IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 19 July 2024, accepted 9 September 2024, date of publication 17 September 2024, date of current version 3 October 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3462531

RESEARCH ARTICLE

On Pre-Processing of Generalized Gamma Fading Channel Samples for Secret Key Generation

GHALIB HUSSAIN[1], SYED JUNAID NAWAZ[1], (Senior Member, IEEE), SHURJEEL WYNE[1], (Senior Member, IEEE), ERNESTINA CIANCA[2], (Member, IEEE), AND MAURO DE SANCTIS[2]

[1]Department of Electrical and Computer Engineering, COMSATS University Islamabad (CUI), Islamabad 45550, Pakistan
[2]Department of Electronics Engineering, University of Rome "Tor Vergata," 00133 Rome, Italy

Corresponding author: Ernestina Cianca (ernestina.cianca@uniroma2.it)

This work was supported by HEC-NRPU Project 20-14731. The work of Ernestina Cianca and Mauro De Sanctis was supported by EU under the INRRP-NextGenerationEU, Partnership on "Telecommunications of the Future" through the Program "RESTART" under Grant PE0000001.

ABSTRACT With the advent of innovative wireless technologies and the rapid growth of diverse connected devices, ensuring communication security has become a critical challenge for the future massively connected beyond 5th generation (B5G) wireless networks. The physical layer security (PLS) approach leverages the inherent physical medium characteristics of communication networks to provide secure communications. In particular, the wireless channel-based secret key generation (SKG) is a PLS approach that creates symmetric keys for message encryption/decryption by exploiting the randomness inherent in wireless channels while relying on the channel to be reciprocal between the nodes. This work proposes a novel SKG algorithm that emphasizes the pre-processing and quantization stages with the aim to increase the key generation rate (KGR) and the key agreement rate (KAR) between the legitimate nodes. The algorithm employs biasing of selective samples and sliding-window weighted averaging of the Generalized Gamma fading channel samples based on the channel's average contiguous duration (ACD) metric, a second-order fading statistic, to enhance the channel reciprocity. The proposed scheme may also be used to improve the key randomness rate (KRR) by using a non-contiguous multi-level quantization strategy that evenly sets the quantization intervals to accommodate a similar number of channel samples across these intervals. Thus, a desired trade-off between the KGR, KAR, and KRR to meet operational requirements can be achieved with the proposed scheme. Finally, a comprehensive analysis of the performance gains of the proposed scheme in relation to other notable works is conducted by investigating the impact of several channel and algorithmic parameters on the KGR, KAR, and KRR of these schemes.

INDEX TERMS Fading channel, generalized gamma fading, physical layer security, pre-processing, quantization, reciprocity, second-order statistics, secret key generation.

I. INTRODUCTION

The increased data traffic of 5th generation (5G) networks has also increased the risks related to data security, privacy, and authentication [1]. Given these networks, fast and secure algorithms are critical for message encryption and decryption [2]. Wireless channel-based key generation is a promising technique for wireless networks especially for scenarios where traditional cryptographic methods are not feasible due to limitations on hardware complexity or battery operation [3]. Such SKG schemes rely on wireless channel randomness and only require the bidirectional channel between the legitimate nodes to be reciprocal. Then some measurable channel characteristics such as the complex-valued channel state information (CSI), received signal envelope, received signal strength (RSS), or the angle of

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

arrival (AoA) statistics may be used to generate a symmetric secret key simultaneously at the legitimate nodes [4]. The performance of SKG schemes is conventionally assessed by metrics such as the Key Generation Rate (KGR), Key Agreement Rate (KAR), and the Key Randomness Rate (KRR) [5]. These metrics serve as measures of the extracted key from given channel samples in terms of length, fraction of mismatched key bits between the legitimate users, and randomness of the extracted secret key, respectively. A given SKG scheme aims to achieve a desirable trade-off between these performance metrics.

A. MOTIVATION

Wireless communications between the legitimate nodes require some security mechanism to protect the broadcast data against adversarial eavesdropping [6]. The information-theoretic security schemes require some form of coding to approach the theoretical maximum secure communication rate between the legitimate nodes but require these nodes to have the eavesdropper's CSI [7]. On the other hand, the traditional key-based cryptographic schemes operate under the assumption of limited computational capability of potential eavesdroppers, which restricts their ability to decipher the encoded message in a reasonable time. Some of these methods also require supporting infrastructure to distribute the secret keys among the legitimate nodes. However, with the Moore's law-based increase in the computational ability of wireless devices, and the introduction of quantum computing [8], the first assumption is being challenged. Furthermore, the required infrastructure for secret key distribution does not scale with increasing user numbers in emerging telecommunications verticals such as vehicular communications and internet-of-things [9], [10].

B. RELATED WORK

The idea to exploit the physical layer in wireless networks for SKG exists since the mid-1990s [11], [12]. In [13], the authors leverage multiple antennas to enhance the SKG rate within a coherence time interval T_c. However, their approach solely explores spatial diversity, it only uses differences in signal strength (like changing reception in different spots) to create secret keys, thereby limiting the improvement in key rate by the number of deployed antennas. In [14], a practical implementation of RSS-based SKG was established in a highly mobile environment. The authors in [15], introduced a novel channel-based key generation scheme for orthogonal frequency-division multiplexing (OFDM) communication, exploiting channel parameters' inherent randomness in indoor and outdoor environments. In [16], the authors proposed an SKG algorithm based on principal component analysis (PCA) with a common eigenvector, that helps improve the key agreement and the randomness of the extracted key. This work also highlights the issues of key agreement over wireless fading channels, which can be characterized by the CSI of the legitimate nodes and the eavesdropper. The work in [17], presents a two-way SKG scheme that improves the randomness of the secret key by eliminating the need for channel estimation and increasing the key rate, compared to the conventional one-way SKG schemes. In [18], a random Gaussian matrix is applied to the RSS measurements, which enhances the randomness of the SKG process while preserving the KAR and KGR. In [10], the authors propose a cumulative distribution function (CDF)-based non-uniform quantization (NUQ) of Nakagammi-m fading channel envelope for SKG, and it is shown that the proposed NUQ scheme provides better key randomness performance when compared with the uniform quantization approach. In [19], an average contiguous duration (ACD) metric is proposed as a generalization of the well-known level-crossing-rate metric, to characterize the second order channel fading statistics. In continuation of this work the same authors in [20] propose an ACD-based NUQ scheme for channel-based SKG while considering a Generalized Gamma fading channel envelope. The proposed ACD-based NUQ scheme is shown to provide performance gains in the trade-off between KGR and KAR in comparison with that provided by uniform quantization or the CDF-based NUQ scheme. The work in [21], develops an integer linear programming (ILP) algorithm that optimizes the key randomness in SKG, by solving an ILP problem to find the optimal quantization levels and codebook for the RSS signals. The work in [22], designed a novel system that combines physically unclonable functions (PUFs) and channel responses (CR) to enable a high KGR. The work in [23], introduced an SKG scheme that leverages the wireless channel characteristics of OFDM systems to achieve a higher KGR.

C. CONTRIBUTIONS

The channel-based SKG technique proposed in this work uses the channel pre-processing and quantization steps to enhance performance trade-off between the KGR, KAR, and KRR metrics, in a given application scenario. The main contributions of this work are listed as follows.

1) A sample importance-based method for pre-processing the received signal envelope is proposed. This method uses selective sample biasing and Gaussian-shaped moving window averaging (G-MWA) to mitigate the effects of measurement noise.
2) A two-stage non-uniform quantizer is derived. The first stage, during pre-processing, involves second-order statistics-based biasing of selective channel samples. The second stage, after pre-processing, uses a non-contiguous multi-level non-uniform quantizer to extract binary secret key bits from the transformed channel samples under Generalized Gamma fading conditions.
3) A comprehensive performance analysis is conducted, demonstrating the performance gains of the proposed algorithm compared to other notable SKG schemes in terms of KAR, KRR, and KGR metrics.

The remainder of the paper is organized as follows: Section II represents system model. Section III provides an analytical framework for the proposed SKG technique. Section IV examines the performance of the proposed SKG scheme and compares it with other notable SKG schemes in the literature. Finally Section V concludes this work. TABLE 1 summarizes the key mathematical notations used in this work.

TABLE 1. Definitions of important parameters.

Notation	Definition
$h_{(\cdot)}$	Channel envelope
β	GG fading shape parameter
υ	Inverse of normalized channel variance
ξ	Statistical expectation of $h_{(\cdot)}^{\beta}$
ρ	Correlation coefficient between channels h_{ba} and h_{ab}
M	Number of quantization levels
Ω	Window Shape
α	Sample wight/Bias
w_s	Window Size
w_o	Window Overlap
μ_w	Window Mean
p_s	Window Position
σ_w	Window standard deviation
σ_w^2	Variance of window
$h_{(\cdot)}^{-}$	Lower threshold
$h_{(\cdot)}^{+}$	Upper threshold
q	Amplitude threshold
$\Xi_{h_{(\cdot)}^{-}}^{q}$	ACD between thresholds $h_{(\cdot)}^{-}$ and q
$\Xi_{q}^{h_{(\cdot)}^{+}}$	ACD between thresholds q and $h_{(\cdot)}^{+}$
ρ_1	Lower quantization threshold
ρ_2	Upper quantization threshold
f_m	Maximum Doppler shift
T_c	Coherence time of main channel
$\mathcal{X}_j$	Qualifying excursions
$\mathcal{I}$	Central indices of qualifying excursions
$\mathcal{K}_G$	Key generation rate (KGR)
$\mathcal{K}_A$	Key agreement rate (KAR)
$\mathcal{K}_{(\cdot)}$	Generated secret key at respected node

II. SYSTEM MODEL

Fig. 1 illustrates a time-division duplex (TDD) wireless communication scenario where two legitimate nodes, Alice and Bob, communicate with each other in the presence of a passive eavesdropper (denoted as Eve). The reciprocal channel between Alice and Bob is referred to as the main channel [24]. In such a TDD system, the main channel is reciprocal within a coherence time slot, i.e., the behavior of the wireless channel remains the same regardless of the direction of transmission. The channels between legitimate nodes (Alice or Bob) and Eve are denoted as eavesdropper's channels.

The channel from Alice to Bob is represented as h_{ab}, while the reciprocal channel from Bob to Alice is denoted as h_{ba}. The channels from Alice to Eve and from Bob to Eve are denoted as h_{ae} and h_{be}, respectively. We model the wireless channels as Generalized Gamma (GG) fading channels for their ability to represent multiple fading conditions with an appropriate choice of its fading shape parameters [25]. The probability density function (PDF) of the GG distributed received signal envelope can be expressed as

$$f(h_{(\cdot)}) = \frac{\beta}{\Gamma(\upsilon)}\left(\frac{\upsilon}{\xi}\right)^{\upsilon} h_{(\cdot)}^{\beta\upsilon-1}\exp\left(-\frac{\upsilon h_{(\cdot)}^{\beta}}{\xi}\right), \tag{1}$$

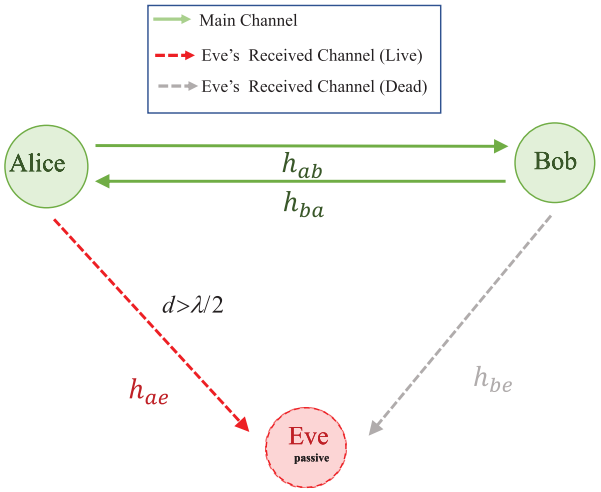


FIGURE 1. Considered system model.

where β is the fading shape parameter, $\Gamma(\cdot)$ is the Gamma function [26], ξ is the statistical expectation of $h_{(\cdot)}^{\alpha}$ (i.e., $\xi = E\left[h_{(\cdot)}^{\alpha}\right]$), and υ is the inverse normalized variance of GG fading channel derived as

$$\upsilon = \frac{E^2[h_{(\cdot)}^{\beta}]}{V[h_{(\cdot)}^{\beta}]}. \tag{2}$$

GG distribution can represent various other types of distributions as its special case e.g., Rayleigh distribution can be obtained by setting ($\beta = 2$ and $\upsilon = 1$), Nakagami-m distribution can be obtained by setting ($\beta = 2$ and $\upsilon = m$), and Weibull distribution can be obtained by setting $\upsilon = 1$, etc. The cumulative distribution function (CDF) of GG fading channels can be expressed as

$$F(h_{(\cdot)}) = \frac{\gamma\left(\upsilon, \frac{h_{(\cdot)}^{\beta}}{\xi}\right)}{\Gamma(\upsilon)}, \tag{3}$$

where $\gamma(\cdot,\cdot)$ is the lower incomplete Gamma function [27].

Given the channel from Alice-to-Bob h_{ab}, the reciprocal channel from Bob-to-Alice h_{ba} can be obtained by employing the Gauss-Markov model [28], which is given as

$$h_{ba} = \rho h_{ab} + \sqrt{1-\rho^2}\varepsilon, \tag{4}$$

where $\rho \sim [0;1]$ represents the correlation coefficient between h_{ab} and h_{ba}, and $\varepsilon \sim \mathcal{N}(0,1)$ represents a Normal-distributed measurement error that is independent of the channel. The Gauss-Markov model given in (4) is commonly employed for representing the reciprocity in Gaussian channels (i.e., Rayleigh fading envelope). However, for other

fading conditions, the addition operation in the Gauss-Markov model leads to the convolution of the distributions of the channel response h_{ab} and the error/noise term ε. This convolution results in a distinct distribution of h_{ba} compared to that of h_{ab}, which may not accurately represent the reciprocal channel. In contrast, a joint CDF inversion-based model recently proposed in [20] aims at preserving the distribution of both reciprocal channels as the target fading distribution such as GG fading conditions. This joint CDF inversion-based model is discussed in the following paragraphs.

The joint PDF of reciprocal GG fading channels h_{ab} and h_{ba} can be expressed as [29]

$$P(h_{ba}, h_{ab}) = \frac{\beta^2 \upsilon^{\upsilon+1} h_{ba}^{\beta\frac{1}{2}(\upsilon+1)-1} h_{ab}^{\beta\frac{1}{2}(\upsilon+1)-1}}{\Gamma(\upsilon)\xi^{\upsilon+1}(1-\rho)\rho^{\frac{\upsilon-1}{2}}} \times \exp\left(-\upsilon\frac{h_{ba}^2+h_{ab}^2}{(1-\rho)\xi}\right) I_{\upsilon-1}\left(\frac{2\upsilon\sqrt{\rho h_{ba}^{\beta} h_{ab}^{\beta}}}{(1-\rho)\xi}\right), \tag{5}$$

where $I_{\upsilon-1}(\cdot)$ represents the Bessel function of the first kind and $(\upsilon-1)^{\text{th}}$ order. By using (1) and (5), the conditional PDF of h_{ba} given h_{ab} can be obtained as

$$P(h_{ba}|h_{ab}) = \exp\left(\frac{\upsilon h_{ab}^{\beta}}{\xi} - \frac{\upsilon(h_{ba}^{\beta}+h_{ab}^{\beta})}{\xi(1-\rho)}\right) \times \frac{\upsilon\beta}{(1-\rho)\xi}\left(\frac{h_{ba}}{\sqrt{(h_{ba}^{\beta}+h_{ab}^{\beta})\rho}}\right)^{\upsilon-1} \times I_{\upsilon-1}\left(\frac{2\upsilon\sqrt{(h_{ba}^{\beta}+h_{ab}^{\beta})\rho}}{(1-\rho)\xi}\right). \tag{6}$$

Subsequently, the conditional CDF of h_{ba} given h_{ab} can be obtained by integrating (6) over h_{ab}, which is

$$F(h_{ba}|h_{ab}) = 1 - \mathrm{Q}_{\upsilon}\left(\sqrt{\frac{2\upsilon\rho h_{ab}^{\beta}}{\xi(1-\rho)}}, \sqrt{\frac{2\upsilon\rho h_{ba}^{\beta}}{\xi(1-\rho)}}\right), \tag{7}$$

where $\mathrm{Q}_{\upsilon}(.,.)$ represents the Marcum-Q function of order υ.

Given the channel samples h_{ab} and the reciprocity condition as described by the correlation coefficient ρ, the conditional CDF given in (7) can be inverted to generate h_{ba}, as described in [10] and [20]. The inverse of the Marcum-Q function used in (7) can be computed by using numerical methods, as discussed in [30]. Alternatively, the first-order approximation of Marcum-Q function given in [31] can be used and a closed-form solution for the inverse of (7) can be obtained. In this study, we employ numerical inversion method, as discussion.

III. PROPOSED SECRET KEY GENERATION (SKG) ALGORITHM

The generic SKG process is illustrated in Fig. 2. The proposed work focuses on the critical stages of pre-processing and quantization for SKG. This research introduces a novel pre-processing technique designed for enhancing channel reciprocity to improve SKG performance in terms of KGR, KAR, and KRR. The method involves biasing the selective channel samples based on ACD metric, a second-order fading statistics metric, and performing sliding-window weighted averaging. The wireless channels are modeled as Generalized Gamma fading channels.

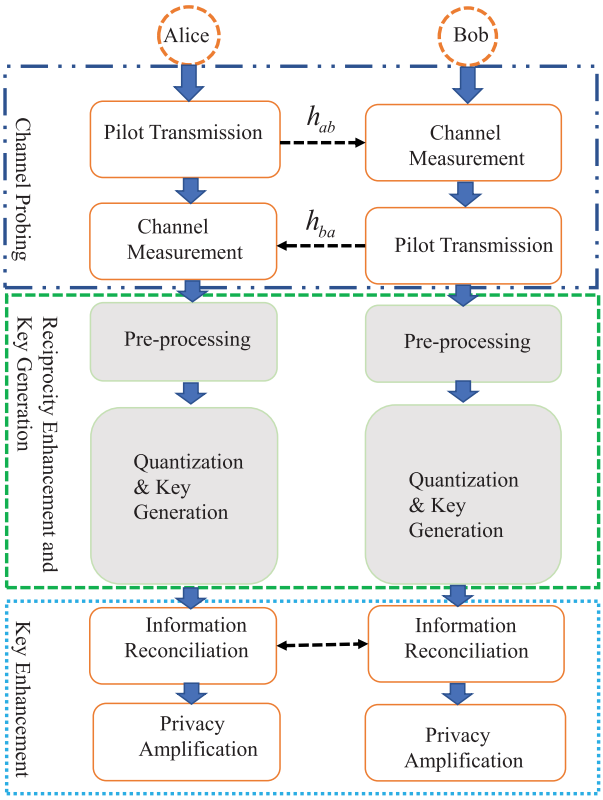


FIGURE 2. Key steps for SKG.

The Algorithm 1 outlines the core steps of the proposed SKG scheme which are described in the following paragraphs. Besides, the composition of channel samples at different intermediate steps along with channel statistics are highlighted in Fig. 3.

A. INPUT/INITIALIZE

The algorithm begins with initializing the key system parameters. These parameters include sample count N, representing the total number of channel samples. The threshold for minimum excursion length to be considered L. Inspired from the level-crossing algorithm proposed in [32], this parameter defines the threshold for minimum number of samples to contiguously fall within a certain quantization interval to be considered as a qualifying excursion of samples. This size of sliding window is represented by w_s. The overlap in the adjacent positions of the sliding window is w_o.

B. PROBE AND ESTIMATE CHANNEL

This step involves estimating the main reciprocal channels at Alice and Bob. This is done by exchanging the pilot

Algorithm 1 Proposed SKG Algorithm

Initialize Parameters:

- Sample count N, threshold for excursion length L, window size w_s, window overlap w_o, etc

Probe/Estimate channel:

- Probe channel and estimate channel samples $h_{(\cdot)}$ (or generate channel samples from Generalized Gamma (GG) fading model as given in (1) for simulations)
  - Estimate/set fading shape parameters β, ξ, and υ
  - Estimate channel mean $\mu_{h_{(\cdot)}}$, channel standard deviation $\sigma_{h_{(\cdot)}}$, channel maximum amplitude $h^{+}_{(\cdot)}$, channel minimum amplitude $h^{-}_{(\cdot)}$

Channel Pre-Process:

- Compute separating amplitude thresholds q_i for achieving M equal ACD intervals
  - e.g., for $M = 2$, solve $\Xi^{q}_{h^{-}_{(\cdot)}} = \Xi^{h^{+}_{(\cdot)}}_{q}$ for q (given in (9) and (8))
- Shift the channel envelope: $\check{h}_{(\cdot)} = h_{(\cdot)} - q$

Sample Selection:

- Identify channel sample excursions, represented as $\mathcal{X}_{j\in\{1,\cdots,J\}}$, with a minimum temporal duration of L samples from the channel $\check{h}_{(\cdot)}$, segmented into two amplitude intervals separated by 0 amplitude
- Compute and record the indices of the central sample for each excursion $\mathcal{X}_j$ within the set $\mathcal{I}$

Window Sliding:

- Set sample bias parameter $\alpha \geq 1$
- Determine window shape $\Omega_{[1\times w_s]}$
  - e.g., Gaussian window $\Omega_{[1\times w_s]} \sim \mathcal{N}(\mu_w, \sigma_w^2)$ as in (11) and rectangular window as in (12)
- Assign biasing weight to the selected samples $\breve{h}_{(\cdot)}(n) = \begin{cases} \alpha\check{h}_{(\cdot)}(n) & ; n \in \mathcal{I} \\ \check{h}_{(\cdot)}(n) & ; n \notin \mathcal{I} \end{cases}$
- Perform sliding window weighted averaging for $n = 1$ to N with overlap of w_o samples $\tilde{h}(n) = \frac{\sum_{i=n}^{n+w_s-1} \Omega(i-n)\breve{h}_{(\cdot)}(i)}{\sum_{i=0}^{w_s-1} \Omega(i)}$

Channel Quantization:

- Compute thresholds ρ_1 and ρ_2 such that $\int_{-\infty}^{\rho_1} f\left(\tilde{h}_{(\cdot)}\right) d\tilde{h} + \int_{\rho_2}^{+\infty} f\left(\tilde{h}_{(\cdot)}\right) d\tilde{h} = \int_{\rho_1}^{\rho_2} f\left(\tilde{h}_{(\cdot)}\right) d\tilde{h}$
- Employ 2-level non-contiguous multi-interval quantization (with binary coding $\mathcal{K}^{b}_{(\cdot)} = \mathcal{H}(\tilde{h}_{(\cdot)})$

Other Steps:

- Key Reconciliation
- Privacy Amplification

signals and estimating the channel from the known pilots and their corresponding received signals. Considering TDD system, both Alice and Bob estimate their channels within a coherence time slot T_c. The received signal envelope for Alice-to-Bob and Bob-to-Alice channels is represented as h_{ab} and h_{ba}, respectively. We represent both channels using a single notation without the subscript as $h_{(\cdot)}$. After estimating the channels, the associated channel parameters can be estimated, i.e., channel envelope mean $\mu_{h_{(\cdot)}}$, channel envelope standard deviation $\sigma_{h_{(\cdot)}}$, maximum envelope value $h^{+}_{(\cdot)}$, minimum envelope value $h^{-}_{(\cdot)}$, and fading shape parameters (β, ξ, and υ).

For the purpose of simulations, the channels are drawn from generalized gamma (GG) fading distribution by first initializing the channel parameters such as $\mu_{h_{(\cdot)}}$, $\sigma_{h_{(\cdot)}}$, β, ξ, and υ. The GG-fading model is considered for its ability to model various diverse fading conditions as its special cases with appropriate choice of its shape parameters, as discussed in Sec. II. The reciprocal channel given one channel can be drawn by using the CDF inversion method discussed in Sec. II.

C. CHANNEL PRE-PROCESSING

After estimating the channel envelope and associated parameters, we strategically segment the channel response $h_{(\cdot)}$ into two intervals ($\mathcal{Q}_1$ and $\mathcal{Q}_2$) with equal average contiguous duration (ACD). The ACD of a fading signal represents the average time period during which the signal consistently stays between two specified thresholds [19]. The separating threshold q for the intervals $\mathcal{Q}_1$ and $\mathcal{Q}_2$ can be obtained by equating the ACD of both the intervals. Such definition of the intervals guarantees that an equal number consecutive channel samples on average fall in both the intervals. The ACD for the amplitude interval $\mathcal{Q}_1$ defined from $h^{-}_{(\cdot)}$ to peak amplitude q can be expressed as,

$$\Xi^{q}_{h^{-}_{(\cdot)}} = \frac{\left(2\pi f_m^2\right)^{\frac{-1}{2}} \left(\frac{\xi}{\upsilon}\right)^{\upsilon-\frac{1}{2}} \left(\gamma\left(\upsilon, \frac{\upsilon q^{\beta}}{\xi}\right) - \gamma\left(\upsilon, \frac{\upsilon\left(h^{-}_{(\cdot)}\right)^{\beta}}{\xi}\right)\right)}{\left(h^{-}_{(\cdot)}\right)^{\frac{\beta}{2}(2\upsilon-1)} \exp\left(-\frac{\upsilon\left(h^{-}_{(\cdot)}\right)^{\beta}}{\xi}\right) + q^{\frac{\beta}{2}(2\upsilon-1)} \exp\left(-\frac{\upsilon q^{\beta}}{\xi}\right)}, \tag{8}$$

where f_m represents the maximum Doppler shift. Similarly, the ACD for the amplitude interval $\mathcal{Q}_2$ defined from the amplitude threshold q to the peak amplitude $h^{-}_{(\cdot)}$ can be expressed as,

$$\Xi^{h^{+}_{(\cdot)}}_{q} = \frac{\left(2\pi f_m^2\right)^{\frac{-1}{2}} \left(\frac{\xi}{\upsilon}\right)^{\upsilon-\frac{1}{2}} \left(\gamma\left(\upsilon, \frac{\upsilon\left(h^{+}_{(\cdot)}\right)^{\beta}}{\xi}\right) - \gamma\left(\upsilon, \frac{\upsilon q^{\beta}}{\xi}\right)\right)}{\left(q^{\frac{\beta}{2}(2\upsilon-1)} \exp\left(-\frac{\upsilon q^{\beta}}{\xi}\right) + \left(h^{+}_{(\cdot)}\right)^{\frac{\beta}{2}(2\upsilon-1)} \exp\left(-\frac{\upsilon\left(h^{+}_{(\cdot)}\right)^{\beta}}{\xi}\right)\right)}. \tag{9}$$

The amplitude threshold q that divides the entire amplitude range into two intervals $\mathcal{Q}_1$ and $\mathcal{Q}_2$ representing an equal

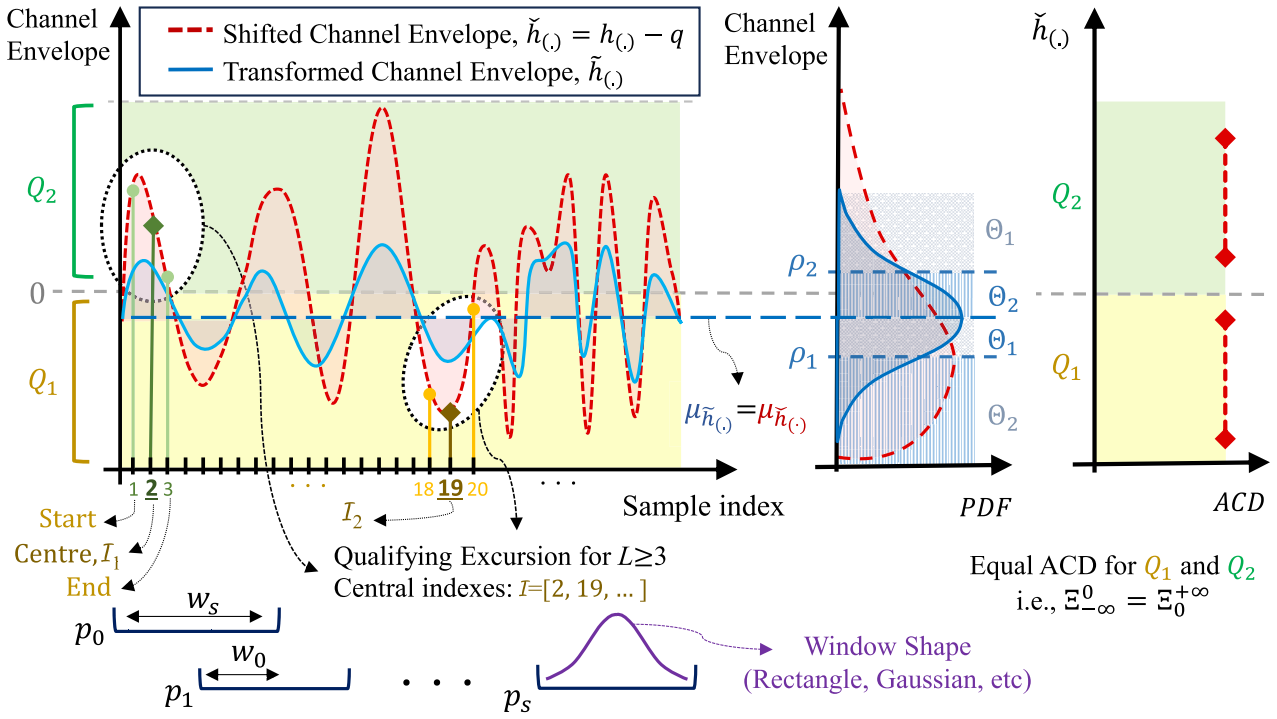


FIGURE 3. Working principle of the proposed SKG algorithm.

ACD level can be obtained by equating (8) and (9) and numerically solving for q. Subsequently, the channel envelope is shifted by subtracting q units from the envelope, i.e., $\check{h}_{(.)} = h_{(.)} - q$. This essentially shifts the entire range of $h_{(.)}$ values such that the separating threshold becomes zero. This shifting operation assists in conveniently biasing the selective channel samples in the later steps of the proposed algorithm.

D. SAMPLE SELECTION

The samples that are more likely to fall in the same quantization interval on both the sides of the link are selected and biased. The algorithm searches for a sequence of samples that consecutively stay within a specific quantization interval, the set of such samples is termed as an excursion of samples. This sample selection is inspired from an existing level-crossing SKG algorithm proposed in [32] and [33]. The algorithm Identify channel sample excursions, represented as $\mathcal{X}_{j\in\{1,\cdots,J\}}$, with a minimum temporal duration of L samples from the channel $\check{h}_{(.)}$, segmented into two amplitude intervals $\mathcal{Q}_1$ and $\mathcal{Q}_2$ separated by 0 amplitude. For the recorded excursions $\mathcal{X}_j$, the indices of the central sample of each excursion is recorded in the set $\mathcal{I} = [\mathcal{I}_1, \mathcal{I}_2, \cdots, \mathcal{I}_J]^T$.

E. CHANNEL TRANSFORM

The samples selected in the previous step are biased and a sliding window weighted averaging is employed. The sample bias parameter is set as $\alpha \geq 1$, with $\alpha = 1$ representing no biasing. This plays a crucial role in emphasizing the importance of selected channel samples. This biasing operation can be expressed as:

$$\check{h}_{(.)}(n) = \begin{cases} \alpha \check{h}_{(.)}(n); & n \in \mathcal{I}, \\ \check{h}_{(.)}(n); & n \notin \mathcal{I}. \end{cases} \tag{10}$$

The proposed SKG algorithm leverages a sliding window weighted averaging function to transform the channel samples. This technique assigns weights to the channel samples within the window, allowing for selective emphasis or de-emphasis of certain samples. The shape of the window function can be chosen from various options to suit the specific performance requirements/targets. Some common window function shapes include Gaussian, Butterworth, ideal rectangular shape windows.

The Gaussian window function is defined by the following equation:

$$\Omega^{\text{Gaussian}}(n) = \frac{1}{\sigma_w \sqrt{2\pi}} \exp\left(-\frac{(n-\mu_w)^2}{2\sigma_w^2}\right), \tag{11}$$

where μ_w and σ_w represent the mean and standard deviation of the window, respectively. Similarly, the rectangular window can be expressed as,

$$\Omega^{\text{Rectangle}}(n) = \begin{cases} 1; & n < w_s, \\ 0; & \text{otherwise}. \end{cases} \tag{12}$$

Moving window averaging effectively reduces rapid/high-frequency fluctuations in received signal envelope, resulting in a lower standard deviation and decreased key bits disagreement between communicating nodes. We selected a Gaussian window shape due to its smooth weighting of samples, giving more importance to those at the center and

less to those on the edges. In contrast, a rectangular window shape assigns equal weights to all samples within the window, resulting in a sharp cutoff at the window edges that can introduce ringing effects in the smoothed signal, particularly for channels with rapid fluctuations.

The window of selected w_s samples is weighted with the function $\Omega(\cdot)$ and averaged to determine the n^{th} sample of the transformed channel $\tilde{h}_{(\cdot)}(n)$. The window then slides forward by $w_s - w_o$ samples and computes the next sample, continuing this process iteratively. This sliding operation results in an overlap of w_o samples between adjacent window positions. This operation can be expressed as,

$$\tilde{h}(n) = \frac{\sum_{i=n}^{n+w_s-1} \Omega(i-n)\check{h}_{(\cdot)}(i)}{\sum_{i=0}^{w_s-1} \Omega(i)}. \tag{13}$$

F. CHANNEL QUANTIZATION

The working principle of the sample selection and sliding window weighted averaging along with the ACD profile and PDFs of the original channel $f(h_{(\cdot)})$ and the transformed channel $f(\tilde{h}_{(\cdot)})$ are highlighted in Fig. 3.

The distribution of the mean of a random variable (i.e., channel envelope), usually termed as sampling distribution of the mean, describes the probability distribution of all possible sample means that can be obtained by taking repeated samples of a fixed size from the population [34]. When the distribution of the population is not normal distributed, still the sampling distribution of the mean approaches normality as the sample/window size increases due to the central limit theorem. To this end, in the context of the proposed channel smoothing operation, when rectangular-shaped window is considered, the distribution of the smoothed signal tends to follow Gaussian distribution, as illustrated in Fig. 3. Subsequently, the mean of the transformed/smoothed channel envelope is equal to the mean of the measured channel envelope, i.e., $\mu_{\tilde{h}_{(\cdot)}} = \mu_{h_{(\cdot)}}$, whereas the standard deviation of the smoothed signal can be related to the standard deviation of the measured channel as $\sigma_{\tilde{h}_{(\cdot)}} = \sigma_{h_{(\cdot)}}/\sqrt{w_s}$, i.e., it decreases with an increase in the window size. To quantize the Gaussian distributed transformed channel samples $\tilde{h}_{(\cdot)}$, we propose defining two-level quantization with multiple non-contiguous intervals, labeled as Θ_1 and Θ_2, with equal densities for both the levels, as shown in Fig. 3. These intervals are defined as non-contiguous with the aim to enhance randomness in the secret generated key bits, as well as to ensure equal matching or mismatching of '1's and '0's in the extracted key bits. As this is being performed on the smoothed/transformed signal, this non-contiguous definition of the intervals provides minimal loss in the agreement rate and a significant gain in randomness properties of the key. The separating thresholds for these non-contiguous intervals of two-level quantizer are ρ_1, ρ_2, and $\mu_{\tilde{h}_{(\cdot)}}$. These thresholds ensure equal density for each quantization level, which can be obtained by solving the following equation.

$$\int_{-\infty}^{\rho_1} f\left(\tilde{h}_{(\cdot)}\right) d\tilde{h} + \int_{\rho_2}^{+\infty} f\left(\tilde{h}_{(\cdot)}\right) d\tilde{h} = \int_{\rho_1}^{\rho_2} f\left(\tilde{h}_{(\cdot)}\right) d\tilde{h}. \tag{14}$$

Based on computed thresholds, the processed channel samples are converted into a key bit sequence. This is achieved by mapping the samples to non-contiguous multi-level quantization levels with associated binary coding, see Fig. 3, expressed using the $\mathcal{H}(\cdot)$ mapping function as:

$$\mathcal{K}_{(\cdot)}^{b} = \mathcal{H}(\tilde{h}_{(\cdot)}). \tag{15}$$

G. INFORMATION RECONCILIATION AND PRIVACY AMPLIFICATION

To rectify the disparity in generated key bits, various information reconciliation techniques can be employed, such as error-correcting codes (ECC), Golay code, Turbo code, binary coded decimal (BCD) code, and Bose, Chaudhuri, and Hocquenghem (BCH) codes. In the reconciliation process, certain information is publicly broadcasted, and the eavesdropper can hear it. This exposed information is then removed through privacy amplification methods.

Both information reconciliation and privacy amplification are crucial for error correction and securing extracted secret keys. While standard techniques are used for these steps, which are outside the scope of this work, our focus lies in improving the pre-processing and quantization stages to extract key bits.

IV. RESULTS AND DISCUSSION

This section presents a comprehensive performance analysis of the proposed SKG algorithm. The performance of the proposed SKG algorithm is analyzed under different channel correlation conditions ρ, channel fading conditions β, window size variations w_s, and the window overlap sizes w_o. The performance is evaluated in terms of three performance metrics, viz: KGR, KAR, and KRR. The KGR is denoted by $\mathcal{K}_G$, which indicates the number of secret bits generated in relation to the number of available channel samples. The KAR is denoted by $\mathcal{K}_A$, which reflects the likelihood of having identical keys at legitimate nodes. The KRR quantifies the randomness in the extracted secret key bits. The KRR is evaluated in terms of the tests suggested in NIST statistical test suite [35]. The tests considered for evaluating the KRR are: Frequency Monobit Test, Frequency Block Test, Run Test, Longest Run of ones Test, Discreate Fourier Transform Test, Cumulative Forward Test, Cumulative Reversed Test, Matrix Rank Test, Linear Complexity Test, respectively.

A. THE INFLUENCE OF CHANNEL CORRELATION COEFFICIENT ρ ON $\mathcal{K}_A$ AND $\mathcal{K}_G$ PERFORMANCE

The impact of correlation coefficient ρ and window overlap w_o on $\mathcal{K}_A$ and $\mathcal{K}_G$ performance is demonstrated in Fig. 4. The experiment is conducted for the setting of $\beta = 2$, $\xi = 1$, and $\upsilon = 1$, where the algorithm parameters are set as: $M = 2$, $L = 3$ and $ws = 10$. Fig. 4 (a) illustrates that as the value of ρ increases, the corresponding value of $\mathcal{K}_A$ also increases which indicates better key agreement at a higher value of ρ. However, Fig. 4 (a) also highlights that an increase in window overlap, denoted by w_o, interestingly maintains $\mathcal{K}_A$ performance. This occurs because, with greater overlap,

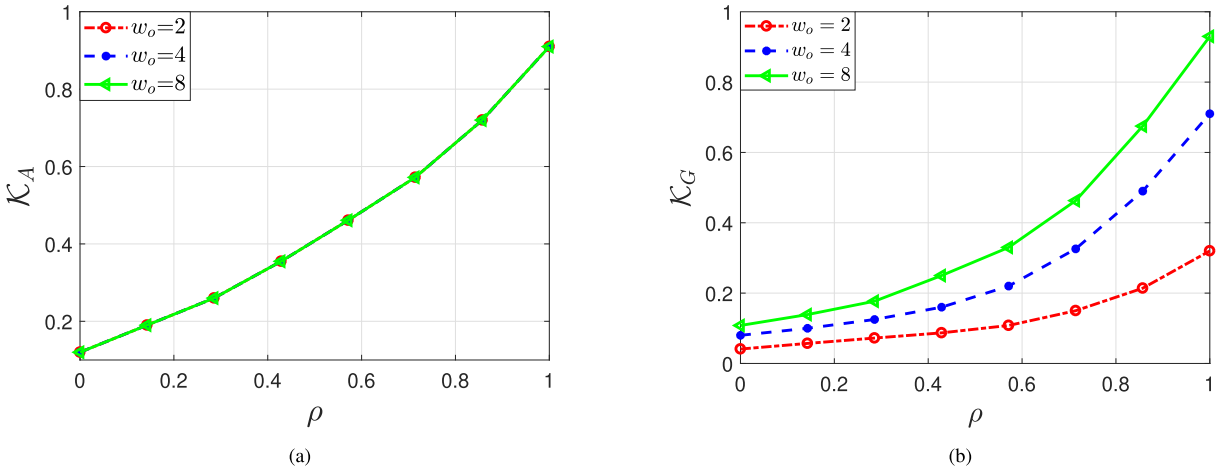


FIGURE 4. The impact of ρ and w_o on $\mathcal{K}_A$ and $\mathcal{K}_G$ in (a) and (b), respectively. Other parameters are: $M = 2$, $L = 3$, $\alpha = 3$, $ws = 10$, $\beta = 2$, $\xi = 1$, and $\upsilon = 1$.

there's an increase in sample reuse between consecutive windows. This reuse effectively boosts the key rate, as more potential key points are considered. However, it's important to note that the ratio of samples generated at the legitimate nodes remains the same.

Fig. 4 (b) shows the impact of the ρ on $\mathcal{K}_G$ performance. As ρ increases, $\mathcal{K}_G$ generally improves, but the rate of improvement varies due to the overlapping factor w_o.

Higher overlap leads to greater $\mathcal{K}_G$ gains because more samples are reused in the SKG process. This suggests a trade-off between overlap and randomness performance, with an optimal balance depending on the specific task and dataset. The proposed algorithm can demonstrate a significant advantage for $\mathcal{K}_G$, especially for low correlation conditions. This indicates the proposed algorithm can generate more secure and reliable keys in challenging environments.

B. THE IMPACT OF FADING PARAMETER β ON $\mathcal{K}_A$ AND $\mathcal{K}_G$ PERFORMANCE

The $\mathcal{K}_A$ and $\mathcal{K}_G$ performance under the influence of fading parameter β, window overlap w_o, and window size w_s is presented in Fig. 5. The results are obtained for the channel shape parameters as $\xi = 1$, and $\upsilon = 1$, while algorithm parameters are set as $M = 2$ and $L = 3$. Fig. 5 (a) presents that the $\mathcal{K}_A$ performance of the proposed technique deteriorates rapidly as β values increase. The increase in β leading to a substantial reduction in $\mathcal{K}_A$ performance is mainly due to the sample rejection ratio (SRR) at the quantization stage. However, during the analysis, it has been observed that an increase in w_s contributes to an improvement in the system's $\mathcal{K}_A$ performance. This observation underscores the sensitivity of $\mathcal{K}_A$ to changes in both β and w_s parameters.

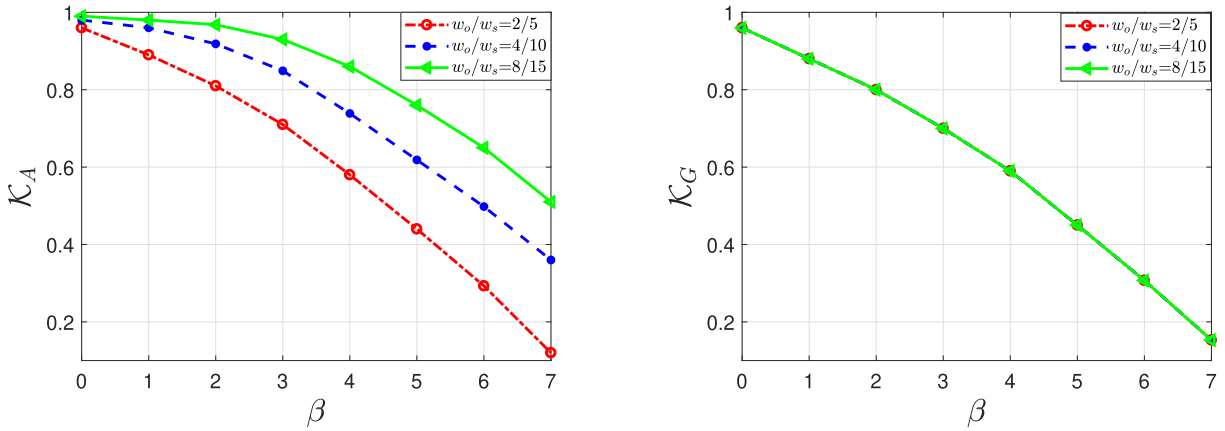
Fig. 5 (b) demonstrates that as the value of β increases, the corresponding value of $\mathcal{K}_G$ decreases which indicates poor key generation at a higher value of β. This happens mainly due to the increase in fading parameter that introduces fluctuations in the channel conditions, which can impact the $\mathcal{K}_G$ by influencing the quality of the received signal and the reliability of communication between the legitimate sender and receiver.

However, Fig. 5 (b) also highlights an increase in w_s notably maintains $\mathcal{K}_G$ performance. Since the w_o between consecutive windows used for key generation isn't constant, fixing the w_o can lead to a degradation in the $\mathcal{K}_G$. These findings emphasize the constructive influence of w_o on key agreement within the proposed key generation approach.

C. THE IMPACT OF QUALIFYING EXCURSION LENGTH L ON WINDOW AVERAGING AT $\alpha = 1$ AND $\alpha = 3$

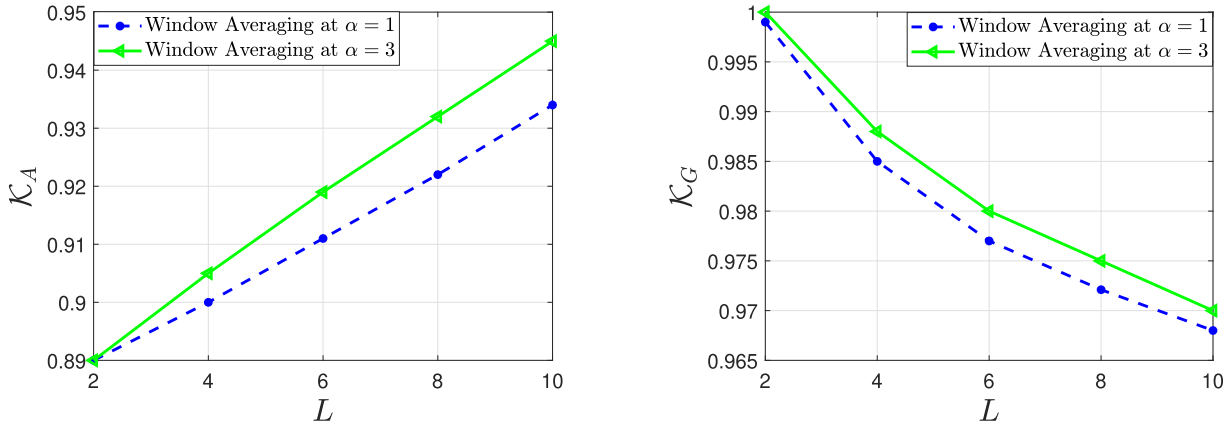
Fig. 6, illustrates how the change in L influences $\mathcal{K}_A$ and $\mathcal{K}_G$ performance of window averaging at $\alpha = 1$ and $\alpha = 3$. Fig. 6 (a), presents that the $\mathcal{K}_A$ performance at $\alpha = 1$ and $\alpha = 3$ increases as L increases, which is due to the key matching process at the information reconciliation stage. Because longer excursions enhance the probability that the same window mean will be used at both ends of the communication channel. Essentially, with more samples within the qualifying excursion, the likelihood of both parties identifying the same key sequence increases. However, at $\alpha = 3$ the system consistently demonstrates superior performance compared to the averaging at $\alpha = 1$.

Fig. 6 (b) illustrates the effect of L on $\mathcal{K}_G$ performance of window averaging at $\alpha = 1$ and $\alpha = 3$. Throughout the analysis, it has been observed that the $\mathcal{K}_G$ performance at $\alpha = 1$ and $\alpha = 3$ is decreasing as L increases due to the sample loss at the quantization stage. The samples are lost at the quantization stage because an increase in excursion length leads to a decrease in the number of bits available for key extraction. This, in turn, reduces the rate at which the system can generate secret keys. Nevertheless, the averaging at $\alpha = 3$ consistently exhibits superior performance compared to the averaging approach $\alpha = 1$. These results are obtained under specific channel shape parameters, with $\xi = 1$, $\upsilon = 1$, and



(a) (b)

FIGURE 5. The impact of β and w_s on $\mathcal{K}_A$ and $\mathcal{K}_G$ in (a) and (b), respectively. Other parameters are: $M = 2$, $L = 3$, $\alpha = 3$, $ws = 10$, $\rho = 80$, $\xi = 1$, and $\upsilon = 1$.



(a) $\mathcal{K}_A$ performance (b) $\mathcal{K}_G$ performance

FIGURE 6. The impact of excursion length L on $\mathcal{K}_A$ and $\mathcal{K}_G$ performance, respectively. Other parameters are: $M = 2$, $L = 3$, $w_s = 20$, $w_o = 5$, $\alpha = 3$, $\rho = 0.80$, $\xi = 1$, $\upsilon = 1$, and $\beta = 2$.

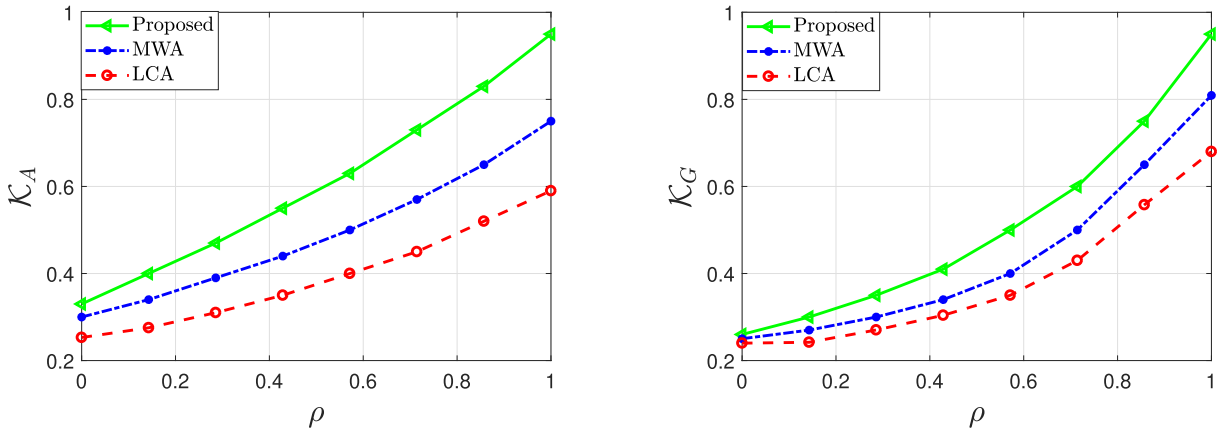
$\beta = 2$ and algorithm parameters are set as $M = 2$, $L = 3$, $w_s = 20$, $\alpha = 3$, $w_o = 5$, and $\rho = 0.80$.

D. THE PERFORMANCE ANALYSIS OF THE PROPOSED ALGORITHM WITH LEVEL-CROSSING ALGORITHM (LCA) AND MOVING WINDOW ALGORITHM (MWA)

In Fig. 7, we analyzed the performance of three key generation algorithms; level-crossing algorithm (LCA) [33], moving window algorithm (MWA) [36], and the proposed Gaussian-shaped moving window algorithm (G-MWA) for different values of ρ. LCA selects samples for key bits based on the level crossings in the signal's values. The MWA smooths the signal by calculating the average within a predefined straight-forward window that slides over the channel samples. The G-MWA is a sample importance-based SKG technique. It uses a sliding window weighted average, where the weights are based on a Gaussian distribution. The system and channel parameters are set as follows: $\xi = 2$, $\beta = 2$, $w_s = 20$, $w_o = 10$, and $L = 5$. Fig. 7 (a) demonstrates that as the value of ρ decreases, the corresponding value of key agreement also decreases which indicates poor $\mathcal{K}_A$ at lower values of ρ and better key agreement at higher values of ρ. During the analysis, it was observed that the $\mathcal{K}_A$ performance of the LCA is poor as compared to MWA and G-MWA. But G-MWA performance consistently outperforms LCA and, MWA.

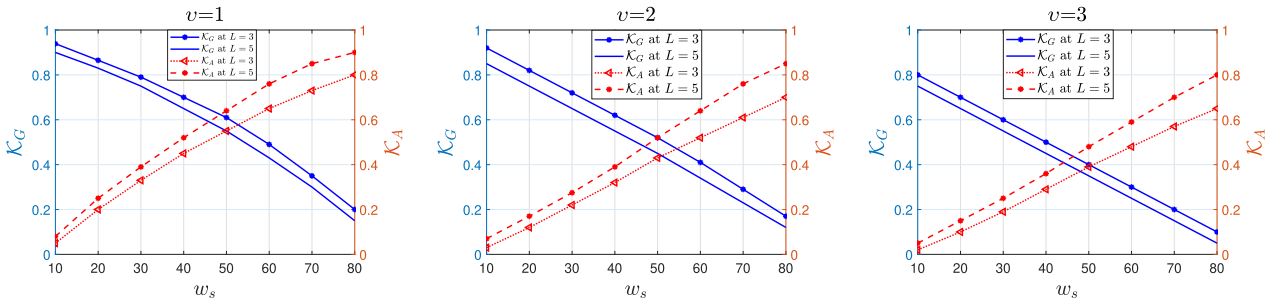
Moreover, in Fig. 7 (b) it has been observed that as ρ increases, the $\mathcal{K}_G$ of all three schemes seem to increase. This trend is because higher values of ρ indicate more identical channels at the legitimate end, which improves $\mathcal{K}_G$ performance, particularly, due to the better matching at the information reconciliation stage.

As evident from Fig. 7 the $\mathcal{K}_G$ of LCA is significantly lower than the other two algorithms. However, $\mathcal{K}_G$ of MWA, and $\mathcal{K}_G$ of G-MWA schemes exhibit comparable results. Nevertheless, the G-MWA scheme offers a superior performance trade-off between $\mathcal{K}_G$ for all values of ρ. This approach minimizes the issue of mismatched excursion loss,



(a) $\mathcal{K}_A$ performance (b) $\mathcal{K}_G$ performance

FIGURE 7. The performance comparison of Proposed SKG algorithm with MWA and LCA. System and channel parameters are: $w_s = 20$, $w_o = 10$, $L = 5$, $\xi = 2$, $\beta = 2$, and $\upsilon = 1$.



(a) (b) (c)

FIGURE 8. Performance comparison at different υ and other parameters are: $\xi = 1$, $L = 3$, $\beta = 2$, $M = 2$, $alpha = 3$, $w_o = 5$, and $\rho = 0.80$.

unlike the other two algorithms, resulting in more reliable and secure key generation.

E. THE IMPACT OF υ ON $\mathcal{K}_G$ AND $\mathcal{K}_A$ PERFORMANCE

Fig. 8 illustrates the impact of distribution variance *upsilon*, window size w_s, and excursion length L on $\mathcal{K}_G$ and $\mathcal{K}_A$ Performance. The experiment is conducted for the parameters set as follows: $\xi = 1$, $\beta = 2$, $M = 2$, $w_o = 5$, and $\rho = 0.80$.

In Fig. 8 (a), (b), and (c), it is evident that as L increases, there is a corresponding decrease in $\mathcal{K}_G$ This occurs because of the loss of channel samples during the smoothing process. However, the increase in L causes to improvement in $\mathcal{K}_A$ which is mainly due to the same samples matching at the information reconciliation stage. Therefore, it's crucial to carefully select the optimal L for a given fading environment to achieve a balanced performance trade-off between $\mathcal{K}_G$ and $\mathcal{K}_A$.

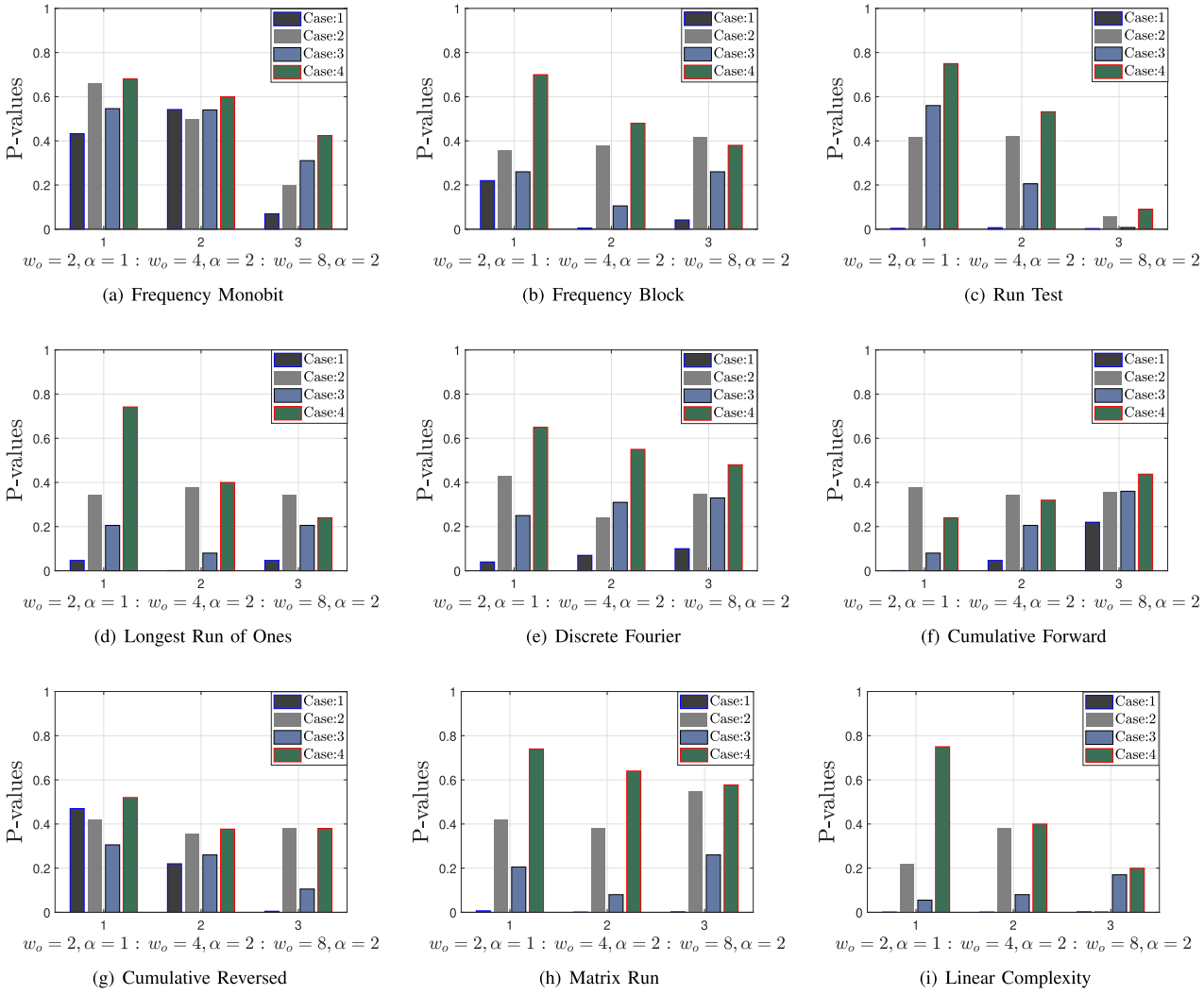
Moreover, it is evident from the Fig. 8 that the increase in υ leads to a degradation in both $\mathcal{K}_G$ and $\mathcal{K}_A$ performance.

Furthermore, it's noticeable in Fig. 8 (b) and Fig. 8 (c) that the $\mathcal{K}_G$ and $\mathcal{K}_A$ performance deteriorates faster compared to Fig. 8 (a). This is because, for secure communication, two parties need to agree on a common secret key. When keys are clustered (low variance), it's easier for both parties to land on a close enough value through the key agreement protocol. But when keys are spread out (high variance), it's statistically less likely that both parties will pick close enough values.

F. KRR PERFORMANCE ANALYSIS

Due to the inherent complexity of randomness assessment, a single metric proves insufficient. This analysis leverages the National Institute of Standards and Technology (NIST) test suite [37], a collection of well-established statistical tests, to investigate the KRR of the proposed scheme effectively.

In this subsection, We analyzed the key randomness performance of the proposed technique by employing nine NIST statistical test suites namely: Frequency Monobit Test, Frequency Block Test, Run Test, Longest Run of ones Test, Discreate Fourier Transform Test, Cumulative Forward Test, Cumulative Reversed Test, Matrix Rank Test, Linear Complexity Test, respectively as shown in Fig. 9. Table 2 provides a visual representation of the P-values corresponding to each conducted randomness test. It's notable that as the w_o increases, there is a decrease in the randomness of the generated key bits. This reduction in randomness is attributed to the considerable overlap observed between adjacent windows, resulting in the appearance of similar and correlated samples. An optimal trade-off among



(a) Frequency Monobit (b) Frequency Block (c) Run Test

(d) Longest Run of Ones (e) Discrete Fourier (f) Cumulative Forward

(g) Cumulative Reversed (h) Matrix Run (i) Linear Complexity

FIGURE 9. KRR performance.

TABLE 2. Impact of window overlap size w_0 on KRR performance.

Test Name	P-value at w_o=0	P-value at w_o=5	P-value at w_o=8
Frequency Monobit Test	0.94	0.86	0.73
Frequency Block Test	0.77	0.72	0.56
Run Test	0.75	0.67	0.59
Longest Run of Ones	0.55	0.53	0.44
Discrete Fourier Transform	0.65	0.60	0.48
Cumulative Forward Test	0.58	0.55	0.35
Cumulative Reversed Test	0.85	0.78	0.28
Matrix Rank Test	0.92	0.89	0.54
Linear Complexity Test	0.8	0.7	0.6

KRR, KGR, and KAR is observed at a 50% window overlap setting. Additionally, Fig. 9 (a)-(i) display a performance analysis of KRR, focusing on four different scenarios related to key randomness. In the first case, simple mean-based thresholding is performed to extract the secret key. In the second case, both sample importance-based thresholding and sample averaging are employed. In the third case, Gaussian window-based thresholding is utilized without considering sample importance. Finally, in the fourth case, both sample importance and Gaussian window-based thresholding are combined to extract the key. It's noted that the fourth scenario demonstrates superior randomness compared to the other cases.

V. CONCLUSION

A novel SKG algorithm has been proposed in this study, focusing on the pre-processing and quantization stages of the generic SKG model for independent symmetric key

generation at the legitimate communication nodes. Our SKG algorithm has employed biasing of selective channel samples that has a higher likelihood of falling in the same quantization interval on the legitimate nodes, followed by weighted averaging with a sliding window to transform the original channel samples into smooth channel samples. This transformation has been combined with non-uniform quantization that employ non-contiguous definition of the quantization intervals for secret key bits extraction, ensuring high key randomness, generation rate, and agreement in the extracted key. A thorough performance analysis and comparison of our scheme with notable existing SKG schemes have been conducted, establishing the validity and superior performance of our scheme compared to its counterparts.

REFERENCES

[1] 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.

[2] A. K. Tyagi, G. Rekha, and N. Sreenath, "Beyond the hype: Internet of Things concepts, security and privacy concerns," in *Proc. Int. Conf. E-Business Telecommun. Adv. Decis. Sci., Image Process., Secur. Comput. Vis. (ICETE)*, vol. 1. Springer, 2020, pp. 393–407.

[3] L. Chen, Z. Chen, T. Lu, and A. Hu, "A physical layer key generation scheme based on deep learning compensation and balanced vector quantization," *Secur. Commun. Netw.*, vol. 2023, no. 1, 2023, Art. no. 4911338.

[4] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci. USA*, vol. 114, no. 1, pp. 19–26, 2017.

[5] M. Bottarelli, G. Epiphaniou, D. K. B. Ismail, P. Karadimas, and H. Al-Khateeb, "Physical characteristics of wireless communication channels for secret key establishment: A survey of the research," *Comput. Secur.*, vol. 78, pp. 454–476, Sep. 2018.

[6] Z. Rezki, M. Zorgui, B. Alomair, and M.-S. Alouini, "Secret key agreement: Fundamental limits and practical challenges," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 72–79, Jun. 2017.

[7] J. Wang, K. Lounis, and M. Zulkernine, "CSKES: A context-based secure keyless entry system," in *Proc. IEEE 43rd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 1, Jul. 2019, pp. 817–822.

[8] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The impact of quantum computing on present cryptography," 2018, *arXiv:1804.00200*.

[9] X. Chen, C. Wu, Z. Liu, N. Zhang, and Y. Ji, "Computation offloading in beyond 5G networks: A distributed learning framework and applications," *IEEE Wireless Commun.*, vol. 28, no. 2, pp. 56–62, Apr. 2021.

[10] M. Adil, S. Wyne, and S. J. Nawaz, "On quantization for secret key generation from wireless channel samples," *IEEE Access*, vol. 9, pp. 21653–21668, 2021.

[11] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[12] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Trans. Commun.*, vol. 43, no. 1, pp. 3–6, Jan. 1995.

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

[14] 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.

[15] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 3048–3056.

[16] G. Li, A. Hu, J. Zhang, L. Peng, C. Sun, and D. Cao, "High-agreement uncorrelated secret key generation based on principal component analysis preprocessing," *IEEE Trans. Commun.*, vol. 66, no. 7, pp. 3022–3034, Jul. 2018.

[17] S. Zhang, L. Jin, Y. Lou, K. Huang, and Z. Zhong, "High-rate secret key generation method using two-way random signal," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery (CyberC)*, Oct. 2018, pp. 32–324.

[18] Z. Wei and W. Guo, "Random matrix based physical layer secret key generation in static channels," 2021, *arXiv:2110.12785*.

[19] S. J. Nawaz, M. Adil, and S. Wyne, "Average contiguous duration—A novel metric for characterizing wireless fading channels," *IEEE Wireless Commun. Lett.*, vol. 10, no. 8, pp. 1790–1794, Aug. 2021.

[20] M. Adil, S. Wyne, S. J. Nawaz, and B. Muhammad, "Average contiguous duration (ACD)-based quantization for secret key generation in generalized gamma fading channels," *IEEE Access*, vol. 9, pp. 110435–110450, 2021.

[21] S. Abdolinezhad, L. Zimmermann, and A. Sikora, "A novel key generation method for group-based physically unclonable function designs," *Electronics*, vol. 10, no. 21, p. 2597, Oct. 2021.

[22] T. Assaf, A. Al-Dweik, Y. Iraqi, S. Jangsher, A. Pandey, J.-P. Giacalone, E. E. Abulibdeh, H. Saleh, and B. Mohammad, "High-rate secret key generation using physical layer security and physical unclonable functions," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 209–225, 2023.

[23] D. V. Linh and V. V. Yem, "Key generation technique based on channel characteristics for MIMO-OFDM wireless communication systems," *IEEE Access*, vol. 11, pp. 7309–7319, 2023.

[24] G. Li, A. Hu, C. Sun, and J. Zhang, "Constructing reciprocal channel coefficients for secret key generation in FDD systems," *IEEE Commun. Lett.*, vol. 22, no. 12, pp. 2487–2490, Dec. 2018.

[25] H. Samimi, "Performance analysis of lognormally shadowed generalized gamma fading channels," *Int. J. Commun. Syst.*, vol. 24, no. 1, pp. 14–26, Jan. 2011.

[26] F. Qi, "Bounds for the ratio of two gamma functions," *J. Inequalities Appl.*, vol. 2010, pp. 1–84, Dec. 2010.

[27] M. A. Chaudhry and S. M. Zubair, "Generalized incomplete gamma functions with applications," *J. Comput. Appl. Math.*, vol. 55, no. 1, pp. 99–124, Oct. 1994.

[28] D. Harville, "Extension of the Gauss-Markov theorem to include the estimation of random effects," *Ann. Statist.*, vol. 4, no. 2, pp. 384–395, 1976.

[29] F. Chatelain, J.-Y. Tourneret, J. Inglada, and A. Ferrari, "Bivariate gamma distributions for image registration and change detection," *IEEE Trans. Image Process.*, vol. 16, no. 7, pp. 1796–1806, Jul. 2007.

[30] A. Gil, J. Segura, and N. M. Temme, "The asymptotic and numerical inversion of the Marcum Q-function," *Stud. Appl. Math.*, vol. 133, no. 2, pp. 257–278, Aug. 2014.

[31] M. Z. Bocus, C. P. Dettmann, and J. P. Coon, "An approximation of the first order Marcum Q-function with application to network connectivity analysis," *IEEE Commun. Lett.*, vol. 17, no. 3, pp. 499–502, Mar. 2013.

[32] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Secret key extraction from level crossings over unauthenticated wireless channels," in *Securing Wireless Communications at the Physical Layer*. Boston, MA, USA: Springer, 2009, pp. 201–230.

[33] 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.

[34] D. P. Bertsekas and J. N. Tsitsiklis, *Introduction to Probability*. Nashua, NH, USA: Athena Scientific, 2008.

[35] K. Marton and A. Suciu, "On the interpretation of results from the NIST statistical test suite," *Sci. Technol.*, vol. 18, no. 1, pp. 18–32, 2015.

[36] A. Badawy, T. Elfouly, T. Khattab, A. Mohamed, and M. Guizani, "Unleashing the secure potential of the wireless physical layer: Secret key generation methods," *Phys. Commun.*, vol. 19, pp. 1–10, Jun. 2016.

[37] J. Zaman and R. Ghosh, "Review on fifteen statistical tests proposed by NIST," *J. Theor. Phys. Cryptogr.*, vol. 1, pp. 18–31, Nov. 2012.

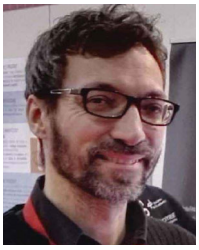
GHALIB HUSSAIN received the master's degree in electrical engineering from the Department of Electrical Engineering, Capital University of Science and Technology (CUST), Islamabad, Pakistan, in 2019. He is currently pursuing the Ph.D. degree in electrical engineering with COMSATS University Islamabad (CUI). His current research interests include optimization of wireless communications, 6G communications, signal processing, and physical layer security.

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

Since September 2005, he has been working on several research and teaching positions with COMSATS University Islamabad (CUI), Islamabad, Pakistan; University of Rome Tor Vergata, Italy; Staffordshire University, U.K.; Federal Urdu University, Pakistan; The University of York, U.K.; and Aristotle University of Thessaloniki, Greece. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, 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, airborne internet, physical layer security, the Internet of Things, localization, and vehicle-to-vehicle communications.

SHURJEEL WYNE (Senior Member, IEEE) received the Ph.D. degree from Lund University, Sweden, in March 2009. Between April 2009 and 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 is currently 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.

ERNESTINA CIANCA (Member, IEEE) was employed by Aalborg University, Denmark, as a Research Engineer, from 2000 to 2001, and an Assistant Professor with the Wireless Networking Group (WING), from 2001 to 2003. She was an Assistant Professor with the University of Rome "Tor Vergata," from 2003 to 2019, where she is currently an Associate Professor with the Department of Electronics Engineering. She teaches: the Internet of Things-principles and applications, digital communications, and internet delle cose with the University of Rome "Tor Vergata." She is also the Director of the Master Program in Engineering and International Space Law in Communication, Navigation, and Sensing via Satellite. She is also the Vice-Director of the Interdepartmental Research Center and the Center for TeleInFrastructures (CTIF), University of Rome "Tor Vergata." She is the author of more than 150 papers published in international journals and conference proceedings. She has participated in several European and national projects. She has been responsible for the University of Rome "Tor Vergata" activities in the several Italian Space Agency and ESA Projects.



MAURO DE SANCTIS received the Ph.D. degree in telecommunications and microelectronics engineering from the University of Rome "Tor Vergata," Italy, in 2006.

From January 2004 to December 2005, he was involved in the My Personal Adaptive Global NET (MAGNET) European FP6 Integrated Project and the SatNEx European Network of Excellence. In 2006, he was a Postdoctoral Research Fellow with European Space Agency (ESA) ARIADNA extended study named "The Flower Constellation Set and its Possible Applications." From January 2006 to June 2008, he was involved in the MAGNET Beyond European FP6 Integrated Project as scientific responsible for the WP on Coexistence of Radio Interfaces. He was with Italian Space Agency (ASI) as a Holder of a two-year research scholarship on the study of Q/V band satellite communication links for a technology demonstration payload, which concluded, in 2008, during this period he participated in the opening and the first trials of the ASI Concurrent Engineering Facility (ASI-CEF). Since 2008, he has been an Assistant Professor with the Department of Electronics Engineering, University of Rome "Tor Vergata." In 2009, he was involved in the ESA Project on Multipurpose Constellation. From 2010 to 2011, he was involved in the ESA Project Telemedicine Services for Health (TESHEALTH). He is currently an Associate Professor in telecommunications with the Department of Electronics Engineering, University of Rome "Tor Vergata," teaching information theory and data science. He is also a Founder Member with the University Spin-Off RadioPoints s.r.l. He has published more than 130 papers in journals and conference proceedings, seven book chapters, one book, and one patent. His main research interests include wireless terrestrial and satellite communication networks, wireless localization and sensing, data science, and information theory. He was a co-recipient of the Best Paper Awards from the 2009 International Conference on Advances in Satellite and Space Communications (SPACOMM 2009) and the 2022 International Symposium on Wireless Personal Multimedia Communications (WPMC 2022). He is serving as an Associate Editor for the Command, Control, and Communications Systems Area for IEEE TRANSACTIONS ON AEROSPACE AND ELECTRONIC SYSTEMS and the Signal Processing and Communication Area for *IEEE Aerospace and Electronic Systems Magazine*.

Open Access funding provided by 'Università degli Studi di Roma "Tor Vergata"' within the CRUI CARE Agreement