.

[45] M. K. Simon and M.-S. Alouini, *Digital Communication Over Fading Channels*. 2nd ed. Hoboken, NJ, USA: Wiley, 2005.

[46] R. Beals and R. Wong, *Special Functions Orthogonal Polynomials*. Cambridge, U.K.: Cambridge Univ. Press, 2016.

[47] Ç. Candan and U. Orguner, "The moment function for the ratio of correlated generalized gamma variables," *Statist. Probab. Lett.*, vol. 83, no. 10, pp. 2353–2356, Oct. 2013.

[48] J. G. Proakis and M. Salehi, *Digital Communications*. 5th ed. New York, NY, USA: McGraw-Hill, 2007.

[49] A. Papoulis and S. U. Pillai, *Probability, Random Variables, and Stochastic Processes*. New York, NY, USA: McGraw-Hill, 2002.

MUHAMMAD ADIL received the master's degree in electrical engineering from the Department of Electrical and Computer Engineering, COMSATS University Islamabad (CUI), Islamabad, Pakistan, in 2016, where he is currently pursuing the Ph.D. degree. His current research interests include information theory and physical layer security, optimization in wireless communications, the Internet-of-Things (IoT), and 5G communications.

SHURJEEL WYNE (Senior Member, IEEE) received the Ph.D. degree from Lund University, Sweden, in March 2009. From April 2009 to April 2010, he was a Postdoctoral Research Fellow funded by the High-Speed Wireless Center, Lund University. Since June 2010, he has been with the Department of Electrical Engineering, COMSATS University Islamabad (CUI), Islamabad, Pakistan, where he currently serves as an Associate Professor. His research interests include wireless channel characterization, multi-antenna systems, cooperative communications, physical layer security, and vehicular communications. He was a co-recipient of the Best Paper Award of the Antennas and Propagation Track at IEEE VTC2013-Spring.

SYED JUNAID NAWAZ (Senior Member, IEEE) received the Ph.D. degree in electronic engineering from Mohammad Ali Jinnah University, Islamabad, Pakistan, in February 2012.

Since September 2005, he worked on several research and teaching positions with COMSATS University Islamabad (CUI), Islamabad; Staffordshire University, U.K.; Federal Urdu University, Pakistan; The University of York, U.K.; and the Aristotle University of Thessaloniki, Greece. Since 2012, he has been working as an Assistant Professor with the Department of Electrical and Computer Engineering, COMSATS University Islamabad (CUI). His current research interests include physical channel modeling, channel estimation and characterization, massive MIMO systems, adaptive signal processing, machine learning, compressed sensing, mmWave channels, the airborne Internet, underwater communications, the Internet of Things, and vehicle-to-vehicle communications.