IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Performance of RIS-secured Short-Packet NOMA Systems with Discrete Phase-Shifter to Protect Digital Content and Copyright against Untrusted User

SANG Q. NGUYEN[1], HYE-YOUNG KIM[2], TAN N. NGUYEN[3,6] (Member, IEEE), BUI VU MINH[4], PHUONG T. TRAN[5] (Senior Member, IEEE), TRAN TRUNG DUY[1], BYUNG-SEO KIM[2], and MIROSLAV VOZNAK[6] (Senior Member, IEEE)

[1]Posts and Telecommunications Institute of Technology, Ho Chi Minh City 70000, Vietnam
[2]School of Games/Game Software, Hongik University, 2639 Sejong-ro, Sejong-si, 30016, Korea
[3]Communications and Signal Processing Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City 70000, Vietnam
[4]Faculty of Engineering and Technology, Nguyen Tat Thanh University, Ho Chi Minh City 754000, Vietnam
[5]Wireless Communications Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City 70000, Vietnam
[6]Faculty of Electrical Engineering and Computer Science, VSB-Technical University of Ostrava, 17. listopadu 2172/15, 70800, Ostrava, Czechia

Corresponding author: Phuong T. Tran (tranthanhphuong@tdtu.edu.vn).

This research is funded by the European Union within the REFRESH project - Research Excellence For Region Sustainability and High-tech Industries ID No. CZ.10.03.01/00/22_003/0000048 of the European Just Transition Fund and by the Ministry of Education, Youth and Sports of the Czech Republic (MEYS CZ) through the project SGS ID No. SP2025/013 conducted by VSB - Technical University of Ostrava. This research was supported by Culture, Sports and Tourism R&D Program through the Korea Creative Content Agency grant funded by the Ministry of Culture, Sports and Tourism in 2024 (Project name: Global Talent Training Program for Copyright Management Technology in Game Contents, Project Number: RS-2024-00396709, Contribution rate: 80%.

ABSTRACT Future wireless communications are expected to serve a wide range of emerging applications, such as Online Gaming, Extended Reality (XR), Metaverses, Healthcare or Telemetry, where communication from diverse connected Internet of Things (IoT) devices require not only stringent conditions such as ultra-reliability and low-latency communication (URLLC) together with high bandwidth but also concerns about content security as well as copyright protection. To deal with URLLC demands, ShortPacket Communication (SPC) has been recently considered a vital solution. Meanwhile, to meet high spectrum utilization, Non-Orthogonal Multiple Access (NOMA) has emerged as a potential technology in the last decade, for its ability to serve multi-user communication simultaneously by exploiting powerdomain rather than time or frequency domains. Especially, incorporating Reconfigurable Intelligent Surfaces (RIS) with NOMA/SPC-based systems can further boost the system's spectral efficiency as well as enhance communication coverage. However, NOMA-based systems hugely demand a reliable user-paring process, which imposes challenges in ensuring secure short-packet delivery for emerging IoT applications. Hence, this paper studies downlink RIS-assisted short-packet NOMA systems with the focus of improving the secure performance of the pairing process with untrusted users. Our study contributes a new strategy for arbitrary paring users by designing a joint power allocation policy and RIS's phase shifter, where untrustworthy users will be allocated with higher power levels while trustworthy users will be configured with sub-optimal phase shift criterion at RIS to maximize its cascaded channel gain. Besides, we also derive closed-form expressions for the average block-error rate (BLER) to analyze the performance of trustworthy users as well as the average secure BLER to quantify the secure performance when untrustworthy users wiretap trustworthy users' information using successive interference mechanisms. Moreover, we further develop asymptotic expressions for both cases to measure the diversity gain and induce key parameters. Subsequently, Monte Carlo simulations are provided as a benchmark to corroborate the theoretical findings. This work can be used as a copyright protection technique for digital content such as games.

INDEX TERMS Content security, copyright protection, error phase-shift, non-orthogonal multiple access, untrusted user, short-packet communication, physical security layer.

I. INTRODUCTION

A. BACKGROUND AND CONCERNS

Next-generation wireless communication systems are expected to be established not only to connect with mobile devices but also with various Internet of Things (IoT) devices to meet emerging applications such as Online Gaming, Extended Reality (XR), Metaverses, Healthcare or Telemetry [1]. Beyond demands of high throughput and improved spectral efficiency in response to these applications, the sixth generation (6G) also requires wireless infrastructure to have advanced ultra-reliability and low-latency communication (URLLC) features [2], where the communication reliability must touch 99.99% and the transmission latency should be preserved within one millisecond. Besides, the openness and broadcast nature of the wireless transmission medium, particularly interactions of diverse IoT domains with the contingent on short-packet delivery, also renders more and more security flaws that potential attackers can exploit to compromise wireless information transmission [3]. On the one hand, this is because IoT devices are often designed with limitations in computing power, processing power, and resilience [4], making their data transmission vulnerable to malicious attacks. On the other hand, traditional physical layer security methods, which rely on the native features of the wireless channel to reduce the eavesdropper's ability to decrypt without requiring complex computation and encryption in the upper layer [5], are mainly based on the theory of secrecy capacity constructed by infinite blocklength coding to ensure perfect secure probability [6]. Therefore, this probability is no longer ensured when packet delivery is used in short form. Therefore, it is urgent to develop technologies that can effectively support large-scale connectivity, achieve URLLC conditions, and improve physical layer security performance.

To meet the growth of IoT devices daily, a pivotal technique that has attracted widespread attention in recent years and promises to improve spectrum utilization and achieve massive connectivity is Non-Orthogonal Multiplexed Access (NOMA) [7, 8, 9]. NOMA facilitates the goal of simultaneous multi-user communication in the same time and frequency resources by encoding user signals in the power domain, where distant users with weaker channel conditions will be allocated with higher power allocation levels than proximate users [10, 11]. Hence, successive interference cancellation (SIC) mechanisms are used at the receiver to decode signals in descending order of power levels. However, as the number of NOMA users increases, the computational complexity of processing SIC also increases [12]. Several user pairing strategies have been, therefore, introduced in the literature [13, 14, 15]. Unfortunately, such a tedious task is highly dominated by distinguishing user channel gains, and wireless communication services are not always preferred for this process. Therefore, another thought of NOMA adoption has been introduced in [16, 17, 18], where pairing users are ordered according to priorities of quality of service demands.

In response to the stringent requirements of URLLC, a promising technique that holds promise for achieving physical transmission with reduced latency is Short-Packet Communication (SPC) [2, 19]. The popularity of SPC is laid by the foundation of a new theory, namely channel coding rate in the finite blocklength regime, developed by Polyanskiy in 2010 [20]. This theory provides a new way of capturing the relation between the number of transmitted information bits, packet length, and block-error rate (BLER) under the received signal-to-noise ratio (SNR). Based on this breakthrough, several studies on the performance of SPC systems have been outlined in the literature from diverse perspectives, for example, multi-hop multi-input multi-output relaying networks [21], multi-hop relaying networks with imperfect channel state information [22], dual-hop relaying networks with optimal resource power allocation [23], cognitive short-packet radio [24], hybrid long-short packet [25], uplink cooperative spectrum sharing [26], and cooperative cellular-IoT networking [27].

On another front, Reconfigurable Intelligent Surfaces (RIS) have emerged as a potential technology to mitigate some of the security risks [28]. Architecturally, RIS consist of square or rectangular arrays of multiple passive programmable components and low-cost implementations, and each component can be controlled by changing the current in an electronic magnetic field using a transistor or photodiode circuit to modify the amplitude and phase of the incoming signal [29]. This has been confirmed via several investigations of RIS-based systems, such as ambient backscatter [30], hardware impairments [31], RIS with imperfect channel estimation [32], cooperative RIS communications [33], and millimeter-wave communication [34], multiple aerial RIS [35], wireless power transfer [36], RIS-assisted two-way communication [37], and energy/rate-reliability trade-offs [38]. Another example is the RIS-based system with SPC and NOMA [39, 40, 41]. Akin to this feature, properly configuring the phase shift of each RIS element according to the legitimate destination can maximize the gap between the legitimate channel and the wiretap ones, thereby enhancing secure performance [42].

B. LITERATURE REVIEW AND MOTIVATION

In terms of SPC-secured systems, the authors in [43] have initialized a theoretic-information framework for evaluating the secure BLER of SPC communication based on the conception of finite blocklength regime theory in [20]. Inspired by this, the work in [44] presented closed-form approximations for the security throughput to quantify the performance of an IoT system with a multi-antenna eavesdropper, revealing how packet length impacts the latency-reliability trade-off under security constraints. In [45], the authors established mathematical frameworks for outage probability and effective throughput evaluations in a way that can ensure security and reliability simultaneously. The work in [46] outlined a comprehensive performance evaluation of with and without channel estimation errors at the eavesdropper and/or legitimate node on the secure transmission rates of SPC. Meanwhile, the performance of multiple eavesdroppers with colluding cooperation was put forward in [47]. In [48], a novel transmission scheme was developed to guarantee the freshness and security of unmanned aerial vehicle-secured data collection systems. In [49], the non-convexity problem of optimizing packet length to maximize the total secrecy throughput subject to the BLER tolerance was formulated and addressed using the block coordinate descent method. In [50], a diamond relay network was proposed to simultaneously guarantee the object of reliability and secrecy. In [51], the authors designed a cooperative jamming scheme to improve the secure performance of multi-hop SPC systems.

Aside from the security issue of SPC-based systems, research on SPC-secured NOMA transmission has also received considerable interest. For instance, the work in [52] proposed a NOMA pairing scheme between delay-sensitive users and security-required users, where a set of closed-form expressions of the connection and secrecy outage probabilities and effective secrecy throughput were calculated under Nakagami-m channels. Besides, to achieve more insights into system performance, the security-reliability/-efficiency tradeoff was also established. Meanwhile, the work in [53] examined the secure performance of a short-packet NOMA system in flat Rayleigh fading channels when cell-edge users become untrusted users. Differently, the work in [54] studied the secrecy energy efficiency of short-packet NOMA transmission for massive machine-type communication, where the problem of implementing joint relay and dynamic power level selection is formulated and solved by a stateless decentralized Q-learning-based multi-agent reinforcement learning algorithm. In [55], the authors proposed a joint power allocation and beamforming design to tackle challenges in NOMA user pairing with the presence of untrusted near users. In [56], the author studied the security performance of control information during short packet transmission from ground to air in the presence of either an untrusted internal unmanned aerial vehicle (UAV) or an external flying eavesdropper. Likewise, the authors in [57] designed a UAV-based security scheme to meet diverse requirements of user cases, including joint privacy and low latency and joint reliability and low latency requirements. Through the stochastic geometry method, closed-form expressions for static and dynamic UAVs are exploited as the key to infer the security rate.

Similarly, research on SPC-secured RIS has received early attention from the research community. For example, the work in [58] developed multiple legitimate user selection schemes to combat the surveillant of an eavesdropper with and without finite-blocklength transmissions. Compared to a relay-based system with decode-and-forward protocols, exploiting RIS can remarkably improve legitimate performance while degrading the same for eavesdroppers. In [59], the authors proposed to solve the problem of spectrum resource shortage caused by massive machine-type communication devices as well as improve eavesdropping resistance, where the achievable sum secrecy capacity is maximized by jointly RIS phase coefficient, optimizing the transmission power, and receive beamforming design. In [60], a finite block-length coding scheme was proposed for the RIS-aided single-input multiple-output channels that are capable of securing themselves when the block length is greater than a certain threshold. Later, this scheme was extended for multiple-input multiple-output/MIMO channels [61]. In [62], a novel Riemannian conjugate gradient-based joint optimization algorithm was proposed to maximize the secrecy transmission rate by jointly optimizing blocklength, beamforming and RIS phase shift under constraints of resource-limited, unit modulus, and unit norm.

C. NOVELTY AND CONTRIBUTIONS

From the above discussion, research on SPC has been individually investigated with NOMA [52, 53, 54, 55, 56, 57] or RIS [58, 59, 60, 61, 62], whereas the investigation on RIS-secured short-packet NOMA remains open, to the best of the authors' knowledge. Therefore, this study seeks to bridge the research gap by exploring the performance of RIS-secured short-packet NOMA systems, where the source node proceeds with the pairing process but encounters a pair of trustworthy and untrustworthy users. Instead of renewing this process which disrupts the service demands of trustworthy users as well as results in wasted resources and even some additional tasks, we aim to overcome such concerns by developing an effective strategy to not only ensure the quality of service (QoS) demands of untrustworthy users but also increase the secure performance of trustworthy users even if untrustworthy users becomes an internal eavesdropper. Based on this, we intend to intelligently exploit RIS functionality combined with modifying orders of NOMA encoding without raising any extra complexity to IoT systems. As such, RIS-based short-packet NOMA systems can partially reduce the risks of pairing untrustworthy users with trustworthy users. The main contributions of this work can be concisely described as follows:

1) An efficient secure communication protocol is introduced, intelligently exploiting the unique feature of RIS operation and NOMA encoding mechanisms. Specifically, untrustworthy users will be allocated with a higher power allocation (PA) coefficient than trustworthy users. Meanwhile, trustworthy users will be prioritized to enhance its channel gains by configuring RIS phase shifters. As such, we can achieve the goal of killing two birds with one stone. The first goal is to bypass the concerns who is proximate or distant users. The second goal is to enhance the performance of trustworthy users while ensuring the minimal quality of service demands of untrustworthy users. This feature will help pair NOMA users' processes to more simple, removing ordering tasks for users according to channel gains and focusing more on quality of service demands.
2) Focusing on the RIS-secured short-packet NOMA system with limited hardware implementation, particularly RIS's phase-shifter, we consider the use of a discrete phase-shift model in the development of RIS, along with the operation of the system under

Nakagami-m fading environments. Accordingly, we analyze the performance of short-packet transmission for both trustworthy and untrustworthy users by deriving closed-form expressions for the average BLER. Besides, we also carry out an analysis of the average BLER asymptotic, which helps us gain useful insights into user diversity order and short-packet designs.

3) To characterize how the PLS performance brought by the proposed scheme above with the worst-case scenario where the untrustworthy users perform SIC to wiretap trustworthy users' information, we further quantify the secure performance by deriving the End-to-End average secure BLER of eavesdropping this secured information. To have more useful information on the impacts of key system parameters on the secure performance floor, we also analyze the average secure BLER asymptotic.
4) Extensive simulation results based on the Monte Carlo method are provided to verify the theoretically developed BLER framework and collect valuable technical insights. Besides, we also present several investigations on varying settings of the PA coefficient, the number of RIS elements, the number of resolution bits used for RIS's phase shifter, the number of information data streams, packet length, and leakage information probability.

D. STRUCTURE AND NOTATION

The remainder of the paper is organized as follows. Section II describes the model consideration. Section III presents details of the methodology and the analysis of the system performance. Next, we show representative numerical results of investigating various use cases in Section III. Finally, Section III concludes the paper with key findings.

Notation: In this paper, we use boldface letters to denote boldface letters and italicized letters to present italicized letters. The notation $F_X(x)$ and $f_X(x)$ represents the CDF and PDF of random variable x. $\Pr[\bullet]$ and $\mathbb{E}\{\bullet\}$ denote the probability and expectation operators, respectively.

II. SYSTEM MODEL

A. MODEL DESCRIPTION

As depicted in Fig. 1, we considered an RIS-secured NOMA system, where a source - Sam (S) - employs a finite channel coding scheme with L channel uses (or packet length) to convey a short data amount of n_{B} information bits for a trustworthy user - Bob (B) - and n_{W} information bits for an untrustworthy user - Willie (W) - through the aid of one RIS (R) having K programmable elements, indexed by $k = 1, 2, ..., K$, due to blocked direct links. In this study, we only consider the secure performance of a user pair since the characteristics of other groups assisted by RIS are similar. Note that in the context of a user pair without an untrustworthy node, one user with lower quality of service demands will be regarded similarly to an untrustworthy user and the other with higher priority will be seen as a trustworthy user.

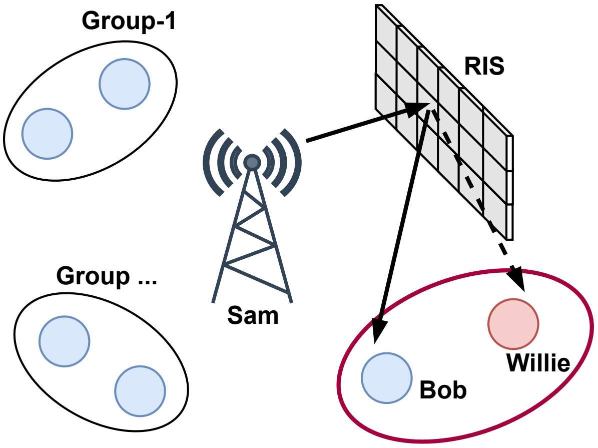

Fig. 1: Illustration of the considered model.

For the sake of notation, we denote $\boldsymbol{h}_{\mathsf{SR}} \in \mathbb{C}^{1\times K}$ and $\boldsymbol{h}_{\mathsf{RX}} \in \mathbb{C}^{K\times 1}$ by the channel vectors from source to RIS and from RIS to node $\mathsf{X} \in \{\mathsf{W}, \mathsf{B}\}$, respectively. Moreover, the diagonal matrix $\mathbf{\Phi} \in \mathbb{C}^{K\times K}$ at RIS can be expressed by

$$\mathbf{\Phi} = \mathrm{diag}(\exp(j\phi_1), ..., \exp(j\phi_k), ... \exp(j\phi_k)), \quad (1)$$

where $\phi_k \in (-\pi, \pi]$ is the k-th element's phase-shift.

To protect Bob's information from eavesdropping by Willie, enhance Bob's quality reception, and achieve simultaneous communication, we consider a joint design of NOMA power allocation (PA) and RIS phase-shifter control:

- **NOMA transmission**: The signal strength of Bob ($\sqrt{P\rho_{\mathsf{B}}}s_{\mathsf{B}}$) must be much lower than that of Willie ($\sqrt{P\rho_{\mathsf{W}}}s_{\mathsf{W}}$), where P is the source transmit power and ρ_{X} is the PA coefficient of symbols s_{X} of node X, with $\mathbb{E}\{|s_{\mathsf{X}}|^2\} = 1$. Accordingly, Sam will take a superimposed encoding signal as
$$x_{\mathrm{noma}} = \sqrt{P\rho_{\mathsf{W}}}s_{\mathsf{W}} + \sqrt{P\rho_{\mathsf{B}}}s_{\mathsf{B}}. \quad (2)$$
- **RIS phase-shifter control**: It is configured so that the cascaded channel from the source node to Bob (i.e., $g_{\mathsf{B}} = |\boldsymbol{h}_{\mathsf{SR}}\mathbf{\Phi}\boldsymbol{h}_{\mathsf{RB}}|^2 = |\sum_{k=1}^{K} h_{\mathsf{SR}}^k \exp(j\phi_k) h_{\mathsf{RB}}^k|^2)$ is maximized. However, it is often difficult to handle a phase shifter with a large number of RIS elements to maximize such a cascaded channel gain. Therefore, to reduce the hardware computational complexity, we consider the actual phase shift model as
$$\phi_k^\star = -\angle h_{\mathsf{SR}}^k - \angle h_{\mathsf{RB}}^k + \theta_k, \forall k = 1, 2, ...K, \quad (3)$$
where $\angle h$ is the phase of channel h and θ_k is the quantified phase-shift of the k-th elements, following uniform distribution model as $\mathcal{U}(-2^{-q}\pi, 2^{-q}\pi)$, with q being the number of resolution bits [63].

It is worth noting that such a consideration yields two advantages. First, Willie, an untrusted node, has sufficient power signal to decode its information. If he tries to wiretap Bob's information, there is no further way except the SIC process.

Second, Bob's cascaded channel gain is robust enough to perform SIC in descending power order.

To capture how the system works well with the considered joint NOMA PA and RIS's phase-shifter, we next turn to analyze the secure performance of the system in the worst-case scenario, where Willie applies SIC to eavesdrop on Bob's information and perfect channel state information is assumed to be available at the terminals. In this investigation, we assume that the system operates under Nakagami-*m* fading environments. Accordingly, the PDF of variable $Z \in \{h_{\mathsf{SR}}^k, h_{\mathsf{RX}}^k, \forall k = 1,2,...,K\}$ with shape $m \in \{m_{\mathsf{SR}}^k, m_{\mathsf{RX}}^k, \forall k = 1,2,...,K\}$ and scale $\Omega \in \{\Omega_{\mathsf{SR}}^k, \Omega_{\mathsf{RX}}^k, \forall k = 1,2,...,K\}$ can be given as

$$f_Z(z) = \frac{2m^m}{\Gamma(m)\Omega^m} z^{2m-1} \exp\left(-\frac{m}{\Omega}z^2\right). \tag{4}$$

From (4) and [64, Eq. (3.326.2)], the n-th moment of Z can be derived as

$$\mu_Z(n) = \mathbb{E}\{Z^n\} = \int_0^\infty z^n f_Z(z)dz = \frac{\Gamma\left(m + n/2\right)}{\Gamma(m)\left(m/\Omega\right)^{n/2}}. \tag{5}$$

B. DATA INFORMATION EXCHANGE

Based on the configured scheme, the signals received by node X will have the form

$$y_{\mathsf{X}} = \boldsymbol{h}_{\mathsf{SR}}\boldsymbol{\theta}\boldsymbol{h}_{\mathsf{RX}}x_{\text{noma}} + w_{\mathsf{X}}, \tag{6}$$

where w_{X} is the additive white Gaussian noises with zero mean and variance σ^2.

Following that, the signal-plus-interference-to-noise ratios (SINRs) achieved at node X to decode s_{W} and s_{B} via perfect SIC process can be respective expressed as

$$\gamma_{\mathsf{X}}^{s_{\mathsf{W}}} = \frac{\rho_{\mathsf{W}}\overline{\gamma}g_{\mathsf{X}}}{\rho_{\mathsf{B}}\overline{\gamma}g_{\mathsf{X}} + 1}, \tag{7}$$

$$\gamma_{\mathsf{X}}^{s_{\mathsf{B}}} = \rho_{\mathsf{B}}\overline{\gamma}g_{\mathsf{X}}, \tag{8}$$

where $\overline{\gamma} = P/\sigma^2$ is the average SNR and g_{X} is the short-notation of the cascaded channel gain at node X, with

$$g_{\mathsf{X}} = \begin{cases} \left|\boldsymbol{h}_{\mathsf{SR}}\boldsymbol{\theta}\boldsymbol{h}_{\mathsf{RB}}\right|^2, & \mathsf{X} = \mathsf{B}, \quad (9) \\ \left|\boldsymbol{h}_{\mathsf{SR}}\boldsymbol{\theta}\boldsymbol{h}_{\mathsf{RW}}\right|^2, & \mathsf{X} = \mathsf{W}. \quad (10) \end{cases}$$

From this formulation, we can see that it is necessary to find the CDF of the PDF of the RVs g_{X} to evaluate the system performance. Details are in the following.

Source-RIS-Bob Links: The PDF of g_{B} can be obtained akin to [63, Theorem 1] as

$$f_{g_{\mathsf{B}}}(x) = \frac{x^{\alpha_{\mathsf{B}}-1}}{\Gamma(\alpha_{\mathsf{B}})}\beta^{\alpha_{\mathsf{B}}} \exp(-\beta_{\mathsf{B}}x), \tag{11}$$

where

$$\alpha_{\mathsf{B}} = \frac{\left(\sum_{k=1}^K \mu_{h_{\mathsf{SR}}^k}(1)\mu_{h_{\mathsf{RB}}^k}(1)\mu_{\theta_k}(1)\right)^2}{4\sum_{k=1}^K \begin{pmatrix} \mu_{h_{\mathsf{SR}}^k}(2)\mu_{h_{\mathsf{RB}}^k}(2)(1+\mu_{\theta_k}(2))/2 \\ -[\mu_{h_{\mathsf{SR}}^k}(1)\mu_{h_{\mathsf{RB}}^k}(1)\mu_{\theta_k}(1)]^2 \end{pmatrix}}, \tag{12}$$

$$\beta_{\mathsf{B}} = \frac{1}{4\sum_{k=1}^K \begin{pmatrix} \mu_{h_{\mathsf{SR}}^k}(2)\mu_{h_{\mathsf{RB}}^k}(2)(1+\mu_{\theta_k}(2))/2 \\ -[\mu_{h_{\mathsf{SR}}^k}(1)\mu_{h_{\mathsf{RB}}^k}(1)\mu_{\theta_k}(1)]^2 \end{pmatrix}}, \tag{13}$$

$$\mu_{\theta_k}(n) = \frac{2^q}{n\pi}\sin(2^{-q}n\pi). \tag{14}$$

Using [64, eq. 3.351.2], the CDF of g_{B} can be derived as

$$F_{g_{\mathsf{B}}}(x) = \int_0^x f_{g_{\mathsf{B}}}(y)dy = 1 - \frac{1}{\Gamma(\alpha_{\mathsf{B}})}\Gamma(\alpha_{\mathsf{B}}, \beta_{\mathsf{B}}x). \tag{15}$$

Source-RIS-Willie Links: The PDF of g_{W} can be obtained akin to [32, Eq. (7)] as

$$f_{g_{\mathsf{W}}}(x) = \beta_{\mathsf{W}}\exp(-\beta_{\mathsf{W}}x), \tag{16}$$

where

$$\beta_{\mathsf{W}} = \frac{1}{\sum_{k=1}^K \Omega_{\mathsf{SR}}^k\Omega_{\mathsf{RW}}^k} = \frac{1}{K\overline{\Omega}_{\mathsf{SR}}\overline{\Omega}_{\mathsf{RW}}}. \tag{17}$$

Making use of [64, Eq. 3.351.2], the CDF of g_{W} can be derived as

$$F_{g_{\mathsf{W}}}(x) = \int_0^x f_{g_{\mathsf{W}}}(y)dy = 1 - \exp(-\beta_{\mathsf{W}}x). \tag{18}$$

III. PERFORMANCE EVALUATION FRAMEWORK

In this section, we will evaluate the secure performance of the considered system.

A. PRELIMINARIES

1) Average BLER of decoding s_{X}

For a short codeword of length L with the decoding error probability ϵ_{X} at node X, the maximal achievable rate of decoding s_{X} can be derived as in [20] as

$$r_{\mathsf{X}} = C(\gamma_{\mathsf{X}}^{s_{\mathsf{X}}}) - \sqrt{\frac{V(\gamma_{\mathsf{X}}^{s_{\mathsf{X}}})}{L}}Q^{-1}(\epsilon_{\mathsf{X}}), \tag{19}$$

where $C(x) = \log_2(1+x)$ is the Shannon capacity, $V(x) = [1-(1+x)^{-2}](\log_2(e))^2$ is the channel dispersion, $Q^{-1}(x)$ is the inverse of the Gaussian Q-function.

From (19), by letting $r_{\mathsf{X}} = n_{\mathsf{X}}/L$ the instantaneous BLER of s_{X} can be derived as

$$\epsilon_{\mathsf{X}}^{s_{\mathsf{X}}} = Q\left(\sqrt{\frac{L}{V(\gamma_{\mathsf{X}}^{s_{\mathsf{X}}})}}\left[C(\gamma_{\mathsf{X}}^{s_{\mathsf{X}}}) - n_{\mathsf{X}}/L\right]\right). \tag{20}$$

On this basis, the average BLER of decoding s_{X} can be derived as in [24] as

$$\overline{\epsilon}_{\mathsf{X}}^{s_{\mathsf{X}}} = \mathbb{E}\left\{\epsilon_{\mathsf{X}}^{s_{\mathsf{X}}}\right\} = \int_0^\infty \epsilon_{\mathsf{X}}^{s_{\mathsf{X}}} f_{\gamma_{\mathsf{X}}^{s_{\mathsf{X}}}}(x)dx = \xi_{\mathsf{X}}\sqrt{L}\int_{\zeta_{\mathsf{X}}}^{\delta_{\mathsf{X}}} F_{\gamma_{\mathsf{X}}^{s_{\mathsf{X}}}}(x)dx, \tag{21}$$

where $\xi_{\mathsf{X}} = [2\pi(2^{2r_{\mathsf{X}}}-1)]^{-1/2}$, $\zeta_{\mathsf{X}} = 2^{r_{\mathsf{X}}} - 1 - 1/(2\xi_{\mathsf{X}}\sqrt{L})$, and $\delta_{\mathsf{X}} = 2^{r_{\mathsf{X}}} - 1 + 1/(2\xi_{\mathsf{X}}\sqrt{L})$.

$$\Xi(x,y)=\frac{y}{\beta_{\mathsf{B}}}\mathcal{H}^{0,2;0,1;1,1}_{2,1;1,1;1,1}\left(\begin{matrix}(-\alpha_{\mathsf{B}};1,1),(0;1,1)\\(-1;1,1)\end{matrix}\middle|\begin{matrix}(1,1)\\(0;1)\end{matrix}\middle|\begin{matrix}(-1,1)\\(0,1)\end{matrix}\middle|\frac{y}{\beta_{\mathsf{B}}x};\rho_{\mathsf{B}}\frac{y}{\beta_{\mathsf{B}}}\right). \tag{28}$$

2) Average Secure BLER

For a short codeword of length L, the secure decoding error probability ε_{B} at Bob, and the information leakage probability Δ, the maximal secrecy rate for Bob can be derived as

$$r_{\mathsf{B}}=\begin{cases}\begin{matrix}C(\gamma_{\mathsf{B}}^{s_{\mathsf{B}}})-\sqrt{\frac{V(\gamma_{\mathsf{B}}^{s_{\mathsf{B}}})}{L}}Q^{-1}(\varepsilon_{\mathsf{B}})\\-C(\gamma_{\mathsf{W}}^{s_{\mathsf{B}}})-\sqrt{\frac{V(\gamma_{\mathsf{W}}^{s_{\mathsf{B}}})}{L}}Q^{-1}(\Delta)\end{matrix}, & \gamma_{\mathsf{B}}^{s_{\mathsf{B}}}>\gamma_{\mathsf{W}}^{x_{\mathsf{W}}},\\ 0, & \gamma_{\mathsf{B}}^{s_{\mathsf{B}}}\le\gamma_{\mathsf{W}}^{x_{\mathsf{W}}}.\end{cases} \tag{22}$$

From (22), by letting $r_{\mathsf{B}}=n_{\mathsf{B}}/L$ the instantaneous secure BLER of s_{B} can be derived as

$$\varepsilon_{\mathsf{B}}^{s_{\mathsf{B}}}=Q\left(\sqrt{\frac{L}{V(\gamma_{\mathsf{B}}^{s_{\mathsf{B}}})}}\left[\begin{matrix}C(\gamma_{\mathsf{B}}^{s_{\mathsf{B}}})-\sqrt{\frac{V(\gamma_{\mathsf{W}}^{s_{\mathsf{B}}})}{L}}Q^{-1}(\Delta)\\-C(\gamma_{\mathsf{W}}^{s_{\mathsf{B}}})-n_{\mathsf{B}}/L\end{matrix}\right]\right). \tag{23}$$

On this basis, the average secure BLER of decoding s_{B} can be derived as in [51, Appendix A] as

$$\begin{aligned}\overline{\varepsilon}_{\mathsf{B}}^{s_{\mathsf{B}}}&=\mathbb{E}\left\{\varepsilon_{\mathsf{B}}^{s_{\mathsf{B}}}\right\}=\int_0^\infty\int_y^\infty\varepsilon_{\mathsf{B}}^{s_{\mathsf{B}}}f_{\gamma_{\mathsf{B}}^{s_{\mathsf{B}}}}(x)f_{\gamma_{\mathsf{W}}^{s_{\mathsf{B}}}}(x)dxdy\\&\simeq 1-\int_0^\infty F_{\gamma_{\mathsf{W}}^{s_{\mathsf{B}}}}(y)f_{\gamma_{\mathsf{B}}^{s_{\mathsf{B}}}}\left(\omega(1+y)-1\right)\omega dy,\end{aligned} \tag{24}$$

where $\omega=2^{\log_2(e)Q^{-1}(\Delta)/\sqrt{L}+n_{\mathsf{B}}/L}$.

B. AVERAGE BLER ANALYSIS

Since Bob performs SIC first to decode s_{W} and then decode s_{B}, the end-to-end (E2E) average BLER of Bob can be derived as in [65] as

$$\overline{\epsilon}_{\mathsf{B}}=\overline{\epsilon}_{\mathsf{B}}^{s_{\mathsf{W}}}+(1-\epsilon_{\mathsf{B}}^{s_{\mathsf{W}}})\overline{\epsilon}_{\mathsf{B}}^{s_{\mathsf{B}}}, \tag{25}$$

where $\overline{\epsilon}_{\mathsf{B}}^{s_{\mathsf{W}}}$ and $\overline{\epsilon}_{\mathsf{B}}^{s_{\mathsf{B}}}$ can be derived using Appendix A as

$$\begin{aligned}\overline{\epsilon}_{\mathsf{B}}^{s_{\mathsf{W}}}&=\xi_{\mathsf{W}}\sqrt{L}(\min\{\delta_{\mathsf{W}},\rho_{\mathsf{W}}/\rho_{\mathsf{B}}\}-\zeta_{\mathsf{W}})-\\&-\xi_{\mathsf{W}}\sqrt{L}\frac{\rho_{\mathsf{W}}}{\Gamma(\alpha_{\mathsf{B}})}\begin{cases}\Xi(c_1,\overline{\gamma}), & \delta_{\mathsf{W}}\ge\frac{\rho_{\mathsf{W}}}{\rho_{\mathsf{B}}},\\ \Xi(c_1,\overline{\gamma})-\Xi(c_2,\overline{\gamma}), & \delta_{\mathsf{W}}<\frac{\rho_{\mathsf{W}}}{\rho_{\mathsf{B}}},\end{cases}\end{aligned} \tag{26}$$

with $c_1=\frac{\zeta_{\mathsf{W}}}{\rho_{\mathsf{W}}-\zeta_{\mathsf{W}}\rho_{\mathsf{B}}}$ $c_2=\frac{\delta_{\mathsf{W}}}{\rho_{\mathsf{W}}-\delta_{\mathsf{W}}\rho_{\mathsf{B}}}$, and $\Xi(x,y)$ in (28), and

$$\begin{aligned}\overline{\epsilon}_{\mathsf{B}}^{s_{\mathsf{B}}}=1-\frac{\xi_{\mathsf{B}}\sqrt{L}}{\Gamma(\alpha_{\mathsf{B}})}&\left[\delta_{\mathsf{B}}\mathcal{G}^{2,1}_{2,3}\left(\begin{matrix}1,0\\\alpha_{\mathsf{B}},-1,0\end{matrix}\middle|\frac{\beta_{\mathsf{B}}\delta_{\mathsf{B}}}{\rho_{\mathsf{B}}\overline{\gamma}}\right)\right.\\&\left.-\zeta_{\mathsf{B}}\mathcal{G}^{2,1}_{2,3}\left(\begin{matrix}1,0\\\alpha_{\mathsf{B}},-1,0\end{matrix}\middle|\frac{\beta_{\mathsf{B}}\zeta_{\mathsf{B}}}{\rho_{\mathsf{B}}\overline{\gamma}}\right)\right].\end{aligned} \tag{27}$$

At high SNR, we employ the Riemann integral approximation [24, eq. (18)] combined with the first-order Taylor series [64, eq. (8.354.2)] to approximate $\overline{\epsilon}_{\mathsf{B}}^{s_{\mathsf{W}}}$ and $\overline{\epsilon}_{\mathsf{B}}^{s_{\mathsf{B}}}$ as

$$\begin{aligned}\overline{\epsilon}_{\mathsf{B}}^{s_{\mathsf{W}}}&\overset{\overline{\gamma}\to\infty}{\simeq}F_{\gamma_{\mathsf{B}}^{s_{\mathsf{W}}}}\left(2^{r_{\mathsf{W}}}-1\right)=F_{g_{\mathsf{B}}}\left(\frac{\gamma_{\mathsf{W}}^{\mathrm{th}}/\overline{\gamma}}{\rho_{\mathsf{W}}-\gamma_{\mathsf{W}}^{\mathrm{th}}\rho_{\mathsf{B}}}\right)\\&\approx\frac{1}{\Gamma(\alpha_{\mathsf{B}}+1)}\left(\frac{\beta_{\mathsf{B}}\gamma_{\mathsf{W}}^{\mathrm{th}}/\overline{\gamma}}{\rho_{\mathsf{W}}-\gamma_{\mathsf{W}}^{\mathrm{th}}\rho_{\mathsf{B}}}\right)^{\alpha_{\mathsf{B}}},\end{aligned} \tag{29}$$

$$\begin{aligned}\overline{\epsilon}_{\mathsf{B}}^{s_{\mathsf{B}}}&\overset{\overline{\gamma}\to\infty}{\simeq}F_{\gamma_{\mathsf{B}}^{s_{\mathsf{B}}}}\left(2^{r_{\mathsf{B}}}-1\right)=F_{g_{\mathsf{B}}}\left(\frac{\gamma_{\mathsf{B}}^{\mathrm{th}}}{\overline{\gamma}\rho_{\mathsf{B}}}\right)\\&\approx\frac{1}{\Gamma(\alpha_{\mathsf{B}}+1)}\left(\frac{\beta_{\mathsf{B}}\gamma_{\mathsf{B}}^{\mathrm{th}}}{\overline{\gamma}\rho_{\mathsf{B}}}\right)^{\alpha_{\mathsf{B}}},\end{aligned} \tag{30}$$

where $\gamma_{\mathsf{X}}^{\mathrm{th}}=2^{r_{\mathsf{X}}}-1$. On this approximation, the E2E average BLER of Bob behaves asymptotically

$$\begin{aligned}\overline{\epsilon}_{\mathsf{B}}&\overset{\overline{\gamma}\to\infty}{\simeq}\overline{\epsilon}_{\mathsf{B}}^{s_{\mathsf{W}}}+\overline{\epsilon}_{\mathsf{B}}^{s_{\mathsf{B}}}\\&\approx\frac{1}{\Gamma(\alpha_{\mathsf{B}}+1)}\left(\frac{\beta_{\mathsf{B}}}{\overline{\gamma}}\right)^{\alpha_{\mathsf{B}}}\left[\frac{(\gamma_{\mathsf{W}}^{\mathrm{th}})^{\alpha_{\mathsf{B}}}}{\left(\rho_{\mathsf{W}}-\gamma_{\mathsf{W}}^{\mathrm{th}}\rho_{\mathsf{B}}\right)^{\alpha_{\mathsf{B}}}}+\frac{(\gamma_{\mathsf{B}}^{\mathrm{th}})^{\alpha_{\mathsf{B}}}}{\rho_{\mathsf{B}}^{\alpha_{\mathsf{B}}}}\right].\end{aligned} \tag{31}$$

Based on the above simplified BLER expressions, some useful insight into system design can be drawn as follows.

Remark 1. The result in (31) states that the higher the transmit SNR, the smaller the E2E average BLER of Bob. Besides, the SNR curve of the BLER is a function of the scaling rate α_{B}. Therefore, the diversity order achieved by Bob is α_{B}. Moreover, when the blocklength L increases, both $\gamma_{\mathsf{W}}^{\mathrm{th}}$ and $\gamma_{\mathsf{B}}^{\mathrm{th}}$ decrease due to $2^{n_{\mathsf{W}}/L}-1\to 0$ and $2^{n_{\mathsf{B}}/L}-1\to 0$, which improves the BLER performance. However, when information per packet increases, for example, n_{W} or n_{B}, $\gamma_{\mathsf{W}}^{\mathrm{th}}$ or $\gamma_{\mathsf{B}}^{\mathrm{th}}$ will be increased, which leads to a higher BLER. This means that transmitting larger data performance results in more errors during communication.

Since Wille directly decode s_{W}, the average BLER of Wille can be derived as

$$\overline{\epsilon}_{\mathsf{W}}=\overline{\epsilon}_{\mathsf{W}}^{s_{\mathsf{W}}}, \tag{32}$$

where $\overline{\epsilon}_{\mathsf{W}}^{s_{\mathsf{W}}}$ can be derived using Appendix B as

$$\begin{aligned}\overline{\epsilon}_{\mathsf{W}}^{s_{\mathsf{W}}}&=\xi_{\mathsf{W}}\sqrt{L}(\min\{\delta_{\mathsf{W}},\rho_{\mathsf{W}}/\rho_{\mathsf{B}}\}-\zeta_{\mathsf{W}})\\&-\frac{\xi_{\mathsf{W}}\sqrt{L}\rho_{\mathsf{W}}}{\rho_{\mathsf{B}}^2}\begin{cases}\Xi(c_1,\overline{\gamma}), & \delta_{\mathsf{W}}\ge\frac{\rho_{\mathsf{W}}}{\rho_{\mathsf{B}}},\\ \Xi(c_1,\overline{\gamma})-\Xi(c_2,\overline{\gamma}), & \delta_{\mathsf{W}}<\frac{\rho_{\mathsf{W}}}{\rho_{\mathsf{B}}},\end{cases}\end{aligned} \tag{33}$$

with

$$\Xi(x,y)=\frac{\exp\left(-\frac{\beta_{\mathsf{W}}x}{y}\right)}{(x+1/\rho_{\mathsf{B}})^2}+\frac{\exp\left(\frac{\beta_{\mathsf{W}}}{\rho_{\mathsf{B}}y}\right)}{\beta_{\mathsf{W}}/y}\mathrm{Ei}\left(-\frac{x\rho_{\mathsf{B}}+1}{\rho_{\mathsf{B}}y/\beta_{\mathsf{W}}}\right), \tag{34}$$

At high SNR, we employ the Riemann integral approximation [24, eq. (18)] combined with the connection $1 - \exp(-x) \simeq x$ to approximate $\overline{\epsilon}_{\mathsf{W}}^{s_{\mathsf{W}}}$ as

$$\overline{\epsilon}_{\mathsf{W}}^{s_{\mathsf{W}}} \overset{\overline{\gamma}\to\infty}{\simeq} F_{\gamma_{\mathsf{W}}^{s_{\mathsf{W}}}}\left(2^{r_{\mathsf{W}}}-1\right) = F_{g_{\mathsf{W}}}\left(\frac{\gamma_{\mathsf{W}}^{\mathrm{th}}/\overline{\gamma}}{\rho_{\mathsf{W}} - \gamma_{\mathsf{W}}^{\mathrm{th}}\rho_{\mathsf{B}}}\right) \\ \approx \frac{\beta_{\mathsf{W}}\gamma_{\mathsf{W}}^{\mathrm{th}}/\overline{\gamma}}{\rho_{\mathsf{W}} - \gamma_{\mathsf{W}}^{\mathrm{th}}\rho_{\mathsf{B}}}. \tag{35}$$

Remark 2. The result in (35) states that the higher the transmit SNR, the smaller the E2E average BLER of Willie. Besides, the SNR curve of the BLER is a function of the scaling rate 1 (i.e., $1/\overline{\gamma}^{1}$). Therefore, the diversity order achieved by Willie is 1. Moreover, when the blocklength L increases, $\gamma_{\mathsf{W}}^{\mathrm{th}}$ decreases due to $2^{n_{\mathsf{W}}/L} - 1 \to 0$, which improves the BLER performance. However, when information per packet increases, for example, n_{W}, $\gamma_{\mathsf{W}}^{\mathrm{th}}$ will be increased, which leads to a higher BLER to Willie.

C. AVERAGE SECURE BLER ANALYSIS

Since Wille performs SIC first to decode s_{W} and then wiretap s_{B}, the average secure BLER of Bob can be derived as

$$\overline{\varepsilon}_{\mathsf{W}} = \overline{\epsilon}_{\mathsf{W}}^{s_{\mathsf{W}}} + (1 - \overline{\epsilon}_{\mathsf{W}}^{s_{\mathsf{W}}})\overline{\varepsilon}_{\mathsf{W}}^{s_{\mathsf{B}}}, \tag{36}$$

where $\overline{\varepsilon}_{\mathsf{W}}^{s_{\mathsf{B}}}$ can be derived using Appendix C as

$$\overline{\varepsilon}_{\mathsf{W}}^{s_{\mathsf{B}}} = 1 - \frac{1}{\Gamma(\alpha_{\mathsf{B}})}\Gamma\left(\alpha_{\mathsf{B}}, \frac{\beta_{\mathsf{B}}}{\rho_{\mathsf{B}}\overline{\gamma}}(\omega-1)\right) \\ + \exp\left(-\beta_{\mathsf{W}}\frac{1-\omega}{\omega\rho_{\mathsf{B}}\overline{\gamma}}\right)\frac{1}{\Gamma(\alpha_{\mathsf{B}})}\left(\frac{\beta_{\mathsf{W}}}{\beta_{\mathsf{B}}\omega}+1\right)^{-\alpha_{\mathsf{B}}} \\ \times\Gamma\left(\alpha_{\mathsf{B}}, \left[\frac{\beta_{\mathsf{W}}}{\omega\rho_{\mathsf{B}}\overline{\gamma}} + \frac{\beta_{\mathsf{B}}}{\rho_{\mathsf{B}}\overline{\gamma}}\right](\omega-1)\right), \tag{37}$$

At high SNR, we employ the first-order Taylor series [64, eq. (8.354.2)] combined with the connection $1 - \exp(-x) \simeq x$ to approximate $\overline{\varepsilon}_{\mathsf{W}}^{s_{\mathsf{B}}}$ as

$$\overline{\varepsilon}_{\mathsf{W}}^{s_{\mathsf{B}}} \overset{\overline{\gamma}\to\infty}{\simeq} \frac{1}{\Gamma(\alpha_{\mathsf{B}}+1)}\left(\frac{\beta_{\mathsf{B}}}{\rho_{\mathsf{B}}\overline{\gamma}}(\omega-1)\right)^{\alpha_{\mathsf{B}}} \\ + \left(1 - \beta_{\mathsf{W}}\frac{1-\omega}{\omega\rho_{\mathsf{B}}\overline{\gamma}}\right)\frac{1}{\Gamma(\alpha_{\mathsf{B}})}\left(\frac{\beta_{\mathsf{W}}}{\beta_{\mathsf{B}}\omega}+1\right)^{-\alpha_{\mathsf{B}}} \\ \times\left(\Gamma(\alpha_{\mathsf{B}}) - \frac{1}{\alpha_{\mathsf{B}}}\left[\frac{\beta_{\mathsf{W}}}{\omega\rho_{\mathsf{B}}\overline{\gamma}} + \frac{\beta_{\mathsf{B}}}{\rho_{\mathsf{B}}\overline{\gamma}}\right]^{\alpha_{\mathsf{B}}}(\omega-1)^{\alpha_{\mathsf{B}}}\right) \\ = \left(\frac{\beta_{\mathsf{B}}\omega}{\beta_{\mathsf{B}}\omega+\beta_{\mathsf{W}}}\right)^{\alpha_{\mathsf{B}}} + \frac{\beta_{\mathsf{W}}(\omega-1)}{\omega\rho_{\mathsf{B}}\overline{\gamma}}\left(\frac{\beta_{\mathsf{B}}\omega}{\beta_{\mathsf{B}}\omega+\beta_{\mathsf{W}}}\right)^{\alpha_{\mathsf{B}}} \\ - \frac{\beta_{\mathsf{W}}(\omega-1)}{\omega\rho_{\mathsf{B}}\overline{\gamma}\Gamma(\alpha_{\mathsf{B}}+1)}\left(\frac{\beta_{\mathsf{B}}(\omega-1)}{\rho_{\mathsf{B}}\overline{\gamma}}\right)^{\alpha_{\mathsf{B}}}. \tag{38}$$

Remark 3. From (35) and (38), it can be seen that if we let $1/\overline{\gamma} = 0$, the average secure BLER of Bob will be a constant value $\left(\frac{\beta_{\mathsf{B}}\omega}{\beta_{\mathsf{B}}\omega+\beta_{\mathsf{W}}}\right)^{\alpha_{\mathsf{B}}}$. This means that the secure diversity order is zero. However, since $\frac{\beta_{\mathsf{B}}\omega}{\beta_{\mathsf{B}}\omega+\beta_{\mathsf{W}}} < 1$ and α_{B} is a function of number of RIS elements. Thus, increasing K will improve the average secure BLER performance.

TABLE 1: Main parameters for our simulations.

Parameter	Value
Monte-Carlo sample	10^4
Number of RIS element - K	16
Number of resolution bits - q	3
PA coefficient for Willie's signal - ρ_{W}	0.7
PA coefficient for Bob's signal - ρ_{B}	0.3
Data information bit for Willie's signal - n_{W}	100
Data information bit for Bob's signal - n_{B}	200
Blocklength - L	128
The information leakage probability Δ	0.2
Shape parameter of source-k-th RIS element links - m_{SR}^{k}	2.2
Shape parameter of the k-th RIS element-Bob links - m_{RB}^{k}	2.5
Shape parameter of the k-th RIS element-Willie links - m_{RW}^{k}	2.3
Scale parameter of source-k-th RIS element links - Ω_{SR}^{k}	0.5
Scale parameter of the k-th RIS element-Bob links - Ω_{RB}^{k}	0.5
Scale parameter of the k-th RIS element-Willie links - Ω_{RW}^{k}	1

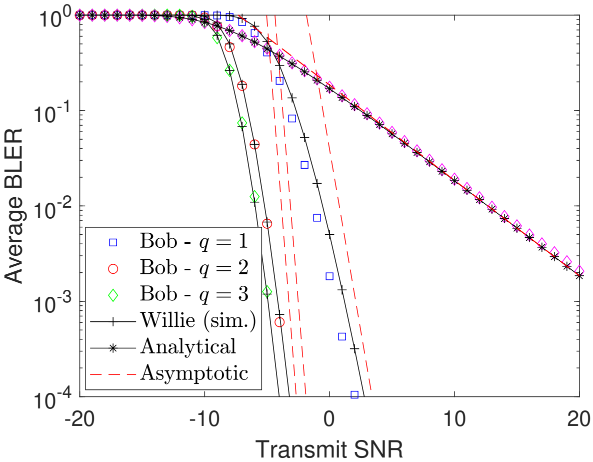

Fig. 2: Average BLER vs SNR $\overline{\gamma}$ under different resolution bit settings q.

IV. NUMERICAL RESULTS AND DISCUSSION

This section provides Monte-Carlo simulations (denoted by markers in the legend of the following figures) to verify the analytical expressions developed in (25) and (36). Unless other specifics, we list the simulation parameters in Table 1.

Fig. 2 plots the average BLER versus (vs) the transmit SNR $\overline{\gamma}$ under different resolution bit settings q. First, we can see that with $q = 1$, the analytical results nearly approximate the simulation markers. However, when $q = 2, 3$, the analytical results almost match the simulation markers, showing the correctness of the derivations. Notably, a 3-resolution bit can save the transmit SNR of 3 dB. Second, when we increase the SNR $\overline{\gamma}$, the quality of SINR reception to decode s_{W} and s_{B} also increases, which leads to the dramatic reduction of the average BLER of Bob. This means that the reliability of short-packet transmission can be improved.

In Fig. 3, we investigate how the average BLER of Bob changes with different packet settings at $\overline{\gamma} = -10$ dB. First, it is observed that when blocklength L increases, the average BLER curves reduce significantly, for example, 100-folds when comparing $L = 160$ and $L = 240$. This is because

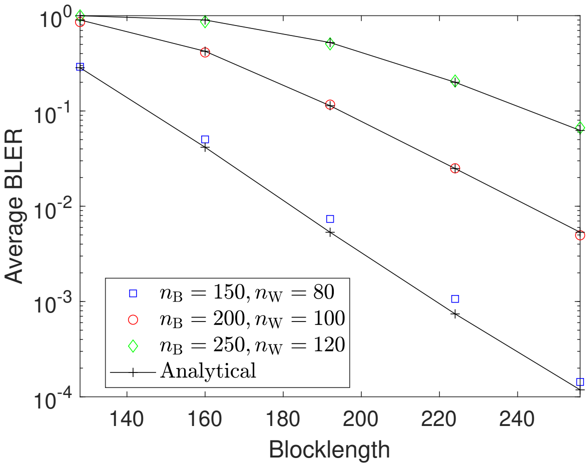

Fig. 3: Average BLER of Bob vs blocklength L under different data stream settings n_X.

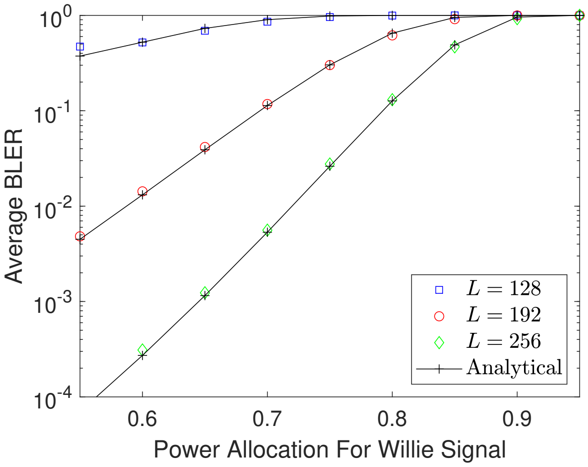

Fig. 4: Average BLER of Bob vs PA coefficient ρ_W under different blocklength settings L.

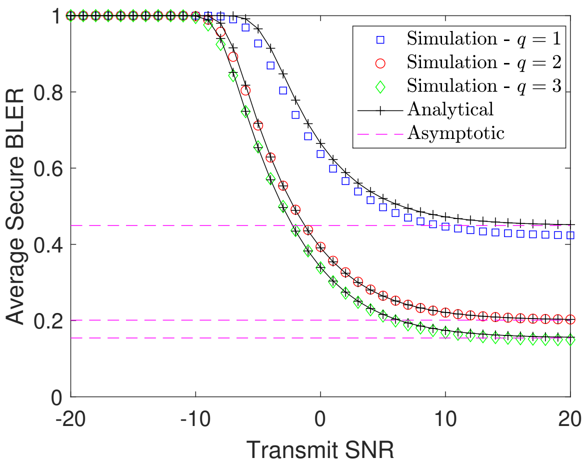

Fig. 5: Average secure BLER vs SNR $\overline{\gamma}$ under different resolution bit settings q.

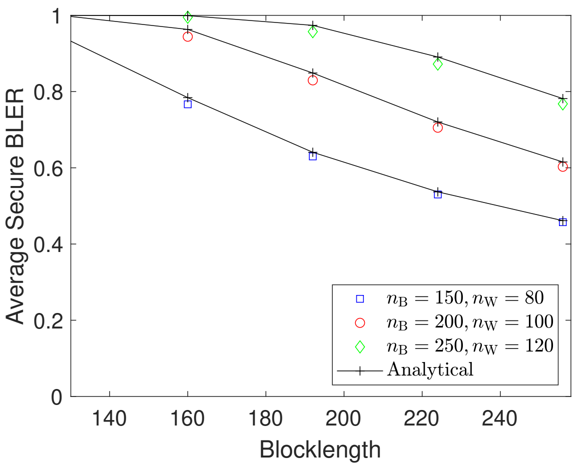

Fig. 6: Average secure BLER vs blocklength L under different data stream settings n_X.

using a larger blocklength (the number of channels used to spread over the spectrum bandwidth) gives more chances to Bob to correct his data information. Second, when data amount (n_B and n_W) distributed per packet increases, the average BLER curves tend to increase. This can be explained by the fact that longer information sent to the networks under fading channels will cause more errors during corrections.

In Fig. 4, we plot the average BLER of Bob as a function of the PA coefficient ρ_W under different blocklength settings L at the SNR of -10 dB. It is first observed that when increasing ρ_W increases the quality of SINR reception of decoding s_W but simultaneously decreases that of decoding s_B. This, therefore, increases the average BLER curers dramatically. However, increasing blocklength L can partly compensate for this performance loss.

Next, we turn to investigate the average secure BLER in Fig. 5. It can be seen that all the average secure BLER curves developed by analytical solutions highly approximate the simulation results when the number of resolution bits increases, which is the same trend with analysis of the average BLER. However, there is still a major difference, where the average secure BLER curves tend to decrease with low and moderate SNR mode and then saturate at high SNR mode. This tendency totally corrects with the analysis in Remark 3.

In Fig. 6, we continue to investigate the average secure BLER performance against variations in packet settings at the SNR of -10 dB. As observed, the average secure BLER curves decrease with an increase in blocklength but increase with an increase in the data amount sent per packet. This performance trend is similar to the case of the average BLER.

In Fig. 7, we once again inspect the average secure BLER performance as a function of the PA coefficient ρ_W under different blocklength settings L at the SNR of -10 dB. The figure shows that the average secure BLER curves have a

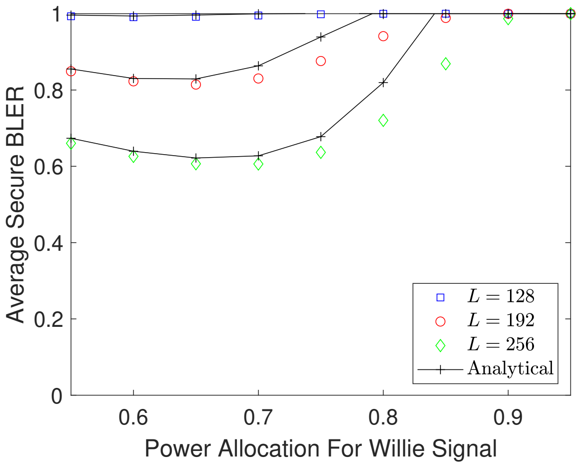

Fig. 7: Average secure BLER vs PA coefficient ρ_{W} under different blocklength settings L.

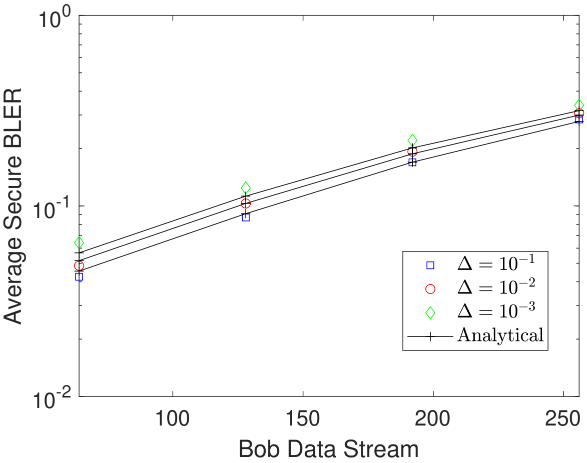

Fig. 8: Average secure BLER vs Bob's data stream n_{B} under varying leakage information probability Δ.

convex form to the PA coefficient ρ_{W}, where the optimal PA value is around 0.68 for $L = 256$ and 0.65 for $L = 192$. This means that besides increasing the number of RIS elements, we can further optimize the average secure BLER. Note that since the average secure BLER can be constructed in a closed-form expression, we can adopt low-complexity search methods like Golden search or bisection search to achieve the optimal PA solution.

In Fig. 8, we study the impact of Bob's data stream n_{B} and leakage information probability Δ on the average secure BLER. From the figure, we can see that when Bob's data stream n_{B} increases, the average secure BLER curves increase dramatically. Meanwhile, the variation of leakage information probability Δ slightly affects the average secure BLER performance. This is because Willie is more likely to eavesdrop and successfully decode Bob's information.

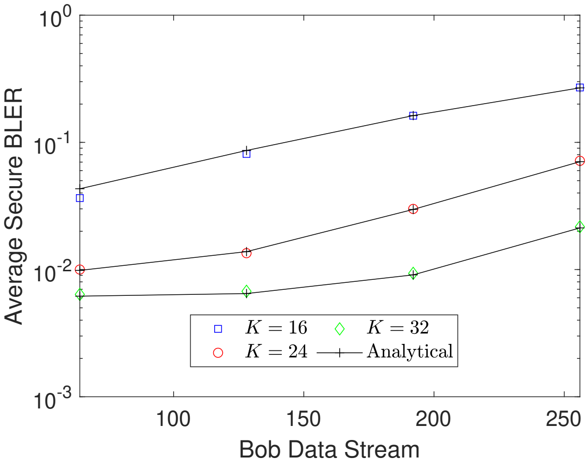

Fig. 9: Average secure BLER vs Bob's data stream n_{B} under various RIS elements K.

In Fig. 9, we examine if increasing the number of RIS elements K improves the average secure BLER when sending a large volume of Bob's data stream n_{B}. From this figure, we can see that the answer is yes. When K is set from 16 to 32, the average secure BLER performance is improved by ten times, irrespective of increasing Bob's data volume. As such, increasing the number of RIS elements K is a great solution for protecting the secure performance of Bob under short-packet transmission.

V. CONCLUSIONS

In this paper, we have studied the performance of RIS-secured short-packet NOMA networks in the presence of arbitrary untrusted users, where the source node communicates in a short-packet manner. Accordingly, a joint PA policy and RIS's phase-shifter is considered to deal with arbitrarily untrusted paring users. In this configuration, we evaluate the system performance by deriving closed-form approximations for the average BLER at Bob and the average secure BLER, along with the asymptotic analysis to achieve knowledge of diversity order and performance limits. All of them are verified via Monte Carlo simulations. In terms of the average BLER performance, it is shown that using a 3-resolution bit (p) can save the transmit SNR of 3 dB compared to that of a 1-resolution bit. Increasing the PA coefficient (ρ_{W}) results in an increase of the BLER of Bob. However, even with the SNR of -10 dB, increasing blocklength (L) from 160 to 240 can improve the average BLER of Bob by 100-fold. In terms of the average secure BLER performance, it is shown that the average secure BLER performance improves as blocklength increases but gets worse as the amount of data sent per packet increases. There exists an optimal PA value at which the average secure BLER can be minimized. While the change in the information leakage probability slightly affects the average secure BLER performance, increasing Bob's data amount significantly reduces.

APPENDIX A PROOF OF AVERAGE BLER OF BOB

A. AVERAGE BLER FOR DECODING S_{W}

From (21) and (7), the average BLER for decoding s_{W} at node B can be derived as

$$\bar{\epsilon}_{\mathsf{B}}^{s_{\mathsf{W}}} = \xi_{\mathsf{W}}\sqrt{L}\int_{\zeta_{\mathsf{W}}}^{\delta_{\mathsf{W}}} F_{\gamma_{\mathsf{B}}^{s_{\mathsf{W}}}}(x)dx, \tag{39}$$

where

$$F_{\gamma_{\mathsf{B}}^{s_{\mathsf{W}}}}(x) = \begin{cases} F_{g_{\mathsf{B}}}\left(\frac{x/\overline{\gamma}}{\rho_{\mathsf{W}} - x\rho_{\mathsf{B}}}\right), & \forall x < \rho_{\mathsf{W}}/\rho_{\mathsf{B}}, \\ 1, & \forall x \geq \rho_{\mathsf{W}}/\rho_{\mathsf{B}}. \end{cases} \tag{40}$$

Thus, the average BLER for decoding s_{W} at node B can be rewritten as

$$\begin{aligned} \bar{\epsilon}_{\mathsf{B}}^{s_{\mathsf{W}}} &= \xi_{\mathsf{W}}\sqrt{L}\int_{\zeta_{\mathsf{W}}}^{\min\{\delta_{\mathsf{W}},\rho_{\mathsf{W}}/\rho_{\mathsf{B}}\}} F_{g_{\mathsf{B}}}\left(\frac{x/\overline{\gamma}}{\rho_{\mathsf{W}} - x\rho_{\mathsf{B}}}\right) dx \\ &= \xi_{\mathsf{W}}\sqrt{L}\int_{\zeta_{\mathsf{W}}}^{\min\{\delta_{\mathsf{W}},\frac{\rho_{\mathsf{W}}}{\rho_{\mathsf{B}}}\}} \left[1 - \frac{\Gamma\left(\alpha_{\mathsf{B}}, \frac{\beta_{\mathsf{B}}x/\overline{\gamma}}{\rho_{\mathsf{W}} - x\rho_{\mathsf{B}}}\right)}{\Gamma(\alpha_{\mathsf{B}})}\right] dx \\ &= \xi_{\mathsf{W}}\sqrt{L}(\min\{\delta_{\mathsf{W}}, \rho_{\mathsf{W}}/\rho_{\mathsf{B}}\} - \zeta_{\mathsf{W}}) \\ &\quad - \xi_{\mathsf{W}}\sqrt{L}\frac{\rho_{\mathsf{W}}}{\Gamma(\alpha_{\mathsf{B}})}\int_{c_1}^{\frac{\min\{\delta_{\mathsf{W}},\rho_{\mathsf{W}}/\rho_{\mathsf{B}}\}}{\rho_{\mathsf{W}} - \min\{\delta_{\mathsf{W}},\rho_{\mathsf{W}}/\rho_{\mathsf{B}}\}\rho_{\mathsf{B}}}} \frac{\Gamma\left(\alpha_{\mathsf{B}}, \beta_{\mathsf{B}}y/\overline{\gamma}\right)}{(\rho_{\mathsf{B}}y + 1)^2} dy. \end{aligned} \tag{41}$$

Case study 1: When $\min\{\delta_{\mathsf{W}}, \rho_{\mathsf{W}}/\rho_{\mathsf{B}}\} = \rho_{\mathsf{W}}/\rho_{\mathsf{B}}$, we can rewrite the integral in (41) as

$$\begin{aligned} I &= \int_{c_1}^{\infty} \frac{\Gamma\left(\alpha_{\mathsf{B}}, \beta_{\mathsf{B}}y/\overline{\gamma}\right)}{(\rho_{\mathsf{B}}y + 1)^2} dy \\ &= \int_{0}^{\infty} \mathsf{H}(y/c_1 - 1)\frac{\Gamma\left(\alpha_{\mathsf{B}}, \beta_{\mathsf{B}}y/\overline{\gamma}\right)}{(\rho_{\mathsf{B}}y + 1)^2} dy. \end{aligned} \tag{42}$$

By using the following transformations

$$\mathsf{H}(y/c_1 - 1) = \mathcal{G}_{1,1}^{0,1}\left(\begin{matrix}1 \\ 0\end{matrix}\middle| \frac{y}{c_1}\right), \tag{43}$$

$$\Gamma\left(\alpha_{\mathsf{B}}, \beta_{\mathsf{B}}y/\overline{\gamma}\right) = \mathcal{G}_{1,2}^{2,0}\left(\begin{matrix}1 \\ \alpha_{\mathsf{B}}, 0\end{matrix}\middle| \beta_{\mathsf{B}}y/\overline{\gamma}\right), \tag{44}$$

$$(\rho_{\mathsf{B}}y + 1)^{-2} = \frac{1}{\Gamma(2)}\mathcal{G}_{1,1}^{1,1}\left(\begin{matrix}-1 \\ 0\end{matrix}\middle| \rho_{\mathsf{B}}y\right), \tag{45}$$

we can rewrite I as

$$\begin{aligned} I = \int_{0}^{\infty} &\mathcal{G}_{1,2}^{2,0}\left(\begin{matrix}1 \\ \alpha_{\mathsf{B}}, 0\end{matrix}\middle| \beta_{\mathsf{B}}\frac{y}{\overline{\gamma}}\right)\mathcal{G}_{1,1}^{0,1}\left(\begin{matrix}1 \\ 0\end{matrix}\middle| \frac{y}{c_1}\right) \\ &\times \mathcal{G}_{1,1}^{1,1}\left(\begin{matrix}-1 \\ 0\end{matrix}\middle| \rho_{\mathsf{B}}y\right) dy \triangleq \Xi(c_1, \overline{\gamma}), \end{aligned} \tag{46}$$

which has standard form as in [41, eq. (51)].

Case study 2: When $\min\{\delta_{\mathsf{W}}, \rho_{\mathsf{W}}/\rho_{\mathsf{B}}\} = \delta_{\mathsf{W}}$, we can rewrite the integral in (41) as

$$\begin{aligned} I &= \int_{c_1}^{c_2} \frac{\Gamma\left(\alpha_{\mathsf{B}}, \beta_{\mathsf{B}}y/\overline{\gamma}\right)}{(\rho_{\mathsf{B}}y + 1)^2} dy \\ &= \int_{c_1}^{\infty} \frac{\Gamma\left(\alpha_{\mathsf{B}}, \beta_{\mathsf{B}}y/\overline{\gamma}\right)}{(\rho_{\mathsf{B}}y + 1)^2} dy - \int_{c_2}^{\infty} \frac{\Gamma\left(\alpha_{\mathsf{B}}, \beta_{\mathsf{B}}y/\overline{\gamma}\right)}{(\rho_{\mathsf{B}}y + 1)^2} dy \\ &= \int_{0}^{\infty} \mathsf{H}(y/c_1 - 1)\frac{\Gamma\left(\alpha_{\mathsf{B}}, \beta_{\mathsf{B}}y/\overline{\gamma}\right)}{(\rho_{\mathsf{B}}y + 1)^2} dy \\ &\quad - \int_{0}^{\infty} \mathsf{H}(y/c_2 - 1)\frac{\Gamma\left(\alpha_{\mathsf{B}}, \beta_{\mathsf{B}}y/\overline{\gamma}\right)}{(\rho_{\mathsf{B}}y + 1)^2} dy \\ &= \Xi(c_1, \overline{\gamma}) - \Xi(c_2, \overline{\gamma}). \end{aligned} \tag{47}$$

B. AVERAGE BLER FOR DECODING S_{B}

From (21) and (8), the average BLER for decoding s_{B} at node B can be derived as

$$\begin{aligned} \bar{\epsilon}_{\mathsf{B}}^{s_{\mathsf{B}}} &= \xi_{\mathsf{B}}\sqrt{L}\int_{\zeta_{\mathsf{B}}}^{\delta_{\mathsf{B}}} F_{\gamma_{\mathsf{B}}^{s_{\mathsf{B}}}}(x)dx \\ &= \xi_{\mathsf{B}}\sqrt{L}\int_{\zeta_{\mathsf{B}}}^{\delta_{\mathsf{B}}} \left[1 - \frac{1}{\Gamma(\alpha_{\mathsf{B}})}\Gamma\left(\alpha_{\mathsf{B}}, \frac{\beta_{\mathsf{B}}x}{\rho_{\mathsf{B}}\overline{\gamma}}\right)\right] dx \\ &= 1 - \frac{\xi_{\mathsf{B}}\sqrt{L}}{\Gamma(\alpha_{\mathsf{B}})}\int_{\zeta_{\mathsf{B}}}^{\delta_{\mathsf{B}}} \Gamma\left(\alpha_{\mathsf{B}}, \frac{\beta_{\mathsf{B}}x}{\rho_{\mathsf{B}}\overline{\gamma}}\right) dx \\ &= 1 - \frac{\xi_{\mathsf{B}}\sqrt{L}}{\Gamma(\alpha_{\mathsf{B}})}\left[\int_{0}^{\infty} \mathsf{H}(1 - y/\delta_{\mathsf{B}})\Gamma\left(\alpha_{\mathsf{B}}, \frac{\beta_{\mathsf{B}}x}{\rho_{\mathsf{B}}\overline{\gamma}}\right) dx\right. \\ &\quad \left. - \int_{0}^{\infty} \mathsf{H}(1 - y/\zeta_{\mathsf{B}})\Gamma\left(\alpha_{\mathsf{B}}, \frac{\beta_{\mathsf{B}}x}{\rho_{\mathsf{B}}\overline{\gamma}}\right) dx\right] \\ &= 1 - \frac{\xi_{\mathsf{B}}\sqrt{L}}{\Gamma(\alpha_{\mathsf{B}})}\left[\int_{0}^{\infty} \mathcal{G}_{1,1}^{1,0}\left(\begin{matrix}1 \\ 0\end{matrix}\middle| \frac{y}{\delta_{\mathsf{B}}}\right)\mathcal{G}_{1,2}^{2,0}\left(\begin{matrix}1 \\ \alpha_{\mathsf{B}}, 0\end{matrix}\middle| \frac{\beta_{\mathsf{B}}y}{\rho_{\mathsf{B}}\overline{\gamma}}\right) dx\right. \\ &\quad \left. - \int_{0}^{\infty} \mathcal{G}_{1,1}^{1,0}\left(\begin{matrix}1 \\ 0\end{matrix}\middle| \frac{y}{\zeta_{\mathsf{B}}}\right)\mathcal{G}_{1,2}^{2,0}\left(\begin{matrix}1 \\ \alpha_{\mathsf{B}}, 0\end{matrix}\middle| \frac{\beta_{\mathsf{B}}y}{\rho_{\mathsf{B}}\overline{\gamma}}\right) dx\right], \end{aligned} \tag{48}$$

which has standard form as in [64, eq. (07.34.21.0011.01)].

APPENDIX B PROOF OF AVERAGE BLER OF WILLIE

From (21) and (7), the average BLER for decoding s_{W} at node W can be derived as

$$\bar{\epsilon}_{\mathsf{W}}^{s_{\mathsf{W}}} = \xi_{\mathsf{W}}\sqrt{L}\int_{\zeta_{\mathsf{W}}}^{\delta_{\mathsf{W}}} F_{\gamma_{\mathsf{W}}^{s_{\mathsf{W}}}}(x)dx, \tag{49}$$

where

$$F_{\gamma_{\mathsf{W}}^{s_{\mathsf{W}}}}(x) = \begin{cases} F_{g_{\mathsf{W}}}\left(\frac{x/\overline{\gamma}}{\rho_{\mathsf{W}} - x\rho_{\mathsf{B}}}\right), & \forall x < \rho_{\mathsf{W}}/\rho_{\mathsf{B}}, \\ 1, & \forall x \geq \rho_{\mathsf{W}}/\rho_{\mathsf{B}}. \end{cases} \tag{50}$$

Thus, the average BLER for decoding s_{W} at node W can be rewritten as

$$\begin{aligned} \bar{\epsilon}_{\mathsf{W}}^{s_{\mathsf{W}}} &= \xi_{\mathsf{W}}\sqrt{L}\int_{\zeta_{\mathsf{W}}}^{\min\{\delta_{\mathsf{W}},\rho_{\mathsf{W}}/\rho_{\mathsf{B}}\}} F_{g_{\mathsf{W}}}\left(\frac{x/\overline{\gamma}}{\rho_{\mathsf{W}} - x\rho_{\mathsf{B}}}\right) dx \\ &= \xi_{\mathsf{W}}\sqrt{L}(\min\{\delta_{\mathsf{W}}, \rho_{\mathsf{W}}/\rho_{\mathsf{B}}\} - \zeta_{\mathsf{W}}) \\ &\quad - \frac{\xi_{\mathsf{W}}\sqrt{L}\rho_{\mathsf{W}}}{\rho_{\mathsf{B}}^2}\int_{c_1}^{\frac{\min\{\delta_{\mathsf{W}},\rho_{\mathsf{W}}/\rho_{\mathsf{B}}\}}{\rho_{\mathsf{W}} - \min\{\delta_{\mathsf{W}},\rho_{\mathsf{W}}/\rho_{\mathsf{B}}\}\rho_{\mathsf{B}}}} \frac{\exp\left(-\beta_{\mathsf{W}}y/\overline{\gamma}\right) dy}{(y + 1/\rho_{\mathsf{B}})^2}. \end{aligned} \tag{51}$$

Case study 1: when $\min\{\delta_{\mathsf{W}}, \rho_{\mathsf{W}}/\rho_{\mathsf{B}}\} = \rho_{\mathsf{W}}/\rho_{\mathsf{B}}$, we can rewrite the integral in (51) as

$$J = \int_{c_1}^{\infty} \exp\left(-\beta_{\mathsf{W}} y/\bar{\gamma}\right) \frac{dy}{(y+1/\rho_{\mathsf{B}})^2} \triangleq \Psi(c_1, \bar{\gamma}), \quad (52)$$

which has standard form as in [64, eq. (3.353.1)].

Case study 2: when $\min\{\delta_{\mathsf{W}}, \rho_{\mathsf{W}}/\rho_{\mathsf{B}}\} = \delta_{\mathsf{W}}$, we can rewrite the integral in (51) as

$$\begin{aligned} J &= \int_{c_1}^{c_2} \exp\left(-\beta_{\mathsf{W}} y/\bar{\gamma}\right) \frac{dy}{(y+1/\rho_{\mathsf{B}})^2} \\ &= \int_{c_1}^{\infty} \exp\left(-\beta_{\mathsf{W}} y/\bar{\gamma}\right) \frac{dy}{(y+1/\rho_{\mathsf{B}})^2} \\ &\quad - \int_{c_2}^{\infty} \exp\left(-\beta_{\mathsf{W}} y/\bar{\gamma}\right) \frac{dy}{(y+1/\rho_{\mathsf{B}})^2} \\ &= \Psi(c_1, \bar{\gamma}) - \Psi(c_2, \bar{\gamma}). \quad (53) \end{aligned}$$

APPENDIX C PROOF OF AVERAGE SECURE BLER OF BOB

To derive (24), we derive the CDF of $\gamma_{\mathsf{W}}^{s\mathsf{B}}$ and PDF of $\gamma_{\mathsf{B}}^{s\mathsf{B}}$ as

$$F_{\gamma_{\mathsf{W}}^{s\mathsf{B}}}(y) = F_{g_{\mathsf{W}}}(y/[\rho_{\mathsf{B}}\bar{\gamma}]) = 1 - \exp(-\beta_{\mathsf{W}} y/[\rho_{\mathsf{B}}\bar{\gamma}]), \quad (54)$$

$$\begin{aligned} f_{\gamma_{\mathsf{B}}^{s\mathsf{B}}}(z) &= \frac{1}{\rho_{\mathsf{B}}\bar{\gamma}} f_{g_{\mathsf{B}}}\left(z/[\rho_{\mathsf{B}}\bar{\gamma}]\right) \\ &= \frac{z^{\alpha_{\mathsf{B}}-1}}{\Gamma(\alpha_{\mathsf{B}})} \left(\frac{\beta_{\mathsf{B}}}{\rho_{\mathsf{B}}\bar{\gamma}}\right)^{\alpha_{\mathsf{B}}} \exp\left(-\frac{\beta_{\mathsf{B}}}{\rho_{\mathsf{B}}\bar{\gamma}} z\right) dz. \quad (55) \end{aligned}$$

Combining these results with the variable transform $z = \omega(1+y) - 1$, we can derive $\bar{\varepsilon}_{\mathsf{B}}^{x\mathsf{B}}$ in (24) as

$$\begin{aligned} \bar{\varepsilon}_{\mathsf{B}}^{x\mathsf{B}} &= 1 - \int_0^{\infty} F_{\gamma_{\mathsf{W}}^{s\mathsf{B}}}(y) f_{\gamma_{\mathsf{B}}^{s\mathsf{B}}}\left(\omega(1+y) - 1\right) \omega dy \\ &= 1 - \int_{\omega-1}^{\infty} \left[1 - \exp\left(-\beta_{\mathsf{W}} \frac{z+1-\omega}{\omega\rho_{\mathsf{B}}\bar{\gamma}}\right)\right] \\ &\quad \times \frac{z^{\alpha_{\mathsf{B}}-1}}{\Gamma(\alpha_{\mathsf{B}})} \left(\frac{\beta_{\mathsf{B}}}{\rho_{\mathsf{B}}\bar{\gamma}}\right)^{\alpha_{\mathsf{B}}} \exp\left(-\frac{\beta_{\mathsf{B}}}{\rho_{\mathsf{B}}\bar{\gamma}} z\right) dz, \quad (56) \end{aligned}$$

which can be solved using [64, eq. (3.351)].

REFERENCES

[1] M. Z. Chowdhury, Md. Shahjalal, S. Ahmed, and Y. M. Jang, “6G Wireless Communication Systems: Applications, Requirements, Technologies, Challenges, and Research Directions,” *IEEE Open J. Commun. Soc.*, vol. 1, pp. 957–975, Jul. 2020.

[2] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding *et al.*, “6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies,” *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 28–41, Jul. 2019.

[3] C.-X. Wang, X. You, X. Gao, X. Zhu, Z. Li *et al.*, “On the Road to 6G: Visions, Requirements, Key Technologies, and Testbeds,” *IEEE Commun. Surv. Tutorials*, vol. 25, no. 2, pp. 905–974, Feb. 2023.

[4] N. Mishra and S. Pandya, “Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review,” *IEEE Access*, vol. 9, pp. 59 353–59 377, Apr. 2021.

[5] O. Aouedi, T.-H. Vu, A. Sacco, D. C. Nguyen, K. Piamrat *et al.*, “A survey on intelligent internet of things: Applications, security, privacy, and future directions,” *IEEE Commun. Surv. Tutorials*, Jul. 2024.

[6] C. Feng and H.-M. Wang, “Secure Short-Packet Communications at the Physical Layer for 5G and Beyond,” *IEEE Commun. Stand. Mag.*, vol. 5, no. 3, pp. 96–102, Oct. 2021.

[7] B. Makki, K. Chitti, A. Behravan, and M.-S. Alouini, “A Survey of NOMA: Current Status and Open Research Challenges,” *IEEE Open J. Commun. Soc.*, vol. 1, pp. 179–189, Jan. 2020.

[8] I. Budhiraja, N. Kumar, S. Tyagi, S. Tanwar, Z. Han *et al.*, “A Systematic Review on NOMA Variants for 5G and Beyond,” *IEEE Access*, vol. 9, pp. 85 573–85 644, May 2021.

[9] Y. Liu, S. Zhang, X. Mu, Z. Ding, R. Schober *et al.*, “Evolution of NOMA Toward Next Generation Multiple Access (NGMA) for 6G,” *IEEE J. Sel. Areas Commun.*, vol. 40, no. 4, pp. 1037–1071, Jan. 2022.

[10] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li *et al.*, “Non-Orthogonal Multiple Access (NOMA) for Cellular Future Radio Access,” in *2013 IEEE 77th Vehicular Technology Conference (VTC Spring)*. IEEE, pp. 02–05.

[11] A. Benjebbour, K. Saito, A. Li, Y. Kishiyama, and T. Nakamura, “Non-orthogonal multiple access (NOMA): Concept, performance evaluation and experimental trials,” in *2015 International Conference on Wireless Networks and Mobile Communications (WINCOM)*. IEEE, pp. 20–23.

[12] Z. Ding, P. Fan, and H. V. Poor, “Impact of User Pairing on 5G Nonorthogonal Multiple-Access Downlink Transmissions,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6010–6023, Sep. 2015.

[13] L. Zhu, J. Zhang, Z. Xiao, X. Cao, and D. O. Wu, “Optimal User Pairing for Downlink Non-Orthogonal Multiple Access (NOMA),” *IEEE Wireless Commun. Lett.*, vol. 8, no. 2, pp. 328–331, Jul. 2018.

[14] J. Zhang, X. Tao, H. Wu, and X. Zhang, “Performance Analysis of User Pairing in Cooperative NOMA Networks,” *IEEE Access*, vol. 6, pp. 74 288–74 302, Nov. 2018.

[15] N. S. Mouni, A. Kumar, and P. K. Upadhyay, “Adaptive User Pairing for NOMA Systems With Imperfect SIC,” *IEEE Wireless Commun. Lett.*, vol. 10, no. 7, pp. 1547–1551, Apr. 2021.

[16] S. Dhakal, P. A. Martin, and P. J. Smith, “NOMA With Guaranteed Weak User QoS: Design and Analysis,” *IEEE Access*, vol. 7, pp. 32 884–32 896, Feb. 2019.

[17] K. Long, P. Wang, W. Li, and D. Chen, “Spectrum Resource and Power Allocation With Adaptive Proportional Fair User Pairing for NOMA Systems,” *IEEE Access*, vol. 7, pp. 80 043–80 057, Jun. 2019.

[18] I. Azam, M. B. Shahab, and S. Y. Shin, “Energy-Efficient Pairing and Power Allocation for NOMA UAV

Network Under QoS Constraints," *IEEE IoT J.*, vol. 9, no. 24, pp. 25 011–25 026, Aug. 2022.

[19] I. F. Akyildiz, A. Kak, and S. Nie, "6G and Beyond: The Future of Wireless Communications Systems," *IEEE Access*, vol. 8, pp. 133 995–134 030, Jul. 2020.

[20] Y. Polyanskiy, H. V. Poor, and S. Verdu, "Channel Coding Rate in the Finite Blocklength Regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, Apr. 2010.

[21] N. H. Tu and K. Lee, "Performance Analysis and Optimization of Multihop MIMO Relay Networks in Short-Packet Communications," *IEEE Trans. Wireless Commun.*, vol. 21, no. 6, pp. 4549–4562, Dec. 2021.

[22] N. H. Tu, T.-D. Hoang, and K. Lee, "Short-Packet URLLCs for MIMO Underlay Cognitive Multihop Relaying With Imperfect CSI," *IEEE Access*, vol. 11, pp. 81 672–81 689, Aug. 2023.

[23] N. T. Y. Linh, N. H. Tu, P. N. Son, and V. N. Q. Bao, "Dual-hop relaying networks for short-packet URLLCs: Performance analysis and optimization," *J. Commun. Networks*, vol. 24, no. 4, pp. 408–418, Jul. 2022.

[24] T.-H. Vu, T.-V. Nguyen, T.-T. Nguyen, and S. Kim, "Performance Analysis and Deep Learning Design of Wireless Powered Cognitive NOMA IoT Short-Packet Communications With Imperfect CSI and SIC," *IEEE IoT J.*, vol. 9, no. 13, pp. 10 464–10 479, Oct. 2021.

[25] T.-H. Vu, T.-V. Nguyen, Q.-V. Pham, D. B. da Costa, and S. Kim, "Hybrid Long- and Short-Packet Based NOMA Systems With Joint Power Allocation and Beamforming Design," *IEEE Trans. Veh. Technol.*, vol. 72, no. 3, pp. 4079–4084, Nov. 2022.

[26] T.-T. Nguyen, T.-H. Vu, L.-T. Tu, T. T. Duy, Q.-S. Nguyen *et al.*, "A Low-Complexity Relaying Protocol for Cooperative Short-Packet NOMA-Based Spectrum Sharing Systems," *IEEE Trans. Veh. Technol.*, vol. 73, no. 6, pp. 9044–9049, Jan. 2024.

[27] T.-T. Nguyen, T.-H. Vu, D. B. da Costa, P. X. Nguyen, and H. Q. Ta, "Short-Packet Communications in IoT-Aided Cellular Cooperative Networks With Non-Orthogonal Multiple Access," *IEEE Trans. Veh. Technol.*, vol. 72, no. 1, pp. 1296–1301, Sep. 2022.

[28] J. Zhang, H. Du, Q. Sun, B. Ai, and D. W. K. Ng, "Physical Layer Security Enhancement With Reconfigurable Intelligent Surface-Aided Networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 3480–3495, May 2021.

[29] X. Pei, H. Yin, L. Tan, L. Cao, Z. Li *et al.*, "RIS-Aided Wireless Communications: Prototyping, Adaptive Beamforming, and Indoor/Outdoor Field Trials," *IEEE Transactions on Communications*, vol. 69, no. 12, pp. 8627–8640, Sep. 2021.

[30] A.-T. Le, T. N. Nguyen, L.-T. Tu, T.-P. Tran, T. T. Duy *et al.*, "Performance Analysis of RIS-Assisted Ambient Backscatter Communication Systems," *IEEE Wireless Communications Letters*, vol. 13, no. 3, pp. 791–795, Dec. 2023.

[31] T. N. Nguyen, N. V. Vinh, B. C. Nguyen, and B. V. Minh, "On performance of RIS-aided bidirectional full-duplex systems with combining of imperfect conditions," *Wireless Networks*, vol. 30, no. 2, pp. 649–660, Feb. 2024.

[32] T.-H. Vu and S. Kim, "Performance analysis of full-duplex two-way ris-based systems with imperfect csi and discrete phase-shift design," *IEEE Commun. Lett.*, vol. 27, no. 2, pp. 512–516, Dec. 2022.

[33] B. C. Nguyen, T. M. Hoang, P. T. Tran, T. N. Nguyen, V.-D. Phan *et al.*, "Cooperative Communications for Improving the Performance of Bidirectional Full-Duplex System With Multiple Reconfigurable Intelligent Surfaces," *IEEE Access*, vol. 9, pp. 134 733–134 742, Sep. 2021.

[34] D. T. Tam, B. C. Nguyen, S. C. Lam, N. Van Vinh, and T. N. Nguyen, "Ser performance of millimeter-wave communications with multiple reconfigurable intelligent surfaces and transmit antenna selection," *AEU-International Journal of Electronics and Communications*, vol. 160, p. 154517, 2023.

[35] L. S. Phu, T. N. Nguyen, M. Voznak, B. C. Nguyen, T. M. Hoang *et al.*, "Improving the Capacity of NOMA Network Using Multiple Aerial Intelligent Reflecting Surfaces," *IEEE Access*, vol. 11, pp. 107 958–107 971, Sep. 2023.

[36] T.-H. Vu, A. Jee, D. B. da Costa, and S. Kim, "STAR-RIS Empowered NOMA Systems With Caching and SWIPT," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 379–396, Dec. 2023.

[37] T.-H. Vu, Q.-V. Pham, T.-T. Nguyen, D. B. da Costa, and S. Kim, "Enhancing RIS-Aided Two-Way Full-Duplex Communication With Nonorthogonal Multiple Access," *IEEE Internet of Things Journal*, vol. 11, no. 11, pp. 19 963–19 977, Feb. 2024.

[38] T.-H. Vu, T. N. Nguyen, T.-T. Nguyen, and S. Kim, "Hybrid Active-Passive STAR-RIS-based NOMA Systems: Energy/Rate-Reliability Trade-offs and Rate Adaptation," *IEEE Wireless Communications Letters*, p. 1, Nov. 2024.

[39] T.-H. Vu, T.-V. Nguyen, D. B. da Costa, and S. Kim, "Intelligent Reflecting Surface-Aided Short-Packet Non-Orthogonal Multiple Access Systems," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 4, pp. 4500–4505, Jan. 2022.

[40] T.-H. Vu, T.-V. Nguyen, Q.-V. Pham, D. B. da Costa, and S. Kim, "STAR-RIS-Enabled Short-Packet NOMA Systems," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 10, pp. 13 764–13 769, May 2023.

[41] D.-T. Vo, T. N. Nguyen, A.-T. Le, V.-D. Phan, and M. Voznak, "Holographic Reconfigurable Intelligent Surface-Aided Downlink NOMA IoT Networks in Short-Packet Communication," *IEEE Access*, vol. 12, pp. 65 266–65 277, May 2024.

[42] R. Kaur, B. Bansal, S. Majhi, S. Jain, C. Huang *et al.*, "A Survey on Reconfigurable Intelligent Surface for

Physical Layer Security of Next-Generation Wireless Communications," *IEEE Open J. Veh. Technol.*, vol. 5, pp. 172–199, Jan. 2024.

[43] W. Yang, R. F. Schaefer, and H. V. Poor, "Finite-blocklength bounds for wiretap channels," in *2016 IEEE International Symposium on Information Theory (ISIT)*. IEEE, pp. 10–15.

[44] H.-M. Wang, Q. Yang, Z. Ding, and H. V. Poor, "Secure Short-Packet Communications for Mission-Critical IoT Applications," *IEEE Trans. Wireless Commun.*, vol. 18, no. 5, pp. 2565–2578, Mar. 2019.

[45] C. Feng, H.-M. Wang, and H. V. Poor, "Reliable and Secure Short-Packet Communications," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1913–1926, Sep. 2021.

[46] C. Li, C. She, N. Yang, and T. Q. S. Quek, "Secure Transmission Rate of Short Packets With Queueing Delay Requirement," *IEEE Trans. Wireless Commun.*, vol. 21, no. 1, pp. 203–218, Jul. 2021.

[47] N. Arı, N. Thomos, and L. Musavian, "Performance Analysis of Short Packet Communications With Multiple Eavesdroppers," *IEEE Trans. Commun.*, vol. 70, no. 10, pp. 6778–6789, Aug. 2022.

[48] X. Chen, N. Zhao, Z. Chang, T. Hämäläinen, and X. Wang, "UAV-Aided Secure Short-Packet Data Collection and Transmission," *IEEE Trans. Commun.*, vol. 71, no. 4, pp. 2475–2486, Feb. 2023.

[49] D. Xu, H. Zhao, and H. Zhu, "Resource Allocation for Secure Short Packet Communications in Wireless Powered IoT Networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 8, pp. 11 000–11 005, Mar. 2023.

[50] S. Qian, "Reliable and Secure Short-Packet Communications in Untrusted Diamond Relay Networks," *IEEE Access*, vol. 11, pp. 24 686–24 695, Mar. 2023.

[51] T.-V. Nguyen, T.-H. Vu, T. Huynh-The, and D. B. da Costa, "Secrecy Performance of Short-Packet Communications in MultiHop IoT Networks With Imperfect CSI," *IEEE Wireless Commun. Lett.*, vol. 13, no. 4, pp. 1093–1097, Feb. 2024.

[52] Z. Xiang, W. Yang, Y. Cai, J. Xiong, Z. Ding *et al.*, "Secure Transmission in a NOMA-Assisted IoT Network With Diversified Communication Requirements," *IEEE IoT J.*, vol. 7, no. 11, pp. 11 157–11 169, May 2020.

[53] X. Lai, T. Wu, Q. Zhang, and J. Qin, "Average Secure BLER Analysis of NOMA Downlink Short-Packet Communication Systems in Flat Rayleigh Fading Channels," *IEEE Trans. Wireless Commun.*, vol. 20, no. 5, pp. 2948–2960, Dec. 2020.

[54] S. Lv, X. Xu, S. Han, X. Tao, and P. Zhang, "Energy-Efficient Secure Short-Packet Transmission in NOMA-Assisted mMTC Networks With Relaying," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 1699–1712, Dec. 2021.

[55] T.-H. Vu, Q.-V. Pham, D. B. da Costa, M. Debbah, and S. Kim, "Physical-Layer Security in Short-Packet NOMA Systems with Untrusted Near Users," in *2023 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, pp. 2023–01.

[56] Z. Feng, H. Lu, N. Zhao, Z. Shi, Y. Chen *et al.*, "Secure Transmission of UAV Control Information via NOMA," *IEEE Trans. Commun.*, vol. 72, no. 8, pp. 4648–4660, Mar. 2024.

[57] K. Yu, Z. Feng, J. Yu, T. Chen, J. Peng *et al.*, "Secure Ultra-Reliable and Low Latency Communication in UAV-Enabled NOMA Wireless Networks," *IEEE Trans. Veh. Technol.*, vol. 73, no. 10, pp. 14 908–14 922, Jun. 2024.

[58] K. Singh, S. K. Singh, and C.-P. Li, "On the Performance Analysis of RIS-Assisted Infinite and Finite Blocklength Communication in Presence of an Eavesdropper," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 854–872, Mar. 2023.

[59] S. Lv, X. Xu, S. Han, and P. Zhang, "RIS-Enhanced Secure Transmission in MTC Networks With Finite Blocklength," *IEEE Trans. Commun.*, vol. 71, no. 6, pp. 3513–3527, Mar. 2023.

[60] G. Xie, C. Yang, and B. Dai, "Secure Finite Blocklength Coding Scheme for the RIS-Aided SIMO Channel with Feedback," in *2022 IEEE Globecom Workshops (GC Wkshps)*. IEEE, pp. 04–08.

[61] G. Xie, C. Yang, Y. Feng, G. Liu, and B. Dai, "Secure Finite Blocklength Coding Schemes for Reconfigurable Intelligent Surface Aided Wireless Channels With Feedback," *IEEE Trans. Commun.*, vol. 71, no. 5, pp. 2931–2946, Mar. 2023.

[62] W. Gao, C. Wang, J. Wang, and Y. Hu, "Joint Resource Allocation and Beamforming Design for Secure Short Packet Communication in RIS-Aided MISO Systems: Invited Paper," in *2024 18th European Conference on Antennas and Propagation (EuCAP)*. IEEE, pp. 17–22.

[63] M.-A. Badiu and J. P. Coon, "Communication through a large reflecting surface with phase errors," *IEEE Wireless Commun. Lett.*, vol. 9, no. 2, pp. 184–188, 2019.

[64] A. Jeffrey and D. Zwillinger, *Table of integrals, series, and products*. Elsevier, 2007.

[65] Y. Yu, H. Chen, Y. Li, Z. Ding, and B. Vucetic, "On the Performance of Non-Orthogonal Multiple Access in Short-Packet Communications," *IEEE Commun. Lett.*, vol. 22, no. 3, pp. 590–593, Dec. 2017.

NGUYEN QUANG SANG received the B.E. degree in Electrical Engineering from Ho Chi Minh City University of Transport, Vietnam, in 2010, the M.E. degree in Telecommunications Engineering from Ho Chi Minh City University of Technology, Vietnam, in 2013, and the Ph.D. degree in Electrical Engineering from the University of Ulsan, South Korea, in 2017. From 2017 to 2021, he was a Lecturer at Duy Tan University, Vietnam. Since May 2021, he has been a Lecturer at Ho Chi Minh City University of Transport, Vietnam. In September 2024, he joined the Post and Telecommunications Institute of Technology, Ho Chi Minh City, as a Lecturer. He also served as a Research Fellow at Queen's University Belfast, United Kingdom, where he contributed to advancements in wireless communications. His research interests include cooperative communications, cognitive radio networks, physical layer security, non-orthogonal multiple access (NOMA), short-packet communications, and backscatter communications. His work primarily focuses on secure and energy-efficient communication solutions for next-generation wireless networks.

HYE-YOUNG KIM received the Ph.D. degree in Computer Science and Engineering from the Korea University, South Korea in February 2005. During her Ph.D. studies, she focused on location management scheme and traffic modeling for mobile IPv6, cellular network and network mobility. She developed a network protocol for 9 years while working as a senior researcher at Hyundai Electronics. Currently, she has been working as a Full Professor at Hongik University, South Korea, since March 2007. Her research interests include traffic modeling, load balancing scheme and copyright technology for digital content on blockchain and web3.

TAN N. NGUYEN (member IEEE) was born in 1986 in Nha Trang City, Vietnam. He received a BS degree in electronics in 2008 from Ho Chi Minh University of Natural Sciences and an MS degree in telecommunications engineering in 2012 from Vietnam National University. He received a Ph.D. in communications technologies in 2019 from the Faculty of Electrical Engineering and Computer Science at VSB – Technical University of Ostrava, Czech Republic. He joined the Faculty of Electrical and Electronics Engineering of Ton Duc Thang University, Vietnam, in 2013, and since then has been lecturing. He started as the Editor-in-Chief of Advances in Electrical and Electronic Engineering (AEEE) journal in 2023. He was appointed as Associate Professor of Electronics in 2024. His major interests are cooperative communications, cognitive radio, signal processing, satellite communication, UAV, and physical layer security.

MINH BUI VU was born on March 02, 1991 in Dong Nai, Vietnam. He graduated in Electrical and Electronic Engineering in 2015 from Nguyen Tat Thanh University, Ho Chi Minh City, Vietnam. End of 2014, he joined the Faculty of Automotive, Mechanical, Electrical and Electronic Engineering of Nguyen Tat Thanh University as Laboratory-Practice management, until in 2017 he was a lecturer. In 2019, he received a Master's degree in Electrical Engineering from Ho Chi Minh City University of Technology and Education, Ho Chi Minh City, Vietnam. His major research interests are Power Electronics, Wireless Networks, Robots, Artificial Neural Network.

PHUONG T. TRAN was born at Ho Chi Minh City, Vietnam. He received B.Eng. and M. Eng. degrees in electrical engineering from Ho Chi Minh University of Technology, Ho Chi Minh City, Vietnam in 2002 and 2005, respectively. In 2007, he became a Vietnam Education Foundation Fellow at Purdue University, U.S.A., where he received his M.S. degree in mathematics and Ph.D. degree in electrical and computer engineering in 2013. In 2013, he joined the Faculty of Electrical and Electronics Engineering of Ton Duc Thang University, Vietnam and served as the Vice Dean of Faculty since October 2014. He is currently a Senior Member of IEEE. His major interests are in the area of wireless communications and network information theory.

TRAN TRUNG DUY was born at Nha Trang City, Vietnam. In 2013, he received the Ph.D degree in electrical engineering from University of Ulsan, South Korea. In 2013, he joined Posts and Telecommunications Institute of Technology, Ho Chi Minh city campus (PTIT-HCM), as a lecturer. From 2017, he is an associate editor for REV Journal on Electronics and Communications Journal and EAI Endorsed Transactions on Industrial Networks and Intelligent Systems Journal. From 2021, he is an associate editor for Frontiers in Communications & Networks Journal, and Journal of Transportation Science and Technology. His major research interests are cooperative communications, cooperative multi-hop, cognitive radio, physical-layer security, energy harvesting, hardware impairments and Fountain codes.

BYOUNG-SEO KIM received his B.S. degree in Electrical Engineering from In-Ha University, Korea in 1998 and his M.S. and Ph.D. degrees in Electrical and Computer Engineering from University of Florida in 2001 and 2004, respectively. His Ph.D. study was supervised by Dr. Yuguang Fang. From Dec. 1997 to June 1999, he worked for Motorola Korea Ltd., Korea as a Computer Integrated Manufacturing Engineer in ATR&D. From Jan. 2005 to Aug. 2007, he worked for Motorola Inc., Schaumburg Illinois, as a Sr. Software Engineer in Networks and Enterprises. In Sept. 2007, he joined the Department of Software and Communications Engineering, Hongik University, Korea, where he is currently a professor. He is IEEE Senior Member and is serving as Associate Editors of IEEE Access, Telecommunication Networks, SPC, AEEE, and Journal of the IEIE. His works have appeared in around 300 publications and 36 patents. His research interests include the design and development of efficient wireless/wired networks and distributed microservice computing.

MIROSLAV VOZNAK (Senior Member, IEEE) received the Ph.D. degree in telecommunications from the Faculty of Electrical Engineering and Computer Science, VSB–Technical University of Ostrava, in 2002, and the Habilitation degree, in 2009. He was appointed as a Full Professor of electronics and communications technologies, in 2017. He has authored or coauthored over 100 articles indexed in SCI/SCIE journals. According to the Stanford University study released in 2020, he is one of the World's Top 2% of scientists in networking and telecommunications and information and communications technologies. He participated in six projects funded by EU in programs managed directly by European Commission. His research interests include ICT, especially on quality of service and experience, network security, wireless networks, and big data analytics. He is also a Principal Investigator in the research project QUANTUM5 funded by NATO, which focuses on the application of quantum cryptography in 5G campus networks. He served as a General Chair for the 11th IFIP Wireless and Mobile Networking Conference, in 2018, and the 24th IEEE/ACM International Symposium on Distributed Simulation and Real Time Applications, in 2020.