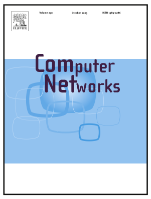
Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet



Research Paper

Novel secure user scheduling for uplink wireless networks against potential eavesdroppers

Woong Son [a,1], Ki-Hun Lee [b,1], Heejung Yu [c,*], Bang Chul Jung [d,*]

[a] C4I R&D Lab., LIG Nex1 Co., Ltd., Yongin, 16911, South Korea
[b] Department of AI Convergence, Kunsan National University, 54150, Gunsan, South Korea
[c] Department of Electronics and Information Engineering, Korea University, 30019, Sejong, South Korea
[d] Department of Electrical and Computer Engineering, Ajou University, 16499, Suwon, South Korea

ARTICLE INFO

Keywords:
Physical-layer security
Potential eavesdroppers
Opportunistic feedback
Secrecy outage probability
Effective secrecy throughput
Multi-user diversity

ABSTRACT

In this paper, we address security threats in an uplink wireless communication network comprising a single base station (BS), multiple legitimate user equipment (UEs), and potential eavesdroppers (EVEs). In this scenario, the EVEs may unintentionally intercept the uplink transmissions of legitimate UEs, posing significant risks to confidentiality. To overcome these threats, we propose novel analytical two-step opportunistic feedback (TOF) strategies to enhance physical-layer security (PLS) under the assumption that each legitimate UE has local channel state information (CSI). The TOF strategy consists of two stages: in the first stage, legitimate UEs perform conservative feedback for user scheduling, assuming all potential EVEs are eavesdropping. If no UE meets the feedback condition, the conventional opportunistic feedback (OF) mechanism is applied in the second stage, where legitimate UEs with channel gains above a predefined threshold send feedback to the BS. We mathematically analyze the secrecy outage probability (SOP) and effective secrecy throughput (EST) of the proposed TOF strategies. Simulation results demonstrate that the TOF strategies significantly outperform the conventional OF approach, achieving lower SOP and higher EST across various scenarios.

1. Introduction

Security has been considered one of the most significant issues in wireless communication networks, given their role in transmitting privacy-sensitive personal and public data through inherently vulnerable broadcast radio signals [1,2]. In particular, modern communication systems are rapidly evolving into the foundational infrastructure for various services, including internet-of-things (IoT), smart cities, eHealth, Industry 4.0, blockchain, and autonomous vehicles. Consequently, the need for robustbreak security and privacy measures in wireless networks has become even more pressing [3–6]. Recognizing these challenges, the International Telecommunication Union Radiocommunication Sector (ITU-R) has highlighted security as one of the fundamental requirements for sixth-generation (6G) mobile communication systems, as outlined in the International Mobile Telecommunications (IMT)-2030 framework [7]. These developments have garnered significant attention from both academic and industrial researchers, underscoring the urgency of addressing security in next-generation wireless networks.

Conventional information and network security methods, including shared-key and private-key encryption, have demonstrated robust security performance under the assumption that eavesdroppers (EVEs) possess limited computational capabilities. However, the advent of EVEs with advanced computational power, such as quantum computing, poses a significant threat to these encryption techniques. To deal with this challenge, physical-layer security (PLS) has emerged as a promising solution, leveraging the inherent properties of the wireless medium to ensure confidentiality independent of the computational capabilities of EVEs [6,8,9]. In particular, PLS has garnered considerable attention as one of the most promising security-providing approaches for various wireless communication networks [10–12].

Based on information theory, the concept of PLS and its performance measures against EVEs' eavesdropping attempts were first explored in [13,14]. These studies paved the way for a theoretical framework for designing wireless communication systems to enable secure transmission even in the presence of EVEs. They also played a crucial role in laying the groundwork for developing feasible PLS techniques that can be implemented in practical wireless networks. Subsequent studies have analyzed PLS performance, e.g., secrecy rate, under various channel models, including discrete memoryless wire-tap channels [13], Gaussian wire-tap channels [14], quasi-static fading channels [15], Gaussian

[*] Corresponding authors.
E-mail addresses: woong.son@lignex1.com (W. Son), kihun@kunsan.ac.kr (K.-H. Lee), heejungyu@korea.ac.kr (H. Yu), bcjung@ajou.ac.kr (B.C. Jung).
[1] Woong Son and Ki-Hun Lee contributed equally to this work.

https://doi.org/10.1016/j.comnet.2025.111825
Received 1 February 2025; Received in revised form 3 August 2025; Accepted 31 October 2025
Available online 3 November 2025

multiple access wire-tap channels [16], and wire-tap channels with multiple antennas [17,18]. These analyses have progressively advanced PLS's theoretical and practical understanding across various wireless network configurations.

To achieve a high secrecy rate, extensive research has been studied on secure transmission techniques, including secure beamforming, artificial noise (AN) generation, and user scheduling, in various network configurations [19–25]. Furthermore, PLS techniques based on innovative communication technologies, such as millimeter-wave (mmWave) and Terahertz (THz) communications, massive multiple-input multiple-output (mMIMO), non-orthogonal multiple access (NOMA), cooperative relaying and backscatter communications, etc., have been developed [26–32]. These innovations have significantly enhanced the robustness and adaptability of PLS strategies, paving the way for their application in complex and diverse wireless networks.

The aforementioned PLS techniques have primarily addressed *passive* eavesdropping scenarios, where EVEs attempt to intercept and decode private messages of legitimate users without emitting any signals. On the other hand, other eavesdropping scenarios have also been investigated, including *active* and *potential* EVEs. In the *active* eavesdropping scenario, EVEs not only try to intercept private messages for legitimate users but also transmit disruptive signals to execute attacks, such as pilot contamination, jamming, and false information feedback, leading to potential network malfunctions [33–35]. In contrast, *potential* EVEs operate within the network and selectively attempt to eavesdrop based on their operational context.

A representative example of potential eavesdropping is observed in time division multiple access (TDMA) networks, where multiple user equipment (UEs) access a base station (BS) in distinct time slots. In this scenario, the scheduled UE acts as a legitimate user, while the unscheduled UEs may serve as potential EVEs [36–41]. Importantly, legitimate UEs can access full or partial channel state information (CSI) of these potential EVEs. Another notable case involves malicious radar targets, whose location and CSI can be estimated using radar functionalities [42]. Similarly, untrusted relays operating in an amplify-and-forward (AF) manner to assist legitimate communications while attempting to decode intercepted signals also exemplify potential EVEs [32,43,44]. In other words, the term *potential* is used in the sense that such communication entities can also participate in their legitimate networks while simultaneously posing a security threat by eavesdropping on communications.

Building on such scenarios, PLS techniques designed to counter potential EVEs have recently garnered considerable attention [41,44–48]. In [41], the PLS performance was analyzed in downlink multi-user multiple-input single-output (MU-MISO) cellular networks under the presence of potential EVEs, where an opportunistic feedback strategy was employed to enhance security performance. In [45], the authors studied energy-efficient cooperative secure transmission in downlink mmWave vehicular networks with potential eavesdropping vehicles, where a deep recurrent reinforcement learning (DRRL) framework was employed to jointly optimize beam allocation, relay selection, and power control. In [44], a low-complexity space-time code-based PLS scheme was proposed for two-way untrusted relay networks, in which the relay primarily assists both terminals while potentially attempting to decode their confidential messages without authorization. Furthermore, advanced communication technologies such as integrated sensing and communication (ISAC) [46] and reconfigurable intelligent surface (RIS) [47,48] have also been incorporated into PLS frameworks. Specifically, in [46], the authors developed a sensing-assisted PLS framework, where an ISAC BS applies the combined Capon and approximate maximum likelihood (CAML) technique to estimate the directions of potential EVEs. In [47], the authors investigated transmit power minimization for secure communication in simultaneously transmitting and reflecting (STAR)-RIS-assisted multiple-input multiple-output (MIMO) networks, where the transmit covariance matrix and the STAR-RIS's transmission and reflection coefficients were jointly optimized using a penalty-based alternating optimization algorithm. In [48], a robust PLS scheme was proposed for STAR-RIS-assisted wireless networks under full-space coverage, where transmit beamforming and STAR-RIS configuration were jointly optimized in the presence of a potential EVE with uncertain location and partial CSI.

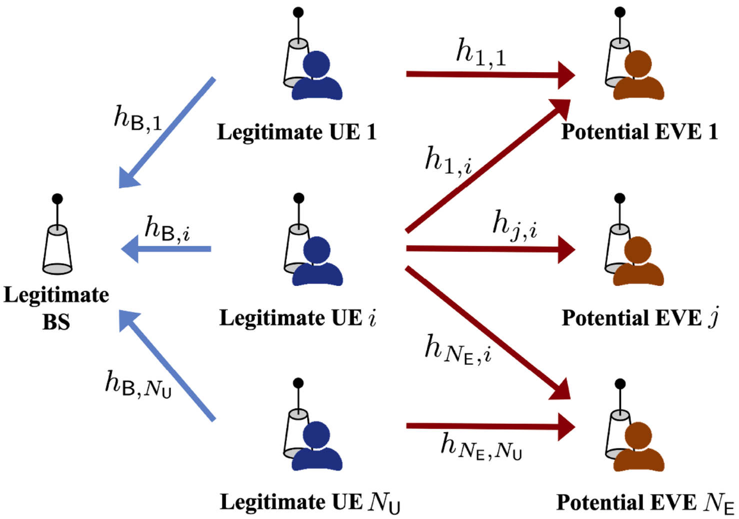


Fig. 1. Illustration of an uplink wireless network with multiple legitimate UEs and potential EVEs.

The behavior of potential EVEs has been modeled based on their eavesdropping probability, and PLS performances against potential EVEs have been investigated in cellular downlink [39,41] and uplink networks [37], respectively. However, no prior work has focused on user feedback schemes specifically designed to enhance PLS performance in uplink wireless networks against potential EVEs. In this paper, we propose novel analytical user scheduling strategies to address this gap, aiming to improve PLS performance in uplink wireless networks. We mathematically analyze the secrecy outage probability (SOP) and effective secrecy throughput (EST) performance of the proposed strategies. To validate their efficacy, we compare the performance with the benchmarks, including the conventional opportunistic feedback (OF) strategy.

The remainder of this paper is organized as follows. In Section 2, we introduce the system model of uplink wireless networks with potential EVEs and conventional OF strategy. In Section 3, we elaborate on the proposed two-step opportunistic feedback (TOF) strategies. In Section 4, we mathematically analyze the PLS performance of the proposed TOF strategies. In Section 5, numerical results are presented with detailed explanations. Finally, Section 6 concludes the paper, summarizing key findings and suggesting future research directions.

2. System model and preliminaries

We consider an uplink wireless network consisting of a base station (BS), N_U legitimate user equipment (UEs), and N_E potential eavesdroppers (EVEs), as depicted in Fig. 1. Here, the potential EVEs are also legitimate UEs that are either served by the BS or another neighboring BS but are inactive in the current time slot [49]. These EVEs may unintentionally overhear data transmission between the BS and legitimate UEs with an eavesdropping probability $\alpha \in [0,1]$.[1] All communication nodes are equipped with a single antenna, and all wireless links in the network are modeled as undergoing independent Rayleigh fading.[2]

[1] This is called the random eavesdropping (RE) strategy. If $\alpha = 1$, it is defined as the full eavesdropping (FE) strategy.

[2] Although we consider single-antenna system models in this paper, the proposed feedback strategies can be readily extended to multi-antenna scenarios by incorporating spatial channel characteristics, depending on the employed

Specifically, in Fig. 1, $h_{\mathsf{B},i} \sim \mathcal{CN}(0, \sigma^2_{\mathsf{B},i})$ and $h_{j,i} \sim \mathcal{CN}(0, \sigma^2_{j,i})$ represent wireless channel coefficients from the ith legitimate UE to the BS and to the jth potential EVE, respectively, where $i \in \mathcal{N}_{\mathsf{U}} \triangleq \{1, 2, \ldots, N_{\mathsf{U}}\}$ and $j \in \mathcal{N}_{\mathsf{E}} \triangleq \{1, 2, \ldots, N_{\mathsf{E}}\}$. The channel variance $\sigma^2_{j,i} \triangleq d^{-n}_{j,i}$ reflects large-scale fading effect, where $d_{j,i}$ denotes the distance between nodes j and i, and n represents the path loss exponent. All wireless channel coefficients are assumed to remain constant for at least one frame transmission between legitimate nodes. For the sake of brevity, in this paper, we assume identical channel variances for all legitimate and eavesdropping links, i.e., $\sigma^2_{\mathsf{B},i} = \sigma^2_{\mathsf{B}}$ and $\sigma^2_{j,i} = \sigma^2_{\mathsf{E}}$ for all $i \in \mathcal{N}_{\mathsf{U}}$ and $j \in \mathcal{N}_{\mathsf{E}}$. Note that the proposed user scheduling strategies are readily generalizable to any network topology, even without this assumption. We also assume that the EVEs operate independently; that is, they do not share any information intercepted from legitimate links with each other.

As noted earlier, unlike active or passive EVEs, potential EVEs are legitimate UEs that do not participate in the feedback phase in the current time slot, e.g., due to having no uplink data to transmit. Therefore, legitimate UEs can obtain the CSI of potential EVEs. For example, they can estimate the CSI of surrounding nodes, including potential EVEs, by leveraging periodically transmitted pilot signals and the channel reciprocity property in time division duplex (TDD) systems. This is particularly relevant to uplink networks, where all UEs—including those that are temporarily inactive—periodically send pilot signals for synchronization and channel estimation purposes at the BS. Therefore, the CSI of potential EVEs remains accessible for secure scheduling purposes.

2.1. Conventional opportunistic feedback (OF) strategy

In the opportunistic feedback (OF) strategy proposed in [38,41], the ith legitimate UE sends its channel gain $|h_{\mathsf{B},i}|^2$ to the BS when it is higher than or equal to a certain threshold ζ, i.e., $|h_{\mathsf{B},i}|^2 \geq \zeta$, where ζ denotes the channel gain threshold for uplink feedback. Based on this feedback, the BS schedules a legitimate UE for transmission. Let $\mathcal{M}_{\mathsf{U}} = \{i \mid |h_{\mathsf{B},i}|^2 \geq \zeta, i \in \mathcal{N}_{\mathsf{U}}\}$ be the set of UEs that send their channel gains to the BS. In the special case where $\zeta = 0$, all legitimate UEs send their channel gains, i.e., $\mathcal{M}_{\mathsf{U}} = \mathcal{N}_{\mathsf{U}}$; this case is called a full feedback (FF) strategy. Once feedback is received, the BS schedules the $i^\star$th UE with the highest channel gain among the UEs in $\mathcal{M}_{\mathsf{U}}$, i.e., $i^\star = \arg\max_{i \in \mathcal{M}_{\mathsf{U}}} |h_{\mathsf{B},i}|^2$. Such a simple scheduling strategy is employed because we focus on the feedback procedure. It is worth noting that scheduling is beyond the scope of this paper, and the proposed techniques are not restricted to a specific user scheduling manner.

2.2. Secrecy outage probability (SOP)

When the ith legitimate UE sends an information-bearing signal to the BS with an average transmission power P_i, the theoretical achievable secrecy rate is defined as

$$R_{\mathrm{sec},i} \triangleq \log_2\left(1 + |h_{\mathsf{B},i}|^2 \rho_i\right) - \max_{j \in \mathcal{M}_{\mathsf{E}}} \log_2\left(1 + |h_{j,i}|^2 \rho_i\right) = \log_2\left(\frac{1 + |h_{\mathsf{B},i}|^2 \rho_i}{1 + \max_{j \in \mathcal{M}_{\mathsf{E}}} |h_{j,i}|^2 \rho_i}\right),$$

where $\mathcal{M}_{\mathsf{E}} \subseteq \mathcal{N}_{\mathsf{E}}$ represents the set of activated potential EVEs attempting to intercept the transmission. It is noteworthy that the activation probability α of each EVE is not explicitly included here, as the SOP is defined conditionally on a fixed realization of the active EVE set. The influence of α is subsequently incorporated when considering all possible active EVE sets, as shown in (5), (17), and (25).

The term $\rho_i \triangleq P_i/N_0$ denotes the average transmit signal-to-noise ratio (SNR), where N_0 is the power of an additive white Gaussian noise (AWGN) at the receive sides, i.e., the BS and potential EVEs. This formulation captures the competitive interplay between the legitimate transmission channel and the potential eavesdropping channels, serving as a foundation for evaluating secrecy performance.

The secrecy outage probability (SOP) quantifies the likelihood that the achievable secrecy rate is lower than a target secrecy rate. That is, the SOP is expressed as

$$P_{\mathrm{out},i}\left(R_{\mathrm{o}}\right) \triangleq \Pr\left(R_{\mathrm{sec},i} < R_{\mathrm{o}}\right),$$

where R_{o} [bps/Hz] represents the target secrecy rate. This means that a secrecy outage occurs when the instantaneous achievable secrecy rate falls below the target rate.

3. Proposed two-step user scheduling strategies

We propose a novel *two-step opportunistic feedback* (TOF) strategy against multiple potential EVEs to improve PLS performance in uplink wireless communication networks. Furthermore, considering realization, we extend the TOF to a practical *two-step opportunistic feedback with quantization* (TOFQ) strategy. For simplicity, we assume that all UEs have the same transmit power P.

3.1. Two-step opportunistic feedback (TOF) strategy

3.1.1. Step I

In the first step, feedback from each legitimate UE is performed under the assumption that all EVEs attempt to eavesdrop on uplink transmissions from the legitimate UEs. Specifically, the ith legitimate UE sends its channel gain $|h_{\mathsf{B},i}|^2$ to the BS so that it can be scheduled by the BS if the following condition of the worst-case secrecy rate is satisfied:

$$\log_2\left(\frac{1 + |h_{\mathsf{B},i}|^2 \rho}{1 + \max_{j \in \mathcal{N}_{\mathsf{E}}} |h_{j,i}|^2 \rho}\right) \geq R_{\mathrm{o}}. \tag{1}$$

Note that since each UE feeds back its channel gain under the assumption that all N_{E} potential EVEs attempt to eavesdrop, if at least one UE out of the N_{U} legitimate UEs meets the worst-case secrecy rate condition, a secrecy outage definitively does not occur regardless of the BS's user scheduling.

3.1.2. Step II

If there is no legitimate UE satisfying the feedback condition in (1), the conventional OF strategy in Section 2.1 is employed. In other words, the ith UE feeds its channel gain back to the BS when $|h_{\mathsf{B},i}|^2 \geq \zeta$; the BS then schedules a UE with the highest channel gain among those UEs.

This fallback is motivated by the need to maintain communication continuity even when the secrecy rate constraint cannot be satisfied. Although the OF strategy may compromise secrecy performance, it enables the BS to still schedule a legitimate UE for uplink transmission, thereby avoiding communication outages under unfavorable channel conditions. It is worth noting that during both phases, the ith UE only exploits CSI from itself to the BS and potential EVEs and does not require the instantaneous activity of each EVE.

The transition from the first to the second step is managed by the BS. If no legitimate UE transmits feedback within the designated interval, the BS detects the absence of valid uplink signals and initiates the second step via a timer-based mechanism or an internal control signal. The BS then broadcasts a scheduling control message to prompt legitimate UEs to proceed with the second step.

3.2. Two-step opportunistic feedback with quantization (TOFQ) strategy

The aforementioned TOF procedure requires the channel gain feedback of a continuous real value, and such a feedback policy causes significant overhead in the uplink control signaling. As an extension of TOF, considering the implementation in realistic wireless networks, a

beamforming technique–such as maximum ratio combining (MRC) or secure beamforming. We leave such extensions to future work, as our current focus is to investigate the fundamental performance trends of the proposed schemes.

practical TOF strategy based on quantization (TOFQ) is developed in this subsection. Briefly, the TOFQ strategy has the same overall procedure as the TOF except that the UE feeds back the quantized channel gains instead of continuous channel gain values. An L-bit quantization of the channel gain status from a legitimate UE to the BS is assumed.

3.2.1. *Step I*

If the ith legitimate UE satisfies the feedback condition of (1), it feeds back the bit stream with all ones, $11\dots1_{(2)}$, i.e., the largest binary value that can be represented by L bits. As in the TOF strategy, a secrecy outage does not occur definitively if at least one legitimate UE feeds back the bit stream with all ones.

3.2.2. *Step II*

In the second step, the ith legitimate UE feeds back a bit stream between $00\dots00_{(2)}$ and $11\dots10_{(2)}$ according to the L-bit quantization of the channel gain $|h_{\mathsf{B},i}|^2$. The more detailed process is illustrated in Fig. 2 with the following simple example.

Example 1 (TOFQ with two quantized bits for channel gain feedback). As shown in Fig. 2, when the number of bits for channel gain quantization $L = 2$, three $(2^L - 1)$ regions (Region 0, 1, and 2) for channel gain feedback can be defined in Step II, and each channel gain region can be sequentially represented by $00_{(2)}, 01_{(2)}$, and $10_{(2)}$. Recall that $11_{(2)}$ has already been defined in Step I. We define a set of $2^L - 2$ channel gain regions with $\mathcal{K} \triangleq \{0, 1, \dots, 2^L - 2\}$. The boundaries between two adjacent regions are determined so that each region has the same probability of channel gain realization, that is, $P_{\text{region}}(L) = 1/(2^L - 1) = 1/3$. Let us define two random variables as $X \triangleq |h_{\mathsf{B},i}|^2$ for $i \in \mathcal{N}_\mathsf{U}$ and $\overline{X} \triangleq |h_{\mathsf{B},i}|^2$ for $i \in \mathcal{M}_\mathsf{U} = \{i||h_{\mathsf{B},i}|^2 \geq \zeta, i \in \mathcal{N}_\mathsf{U}\}$. The probability density function (PDF) and cumulative distribution function (CDF) of X, denoted by $f_X(x)$ and $F_X(x)$, are given by

$$f_X(x) = \frac{1}{\sigma_\mathsf{B}^2} \exp\left(-\frac{x}{\sigma_\mathsf{B}^2}\right) \tag{2}$$

and

$$F_X(x) = 1 - \exp\left(-\frac{x}{\sigma_\mathsf{B}^2}\right), \tag{3}$$

respectively. Since the PDF of $\overline{X}, f_{\overline{X}}(x)$, is given by

$$f_{\overline{X}}(x) = \frac{f_X(x)}{1 - F_X(\zeta)} = \frac{1}{\sigma_\mathsf{B}^2} \exp\left(-\frac{x-\zeta}{\sigma_\mathsf{B}^2}\right) \tag{4}$$

from (2) and (3), the region boundary η_k for $k \in \mathcal{K}$ is obtained by $\eta_0 = \zeta$ and $\eta_k = -\sigma_\mathsf{B}^2 \ln(e^{-(\eta_{k-1}-\eta_0)/\sigma_\mathsf{B}^2} - (2^L - 1)^{-1}) + \eta_0$ for $k > 0$; e.g., when $L = 2, \sigma_\mathsf{B}^2 = 1$, and $\zeta = 1$, the region boundaries are given by $\eta_0 = 1, \eta_1 \approx 1.4055$, and $\eta_2 \approx 2.0986$, respectively.

The BS then schedules a legitimate UE that feeds back the highest quantized channel gain. If multiple UEs send the highest quantized channel gain to the BS, the BS randomly schedules one of them.

4. Secrecy performance analysis

In this section, we mathematically analyze the SOP performance of the proposed TOF and TOFQ strategies in an uplink wireless network with potential EVEs. Before deriving the analysis of the proposed strategies, we reanalyze the SOP of the conventional OF strategy when applying it to the uplink network.

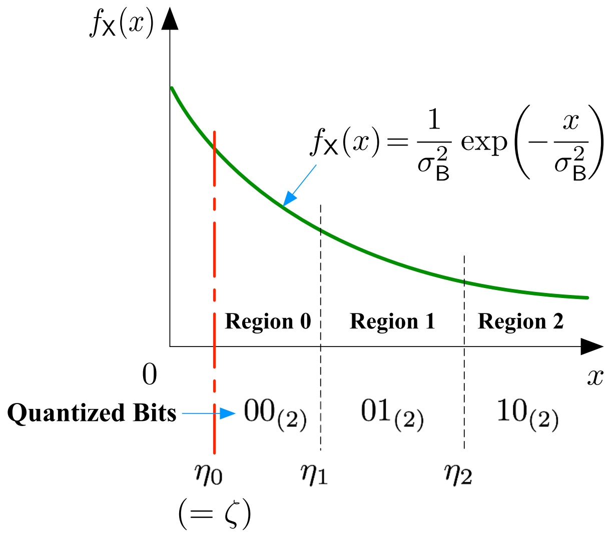


Fig. 2. An example of quantized channel gain region when $L = 2$ in the proposed TOFQ strategy.

4.1. *Conventional opportunistic feedback strategy*

From [38, Theorem 1], the SOP for the conventional OF strategy, denoted by $P_{\text{out}}^{\text{OF}}(\mathcal{N}_\mathsf{U}, \mathcal{N}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, \zeta, \alpha, R_\text{o})$, is given as follows:

$$\begin{aligned}
&P_{\text{out}}^{\text{OF}}\left(\mathcal{N}_\mathsf{U}, \mathcal{N}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, \zeta, \alpha, R_\text{o}\right)\\
&= 1 - P_{\text{non}}^{\text{OF}}\left(\mathcal{N}_\mathsf{U}, \mathcal{N}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, \zeta, \alpha, R_\text{o}\right)\\
&= 1 - \textstyle\sum_{\substack{\mathcal{M}_\mathsf{U} \in \mathcal{P}(\mathcal{N}_\mathsf{U})\\ \mathcal{M}_\mathsf{U} \neq \varnothing}} P_\mathsf{U}^{\text{OF}}(\sigma_\mathsf{B}^2, \zeta)^{|\mathcal{M}_\mathsf{U}|}\left(1 - P_\mathsf{U}^{\text{OF}}(\sigma_\mathsf{B}^2, \zeta)\right)^{N_\mathsf{U}-|\mathcal{M}_\mathsf{U}|}\\
&\quad \times \Bigg[\textstyle\sum_{\substack{\mathcal{M}_\mathsf{E} \in \mathcal{P}(\mathcal{N}_\mathsf{E})\\ \mathcal{M}_\mathsf{E} \neq \varnothing}} \alpha^{|\mathcal{M}_\mathsf{E}|}(1-\alpha)^{N_\mathsf{E}-|\mathcal{M}_\mathsf{E}|} P_{\text{non}}^{\text{OF}}\left(\mathcal{M}_\mathsf{U}, \mathcal{M}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, \zeta, R_\text{o}\right)\\
&\qquad + (1-\alpha)^{N_\mathsf{E}} P_{\text{non}}^{\text{OF}}\left(\mathcal{M}_\mathsf{U}, \sigma_\mathsf{B}^2, \zeta, R_\text{o}\right)\Bigg],
\end{aligned} \tag{5}$$

where $\mathcal{P}(\cdot)$ denotes the power set operator and $|\cdot|$ represents the cardinality of a set, which is defined as the number of elements in the set. Furthermore, $P_{\text{non}}^{\text{OF}}(\cdot)$ and $P_\mathsf{U}^{\text{OF}}(\cdot)$ represent the secrecy non-outage probability (SNOP) and the feedback probability of each legitimate UE, respectively. The SNOP expression has the following three cases, depending on the particular subsets of legitimate UEs and EVEs considered:

- $P_{\text{non}}^{\text{OF}}\left(\mathcal{N}_\mathsf{U}, \mathcal{N}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, \zeta, \alpha, R_\text{o}\right)$ denotes the overall SNOP of the system, considering all legitimate UEs and potential EVEs,
- $P_{\text{non}}^{\text{OF}}\left(\mathcal{M}_\mathsf{U}, \mathcal{M}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, \zeta, R_\text{o}\right)$ represents the SNOP when $\mathcal{M}_\mathsf{E}$ potential EVEs attempt to eavesdrop and $\mathcal{M}_\mathsf{U}$ out of $\mathcal{N}_\mathsf{U}$ legitimate UEs feed their channel gain back to the BS
- $P_{\text{non}}^{\text{OF}}\left(\mathcal{M}_\mathsf{U}, \sigma_\mathsf{B}^2, \zeta, R_\text{o}\right)$ denotes the SNOP when $\mathcal{M}_\mathsf{U}$ legitimate UEs send feedback, and there are no potential EVEs attempting to eavesdrop, i.e., $\mathcal{M}_\mathsf{E} = \varnothing$.

First, $P_{\text{non}}^{\text{OF}}(\mathcal{M}_\mathsf{U}, \mathcal{M}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, \zeta, R_\text{o})$, is derived as follows:

$$\begin{aligned}
&P_{\text{non}}^{\text{OF}}\left(\mathcal{M}_\mathsf{U}, \mathcal{M}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, \zeta, R_\text{o}\right)\\
&= \Pr\left(\log_2\left(\frac{1+|h_{\mathsf{B},i^\star}|^2\rho}{1+\max\limits_{j\in\mathcal{M}_\mathsf{E}}|h_{j,i^\star}|^2\rho}\right) \geq R_\text{o} \,\middle|\, |h_{\mathsf{B},i^\star}|^2 \geq \zeta\right)\\
&= \Pr\left(\max\nolimits_{j\in\mathcal{M}_\mathsf{E}}|h_{j,i^\star}|^2 \leq \frac{1}{\rho}\left(\frac{1+|h_{\mathsf{B},i^\star}|^2\rho}{2^{R_\text{o}}} - 1\right) \,\middle|\, |h_{\mathsf{B},i^\star}|^2 \geq \zeta\right)\\
&= \textstyle\int_\theta^\infty f_{\widetilde{X}}(x) F_{\widetilde{Y}}\left(\frac{1}{\rho}\left(\frac{1+x\rho}{2^{R_\text{o}}} - 1\right)\right) dx,
\end{aligned} \tag{6}$$

where two random variables are defined as $\widetilde{X} \triangleq \max\limits_{i\in\mathcal{M}_\mathsf{U}} |h_{\mathsf{B},i}|^2$ and $\widetilde{Y} \triangleq \max\limits_{j\in\mathcal{M}_\mathsf{E}} |h_{j,i}|^2$. Since the PDF of $\widetilde{X}$ and the CDF of $\widetilde{Y}$, denoted by $f_{\widetilde{X}}(x)$ and

$F_{\widetilde{Y}}(y)$, respectively, are given by

$$f_{\widetilde{X}}(x)=\frac{M_{\mathrm{U}}}{\sigma_{\mathrm{B}}^2}\exp\left(-\frac{x-\zeta}{\sigma_{\mathrm{B}}^2}\right)\left(1-\exp\left(-\frac{x-\zeta}{\sigma_{\mathrm{B}}^2}\right)\right)^{M_{\mathrm{U}}-1}$$
$$=\frac{M_{\mathrm{U}}}{\sigma_{\mathrm{B}}^2}\sum_{m_{\mathrm{U}}=0}^{M_{\mathrm{U}}-1}\binom{M_{\mathrm{U}}-1}{m_{\mathrm{U}}}(-1)^{m_{\mathrm{U}}}\exp\left(-\frac{(m_{\mathrm{U}}+1)(x-\zeta)}{\sigma_{\mathrm{B}}^2}\right) \tag{7}$$

and

$$F_{\widetilde{Y}}(y)=\left(1-e^{-\frac{y}{\sigma_{\mathrm{E}}^2}}\right)^{M_{\mathrm{E}}}=\sum_{m_{\mathrm{E}}=0}^{M_{\mathrm{E}}}\binom{M_{\mathrm{E}}}{m_{\mathrm{E}}}(-1)^{m_{\mathrm{E}}}\exp\left(-\frac{m_{\mathrm{E}}y}{\sigma_{\mathrm{E}}^2}\right), \tag{8}$$

where $M_{\mathrm{U}}=|\mathcal{M}_{\mathrm{U}}|$ and $M_{\mathrm{E}}=|\mathcal{M}_{\mathrm{E}}|$, (6) is derived as follows:

$$P_{\mathrm{non}}^{\mathrm{OF}}(\mathcal{M}_{\mathrm{U}},\mathcal{M}_{\mathrm{E}},\sigma_{\mathrm{B}}^2,\sigma_{\mathrm{E}}^2,\zeta,R_{\mathrm{o}})$$
$$=\sum_{m_{\mathrm{U}}=0}^{M_{\mathrm{U}}-1}\sum_{m_{\mathrm{E}}=0}^{M_{\mathrm{E}}}\binom{M_{\mathrm{U}}-1}{m_{\mathrm{U}}}\binom{M_{\mathrm{E}}}{m_{\mathrm{E}}}\frac{(-1)^{m_{\mathrm{U}}+m_{\mathrm{E}}}\sigma_{\mathrm{E}}^2M_{\mathrm{U}}2^{R_{\mathrm{o}}}}{\sigma_{\mathrm{E}}^2(m_{\mathrm{U}}+1)2^{R_{\mathrm{o}}}+\sigma_{\mathrm{B}}^2m_{\mathrm{E}}}$$
$$\times\exp\left(-\frac{(m_{\mathrm{U}}+1)(\theta-\zeta)}{\sigma_{\mathrm{B}}^2}-\frac{m_{\mathrm{E}}}{\sigma_{\mathrm{E}}^2\rho}\left(\frac{1+\theta\rho}{2^{R_{\mathrm{o}}}}-1\right)\right), \tag{9}$$

where

$$\theta=\begin{cases}\frac{2^{R_{\mathrm{o}}}-1}{\rho}, & \text{if } \zeta<\frac{2^{R_{\mathrm{o}}}-1}{\rho},\\ \zeta, & \text{otherwise.}\end{cases} \tag{10}$$

Moreover, $P_{\mathrm{non}}^{\mathrm{OF}}(\mathcal{M}_{\mathrm{U}},\sigma_{\mathrm{B}}^2,\zeta,R_{\mathrm{o}})$ is derived as follows:

$$P_{\mathrm{non}}^{\mathrm{OF}}(\mathcal{M}_{\mathrm{U}},\sigma_{\mathrm{B}}^2,\zeta,R_{\mathrm{o}})=\Pr\left(\log_2\left(1+|h_{\mathrm{B},i^\star}|^2\rho\right)\geq R_{\mathrm{o}}\middle||h_{\mathrm{B},i^\star}|^2\geq\zeta\right)$$
$$=1-F_{\widetilde{X}}(\theta)=1-\left(1-\exp\left(-\frac{\theta-\zeta}{\sigma_{\mathrm{B}}^2}\right)\right)^{M_{\mathrm{U}}}, \tag{11}$$

since the CDF of $\widetilde{X}$, $F_{\widetilde{X}}(x)$, is given by

$$F_{\widetilde{X}}(x)=\left(1-\exp\left(-\frac{x-\zeta}{\sigma_{\mathrm{B}}^2}\right)\right)^{M_{\mathrm{U}}}. \tag{12}$$

Finally, the feedback probability of each legitimate UE, denoted by $P_{\mathrm{U}}^{\mathrm{OF}}\left(\sigma_{\mathrm{B}}^2,\zeta\right)$, is given by

$$P_{\mathrm{U}}^{\mathrm{OF}}\left(\sigma_{\mathrm{B}}^2,\zeta\right)=\Pr\left(|h_{\mathrm{B},i}|^2\geq\zeta\right)=\exp\left(-\frac{\zeta}{\sigma_{\mathrm{B}}^2}\right), \tag{13}$$

because $|h_{\mathrm{B},i}|^2$ is a random variable following an independent and identically distributed exponential distribution with a rate parameter of $1/\sigma_{\mathrm{B}}^2$.

A closed-form expression of the SOP for the conventional OF strategy in an uplink wireless network with potential EVEs is then obtained by plugging (9), (11), and (13) into (5).

4.2. Proposed two-step OF (TOF)

Now, we analyze the proposed TOF strategy in Section 3.1. Before presenting the analysis results, we define an additional random variable $\overline{Y}\triangleq\max_{j\in\mathcal{N}_{\mathrm{E}}}|h_{j,i}|^2$ in addition to (2)–(4), (7), (8), and (12) that is required during derivation. The CDF of $\overline{Y}$, $F_{\overline{Y}}(y)$, is given by

$$F_{\overline{Y}}(y)=\left(1-e^{-\frac{y}{\sigma_{\mathrm{E}}^2}}\right)^{N_{\mathrm{E}}}=\sum_{m_{\mathrm{E}}=0}^{N_{\mathrm{E}}}\binom{N_{\mathrm{E}}}{m_{\mathrm{E}}}(-1)^{m_{\mathrm{E}}}\exp\left(-\frac{m_{\mathrm{E}}y}{\sigma_{\mathrm{E}}^2}\right). \tag{14}$$

For a given topology and target secrecy rate R_{o} [bps/Hz], the SOP of the proposed TOF strategy, denoted by $P_{\mathrm{out}}^{\mathrm{TOF}}(\mathcal{N}_{\mathrm{U}},\mathcal{N}_{\mathrm{E}},\sigma_{\mathrm{B}}^2,\sigma_{\mathrm{E}}^2,\alpha,\zeta,R_{\mathrm{o}})$, can be defined as follows:

$$P_{\mathrm{out}}^{\mathrm{TOF}}(\mathcal{N}_{\mathrm{U}},\mathcal{N}_{\mathrm{E}},\sigma_{\mathrm{B}}^2,\sigma_{\mathrm{E}}^2,\alpha,\zeta,R_{\mathrm{o}}) \tag{15}$$
$$=1-\Big[P_{\mathrm{non},1}^{\mathrm{TOF}}(\mathcal{N}_{\mathrm{U}},\mathcal{N}_{\mathrm{E}},\sigma_{\mathrm{B}}^2,\sigma_{\mathrm{E}}^2,R_{\mathrm{o}})$$
$$+\left(1-P_{\mathrm{non},1}^{\mathrm{TOF}}(\mathcal{N}_{\mathrm{U}},\mathcal{N}_{\mathrm{E}},\sigma_{\mathrm{B}}^2,\sigma_{\mathrm{E}}^2,R_{\mathrm{o}})\right)P_{\mathrm{non},2}^{\mathrm{TOF}}(\mathcal{N}_{\mathrm{U}},\mathcal{N}_{\mathrm{E}},\sigma_{\mathrm{B}}^2,\sigma_{\mathrm{E}}^2,\alpha,\zeta,R_{\mathrm{o}})\Big]$$
$$=\left[1-P_{\mathrm{non},1}^{\mathrm{TOF}}(\mathcal{N}_{\mathrm{U}},\mathcal{N}_{\mathrm{E}},\sigma_{\mathrm{B}}^2,\sigma_{\mathrm{E}}^2,R_{\mathrm{o}})\right]\left[1-P_{\mathrm{non},2}^{\mathrm{TOF}}(\mathcal{N}_{\mathrm{U}},\mathcal{N}_{\mathrm{E}},\sigma_{\mathrm{B}}^2,\sigma_{\mathrm{E}}^2,\alpha,\zeta,R_{\mathrm{o}})\right],$$

where $P_{\mathrm{non},t}^{\mathrm{TOF}}(\cdot)$ represents SNOP at the $t\in\{1,2\}$th step of the TOF strategy; and they are respectively derived as follows:

$$P_{\mathrm{non},1}^{\mathrm{TOF}}=1-\left(1-P_{\mathrm{U},1}^{\mathrm{TOF}}(\mathcal{N}_{\mathrm{E}},\sigma_{\mathrm{B}}^2,\sigma_{\mathrm{E}}^2,R_{\mathrm{o}})\right)^{N_{\mathrm{U}}}, \tag{16}$$

and

$$P_{\mathrm{non},2}^{\mathrm{TOF}}=\sum_{\substack{\mathcal{M}_{\mathrm{U}}\in\mathcal{P}(\mathcal{N}_{\mathrm{U}})\\ \mathcal{M}_{\mathrm{U}}\neq\varnothing}}P_{\mathrm{U},2}^{\mathrm{TOF}}(\sigma_{\mathrm{B}}^2,\zeta)^{|\mathcal{M}_{\mathrm{U}}|}\left(1-P_{\mathrm{U},2}^{\mathrm{TOF}}(\sigma_{\mathrm{B}}^2,\zeta)\right)^{N_{\mathrm{U}}-|\mathcal{M}_{\mathrm{U}}|}$$
$$\times\Bigg[\sum_{\substack{\mathcal{M}_{\mathrm{E}}\in\mathcal{P}(\mathcal{N}_{\mathrm{E}})\\ \mathcal{M}_{\mathrm{E}}\neq\varnothing,\mathcal{M}_{\mathrm{E}}\neq\mathcal{N}_{\mathrm{E}}}}\alpha^{|\mathcal{M}_{\mathrm{E}}|}(1-\alpha)^{N_{\mathrm{E}}-|\mathcal{M}_{\mathrm{E}}|} \tag{17}$$
$$\times P_{\mathrm{non}}^{\mathrm{TOF}}(\mathcal{M}_{\mathrm{U}},\mathcal{M}_{\mathrm{E}},\sigma_{\mathrm{B}}^2,\sigma_{\mathrm{E}}^2,\zeta,R_{\mathrm{o}})$$
$$+(1-\alpha)^{N_{\mathrm{E}}}P_{\mathrm{non}}^{\mathrm{TOF}}(\mathcal{M}_{\mathrm{U}},\sigma_{\mathrm{B}}^2,\zeta,R_{\mathrm{o}})],$$

where $P_{\mathrm{U},t}^{\mathrm{TOF}}(\cdot)$ and $P_{\mathrm{non}}^{\mathrm{TOF}}(\cdot)$ denote the feedback probability of each legitimate UE at the tth step and the SNOP according to the potential EVEs attempting to eavesdrop, respectively. It is worth noting in (17) that the case in which all EVEs are active is excluded, i.e., $\mathcal{M}_{\mathrm{E}}\neq\mathcal{N}_{\mathrm{E}}$, as we assume in the first step that all potential EVEs are already attempting to eavesdrop.

The feedback probability of each legitimate UE at the first step, denoted by $P_{\mathrm{U},1}^{\mathrm{TOF}}(\mathcal{N}_{\mathrm{E}},\sigma_{\mathrm{B}}^2,\sigma_{\mathrm{E}}^2,R_{\mathrm{o}})$, is given by

$$P_{\mathrm{U},1}^{\mathrm{TOF}}(\mathcal{N}_{\mathrm{E}},\sigma_{\mathrm{B}}^2,\sigma_{\mathrm{E}}^2,R_{\mathrm{o}})=\Pr\left(\log_2\left(\frac{1+|h_{\mathrm{B},i}|^2\rho}{1+\max_{j\in\mathcal{N}_{\mathrm{E}}}|h_{j,i}|^2\rho}\right)\geq R_{\mathrm{o}}\right) \tag{18}$$
$$=\int_{\frac{2^{R_{\mathrm{o}}}-1}{\rho}}^{\infty}f_X(x)F_{\overline{Y}}\left(\frac{1}{\rho}\left(\frac{1+x\rho}{2^{R_{\mathrm{o}}}}-1\right)\right)dx$$
$$=\sum_{m_{\mathrm{E}}=0}^{N_{\mathrm{E}}}\binom{N_{\mathrm{E}}}{m_{\mathrm{E}}}\frac{(-1)^{m_{\mathrm{E}}}\sigma_{\mathrm{E}}^22^{R_{\mathrm{o}}}}{\sigma_{\mathrm{E}}^22^{R_{\mathrm{o}}}+\sigma_{\mathrm{B}}^2m_{\mathrm{E}}}\exp\left(-\frac{2^{R_{\mathrm{o}}}-1}{\sigma_{\mathrm{B}}^2\rho}\right).$$

In the first step, each legitimate UE evaluates its worst-case secrecy rate under the conservative assumption that all potential EVEs are eavesdropping. Since this condition is stricter than the actual secrecy outage criterion, the presence of at least one legitimate UE that feeds back its channel gain ensures that a secrecy outage has not occurred. Accordingly, the SNOP at the first step of the TOF strategy is derived in (16) as one minus the probability that no UE sends feedback.

In addition, using Bayes' theorem, the feedback probability of each legitimate UE in the second step, denoted by $P_{\mathrm{U},2}^{\mathrm{TOF}}\left(\sigma_{\mathrm{B}}^2,\zeta\right)$, is given by

$$P_{\mathrm{U},2}^{\mathrm{TOF}}\left(\sigma_{\mathrm{B}}^2,\zeta\right)=\Pr\left(|h_{\mathrm{B},i}|^2\geq\zeta\middle|\log_2\left(\frac{1+|h_{\mathrm{B},i}|^2\rho}{1+\max_{j\in\mathcal{N}_{\mathrm{E}}}|h_{j,i}|^2\rho}\right)<R_{\mathrm{o}}\right) \tag{19}$$
$$=\frac{\Pr\left(\log_2\left(\frac{1+|h_{\mathrm{B},i}|^2\rho}{1+\max_{j\in\mathcal{N}_{\mathrm{E}}}|h_{j,i}|^2\rho}\right)<R_{\mathrm{o}}\middle||h_{\mathrm{B},i}|^2\geq\zeta\right)\Pr\left(|h_{\mathrm{B},i}|^2\geq\zeta\right)}{\Pr\left(\log_2\left(\frac{1+|h_{\mathrm{B},i}|^2\rho}{1+\max_{j\in\mathcal{N}_{\mathrm{E}}}|h_{j,i}|^2\rho}\right)<R_{\mathrm{o}}\right)},$$

where the probabilities are derived as

$$\Pr\left(\log_2\left(\frac{1+|h_{\mathrm{B},i}|^2\rho}{1+\max_{j\in\mathcal{N}_{\mathrm{E}}}|h_{j,i}|^2\rho}\right)<R_{\mathrm{o}}\middle||h_{\mathrm{B},i}|^2\geq\zeta\right) \tag{20}$$
$$=1-\Pr\left(\log_2\left(\frac{1+|h_{\mathrm{B},i}|^2\rho}{1+\max_{j\in\mathcal{N}_{\mathrm{E}}}|h_{j,i}|^2\rho}\right)\geq R_{\mathrm{o}}\middle||h_{\mathrm{B},i}|^2\geq\zeta\right)$$
$$=1-\int_{\theta}^{\infty}f_{\overline{X}}(x)F_{\overline{Y}}\left(\frac{1}{\rho}\left(\frac{1+x\rho}{2^{R_{\mathrm{o}}}}-1\right)\right)dx$$

$$= 1 - \sum_{m_\mathsf{E}=0}^{N_\mathsf{E}} \binom{N_\mathsf{E}}{m_\mathsf{E}} \frac{(-1)^{m_\mathsf{E}} \sigma_\mathsf{E} 2^{R_\mathrm{o}}}{\sigma_\mathsf{E}^2 2^{R_\mathrm{o}} + \sigma_\mathsf{B}^2 m_\mathsf{E}} \exp\left(-\left(\frac{\theta - \zeta}{\sigma_\mathsf{B}^2} + \frac{m_\mathsf{E}}{\sigma_\mathsf{E}^2 \rho}\left(\frac{1+\theta\rho}{2^{R_\mathrm{o}}} - 1\right)\right)\right),$$

$$\Pr\left(|h_{\mathsf{B},i}|^2 \geq \zeta\right) = 1 - F_X(\zeta) = \exp\left(-\frac{\zeta}{\sigma_\mathsf{B}^2}\right), \tag{21}$$

and (18), respectively. Moreover, θ is given by (10).

On the other hand, when one or more potential EVEs attempt to eavesdrop and $\mathcal{M}_\mathsf{U}$ out of $\mathcal{N}_\mathsf{U}$ legitimate UEs feed their channel gain back to the BS, the SNOP denoted by $P_{\mathrm{non}}^{\mathrm{TOF}}\left(\mathcal{M}_\mathsf{U}, \mathcal{M}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, \zeta, R_\mathrm{o}\right)$ is given by

$$\begin{aligned}
&P_{\mathrm{non}}^{\mathrm{TOF}}\left(\mathcal{M}_\mathsf{U}, \mathcal{M}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, \zeta, R_\mathrm{o}\right) \\
&= \Pr\left(\log_2\left(\frac{1+\max\limits_{i\in\mathcal{M}_\mathsf{U}} |h_{\mathsf{B},i}|^2\rho}{1+\max\limits_{j\in\mathcal{M}_\mathsf{E}} |h_{j,i}|^2\rho}\right) \geq R_\mathrm{o} \middle| |h_{\mathsf{B},i}|^2 \geq \zeta, \log_2\left(\frac{1+\max\limits_{i\in\mathcal{M}_\mathsf{U}} |h_{\mathsf{B},i}|^2\rho}{1+\max\limits_{j\in\mathcal{N}_\mathsf{E}} |h_{j,i}|^2\rho}\right) < R_\mathrm{o}\right) \\
&\overset{(a)}{\geq} \Pr\left(\log_2\left(\frac{1+\max\limits_{i\in\mathcal{M}_\mathsf{U}} |h_{\mathsf{B},i}|^2\rho}{1+\max\limits_{j\in\mathcal{M}_\mathsf{E}} |h_{j,i}|^2\rho}\right) \geq R_\mathrm{o} \middle| |h_{\mathsf{B},i}|^2 \geq \zeta\right) \\
&= \int_\theta^\infty f_{\tilde{X}}(x) F_{\tilde{Y}}\left(\frac{1}{\rho}\left(\frac{1+x\rho}{2^{R_\mathrm{o}}} - 1\right)\right) dx \\
&= \sum_{m_\mathsf{U}=0}^{M_\mathsf{U}-1} \sum_{m_\mathsf{E}=0}^{M_\mathsf{E}} \binom{M_\mathsf{U}-1}{m_\mathsf{U}} \binom{M_\mathsf{E}}{m_\mathsf{E}} \frac{(-1)^{m_\mathsf{U}+m_\mathsf{E}} \sigma_\mathsf{E}^2 M_\mathsf{U} 2^{R_\mathrm{o}}}{\sigma_\mathsf{E}^2 (m_\mathsf{U}+1) 2^{R_\mathrm{o}} + \sigma_\mathsf{B}^2 m_\mathsf{E}} e^{-\left(\frac{(m_\mathsf{U}+1)(\theta-\zeta)}{\sigma_\mathsf{B}^2} + \frac{m_\mathsf{E}}{\sigma_\mathsf{E}^2\rho}\left(\frac{1+\theta\rho}{2^{R_\mathrm{o}}} - 1\right)\right)},
\end{aligned} \tag{22}$$

where inequality (a) is derived from the definition of conditional probability and is applied to facilitate the derivation of a closed-form expression by eliminating a conditioning event. According to the definition of conditional probability, removing the conditioning term results in a probability that is less than or equal to the original. With the same approach, when no EVE is attempting to intercept the uplink transmission from the legitimate UE, the SNOP, which is denoted by $P_{\mathrm{non}}^{\mathrm{TOF}}\left(\mathcal{M}_\mathsf{U}, \sigma_\mathsf{B}^2, \zeta, R_\mathrm{o}\right)$, can be lower bounded as follows:

$$\begin{aligned}
&P_{\mathrm{non}}^{\mathrm{TOF}}\left(\mathcal{M}_\mathsf{U}, \sigma_\mathsf{B}^2, \zeta, R_\mathrm{o}\right) \\
&= \Pr\left(\log_2\left(1+\max_{i\in\mathcal{M}_\mathsf{U}} |h_{\mathsf{B},i}|^2\rho\right) \geq R_\mathrm{o} \middle| |h_{\mathsf{B},i}|^2 \geq \zeta, \log_2\left(\frac{1+\max\limits_{i\in\mathcal{M}_\mathsf{U}} |h_{\mathsf{B},i}|^2\rho}{1+\max\limits_{j\in\mathcal{N}_\mathsf{E}} |h_{j,i}|^2\rho}\right) < R_\mathrm{o}\right) \\
&\geq \Pr\left(\log_2\left(1+\max_{i\in\mathcal{M}_\mathsf{U}} |h_{\mathsf{B},i}|^2\rho\right) \geq R_\mathrm{o} \middle| |h_{\mathsf{B},i}|^2 \geq \zeta\right) \\
&= \int_\theta^\infty f_{\tilde{X}}(x) dx = 1 - F_{\tilde{X}}(\theta) = 1 - \left(1 - \exp\left(-\frac{\theta - \zeta}{\sigma_\mathsf{B}^2}\right)\right)^{M_\mathsf{U}}.
\end{aligned} \tag{23}$$

Therefore, an upper bound of the SOP for the proposed TOF strategy is obtained by substituting (16)–(23) into (15).

4.3. Proposed two-step OF with quantization (TOFQ)

With the same approach as (15), the SOP of the proposed TOFQ strategy, $P_{\mathrm{out}}^{\mathrm{TOFQ}}(\mathcal{N}_\mathsf{U}, \mathcal{N}_\mathsf{E}, \alpha, \zeta, R_\mathrm{o}, L)$, can be defined as follows:

$$\begin{aligned}
&P_{\mathrm{out}}^{\mathrm{TOFQ}}\left(\mathcal{N}_\mathsf{U}, \mathcal{N}_\mathsf{E}, \alpha, \zeta, R_\mathrm{o}, L\right) \\
&\quad = \left[1 - P_{\mathrm{non},1}^{\mathrm{TOFQ}}\left(\mathcal{N}_\mathsf{U}, \mathcal{N}_\mathsf{E}, R_\mathrm{o}\right)\right]\left[1 - P_{\mathrm{non},2}^{\mathrm{TOFQ}}\left(\mathcal{N}_\mathsf{U}, \mathcal{N}_\mathsf{E}, \alpha, \zeta, R_\mathrm{o}, L\right)\right],
\end{aligned} \tag{24}$$

where $P_{\mathrm{non},t}^{\mathrm{TOFQ}}(\cdot)$ represents SNOP at the tth step of the TOFQ strategy, and we can intuitively state that $P_{\mathrm{non},1}^{\mathrm{TOFQ}} = P_{\mathrm{non},1}^{\mathrm{TOF}}$ in (16) because it is not related to quantization. Furthermore, $P_{\mathrm{non},2}^{\mathrm{TOFQ}}$ is derived as follows:

$$\begin{aligned}
P_{\mathrm{non},2}^{\mathrm{TOFQ}} = &\sum_{\substack{\mathcal{M}_\mathsf{U}\in\mathcal{P}(\mathcal{N}_\mathsf{U})\\ \mathcal{M}_\mathsf{U}\neq\emptyset}} P_{\mathsf{U},2}^{\mathrm{TOFQ}}(\sigma_\mathsf{B}^2, \zeta)^{|\mathcal{M}_\mathsf{U}|}\left(1 - P_{\mathsf{U},2}^{\mathrm{TOFQ}}(\sigma_\mathsf{B}^2, \zeta)\right)^{N_\mathsf{U}-|\mathcal{M}_\mathsf{U}|} \\
&\times \sum_{k\in\mathcal{K}} P(\mathcal{M}_\mathsf{U}, k)\Bigg[\sum_{\substack{\mathcal{M}_\mathsf{E}\in\mathcal{P}(\mathcal{N}_\mathsf{E})\\ \mathcal{M}_\mathsf{E}\neq\emptyset, \mathcal{M}_\mathsf{E}\neq\mathcal{N}_\mathsf{E}}} \alpha^{|\mathcal{M}_\mathsf{E}|}(1-\alpha)^{N_\mathsf{E}-|\mathcal{M}_\mathsf{E}|} \\
&\qquad \times P_{\mathrm{non}}^{\mathrm{TOFQ}}(\mathcal{M}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, \zeta, R_\mathrm{o}, k) \\
&\qquad + (1-\alpha)^{N_\mathsf{E}} P_{\mathrm{non}}^{\mathrm{TOFQ}}(\sigma_\mathsf{B}^2, \zeta, R_\mathrm{o}, k)\Bigg],
\end{aligned} \tag{25}$$

where the feedback probability for each legitimate UE, denoted by $P_{\mathsf{U},t}^{\mathrm{TOFQ}}(\cdot)$, is equal to $P_{\mathsf{U},t}^{\mathrm{TOF}}(\cdot)$ in (18) and (19) because it is also independent of quantization; and $P(\mathcal{M}_\mathsf{U}, k)$ represents the probability that the highest channel gain among $\mathcal{M}_\mathsf{U}$ legitimate UEs is between η_k and η_{k+1} and that at least one UE exists in the region $k \in \mathcal{K} \triangleq \{0, 1, \ldots, 2^L - 2\}$, which is given by

$$P(\mathcal{M}_\mathsf{U}, k) = \left(1 - \sum_{l=k}^{2^L-2} P(\mathcal{M}_\mathsf{U}, l+1)\right)\left(1 - \left(1 - \frac{1}{k+1}\right)^{M_\mathsf{U}}\right), \tag{26}$$

where $\eta_{2^L-1} = \infty$ and $P(\mathcal{M}_\mathsf{U}, 2^L - 1) = 0$ because this region is for the first step. As described in 3.2, considering the L-bit quantization for channel gain feedback, $2^L - 1$ regions from 0 to $2^L - 2$ are given in the second step. Finally, with the same approach as (22) and (23), the SNOPs, denoted by $P_{\mathrm{non}}^{\mathrm{TOFQ}}(\cdot)$, can be derived as

$$\begin{aligned}
&P_{\mathrm{non}}^{\mathrm{TOFQ}}\left(\mathcal{M}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, \zeta, R_\mathrm{o}, k\right) \\
&\geq \Pr\left(\log_2\left(\frac{1+|h_{\mathsf{B},i}|^2\rho}{1+\max\limits_{j\in\mathcal{M}_\mathsf{E}} |h_{j,i}|^2\rho}\right) \geq R_\mathrm{o} \middle| \eta_k \leq |h_{\mathsf{B},i}|^2 < \eta_{k+1}\right) \\
&= \int_{\theta_k}^{\theta_{k+1}} f_{X_k}(x) F_{\tilde{Y}}\left(\frac{1}{\rho}\left(\frac{1+x\rho}{2^{R_\mathrm{o}}} - 1\right)\right) dx \\
&= \sum_{m_\mathsf{E}=0}^{M_\mathsf{E}} \binom{M_\mathsf{E}}{m_\mathsf{E}} \frac{(-1)^{m_\mathsf{E}} \sigma_\mathsf{E}^2 2^{R_\mathrm{o}} e^{\frac{\zeta}{\sigma_\mathsf{B}^2} - \frac{m_\mathsf{E}}{\sigma_\mathsf{E}^2\rho}\left(\frac{1}{2^{R_\mathrm{o}}} - 1\right)}}{\sigma_\mathsf{E}^2 2^{R_\mathrm{o}} + \sigma_\mathsf{B}^2 m_\mathsf{E}} \\
&\quad \times \frac{e^{-\theta_k\left(\frac{1}{\sigma_\mathsf{B}^2} + \frac{m_\mathsf{E}}{\sigma_\mathsf{E}^2 2^{R_\mathrm{o}}}\right)} - e^{-\theta_{k+1}\left(\frac{1}{\sigma_\mathsf{B}^2} + \frac{m_\mathsf{E}}{\sigma_\mathsf{E}^2 2^{R_\mathrm{o}}}\right)}}{e^{-(\eta_k - \zeta)/\sigma_\mathsf{B}^2} - e^{-(\eta_{k+1} - \zeta)/\sigma_\mathsf{B}^2}},
\end{aligned} \tag{27}$$

and

$$\begin{aligned}
&P_{\mathrm{non}}^{\mathrm{TOFQ}}\left(\sigma_\mathsf{B}^2, \zeta, R_\mathrm{o}, k\right) \\
&\geq \Pr\left(\log_2\left(1+|h_{\mathsf{B},i}|^2\rho\right) \geq R_\mathrm{o} \middle| \eta_k \leq |h_{\mathsf{B},i}|^2 < \eta_{k+1}\right) \\
&= \int_{\theta_k}^{\theta_{k+1}} f_{X_k}(x) dx = \frac{e^{-(\theta_k - \zeta)/\sigma_\mathsf{B}^2} - e^{-(\theta_{k+1} - \zeta)/\sigma_\mathsf{B}^2}}{e^{-(\eta_k - \zeta)/\sigma_\mathsf{B}^2} - e^{-(\eta_{k+1} - \zeta)/\sigma_\mathsf{B}^2}},
\end{aligned} \tag{28}$$

respectively, where $X_k \triangleq |h_{j,i}|^2$ is a random variable for $\eta_k \leq |h_{j,i}|^2 < \eta_{k+1}$; and the PDF of X_k is given by

$$f_{X_k}(x) = \frac{f_{\overline{X}}(x)}{\int_{\eta_k}^{\eta_{k+1}} f_{\overline{X}}(x) dx} = \frac{1}{\sigma_\mathsf{B}^2} \frac{e^{-(x-\zeta)/\sigma_\mathsf{B}^2}}{e^{-(\eta_k - \zeta)/\sigma_\mathsf{B}^2} - e^{-(\eta_{k+1} - \zeta)/\sigma_\mathsf{B}^2}}.$$

In addition, θ_k is given by

$$\theta_k = \begin{cases} \frac{2^{R_\mathrm{o}}-1}{\rho}, & \text{if } \eta_k < \frac{2^{R_\mathrm{o}}-1}{\rho}, \\ \eta_k, & \text{otherwise.} \end{cases}$$

An upper bound of the SOP for the proposed TOFQ strategy is then achieved by substituting (16), (18), (19), and (25)–(28) into (24).

5. Simulation results

We evaluate the SOP and effective secrecy throughput (EST) of the proposed TOF strategies, including its quantized variant, TOFQ, and verify the mathematical expressions in 4 through extensive computer simulations. Along with the conventional opportunistic feedback (OF) strategy, we further consider the following two extreme cases as benchmarks.

- *Ideal Case (IC):* It is assumed that each legitimate UE can exploit not only the channel gains to all potential EVEs but also their instantaneous activities (eavesdropping or not). Although this is infeasible in practice, it is meaningful in that it provides a *lower-bound* of the achievable SOP for a given system model. Specifically, when the ith legitimate UE satisfies the feedback condition of

$$\log_2\left(\frac{1+|h_{\mathsf{B},i}|^2\rho}{1+\max\limits_{j\in\mathcal{M}_\mathsf{E}} |h_{j,i}|^2\rho}\right) \geq R_\mathrm{o},$$

it feeds back its channel gain to the legitimate BS to request scheduling.

- *Worst Case (WC):* Each legitimate UE conservatively feeds back its channel gain to the BS. To be specific, each legitimate UE assumes that all potential EVEs always attempt to eavesdrop on the secure message, i.e., $\alpha = 1$; hence, the ith legitimate UE feeds back its channel gain when the feedback condition of (1) is satisfied.

The mathematical expressions of the SOPs for both cases are given as follows:

- *Ideal Case:* For a given topology and target secrecy rate R_o [bps/Hz], the SOP of this case, denoted by $P_\mathrm{out}^\mathrm{IC}(\mathcal{N}_\mathsf{U}, \mathcal{N}_\mathsf{E}, \alpha, R_\mathrm{o})$, can be defined as follows:

$$\begin{aligned} P_\mathrm{out}^\mathrm{IC}\left(\mathcal{N}_\mathsf{U}, \mathcal{N}_\mathsf{E}, \alpha, R_\mathrm{o}\right) &= 1 - P_\mathrm{non}^\mathrm{IC}\left(\mathcal{N}_\mathsf{U}, \mathcal{N}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, \alpha, R_\mathrm{o}\right) \\ &= 1 - \Bigg[\sum_{\substack{\mathcal{M}_\mathsf{E} \in \mathcal{P}(\mathcal{N}_\mathsf{E}) \\ \mathcal{M}_\mathsf{E} \neq \varnothing}} \alpha^{|\mathcal{M}_\mathsf{E}|}(1-\alpha)^{N_\mathsf{E} - |\mathcal{M}_\mathsf{E}|} \\ &\qquad \times P_\mathrm{non}^\mathrm{IC}\left(\mathcal{N}_\mathsf{U}, \mathcal{M}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, R_\mathrm{o}\right) \\ &\qquad + (1-\alpha)^{N_\mathsf{E}} P_\mathrm{non}^\mathrm{IC}\left(\mathcal{N}_\mathsf{U}, \sigma_\mathsf{B}^2, R_\mathrm{o}\right)\Bigg], \end{aligned}$$

  where the SNOP when one or more potential EVEs attempt to eavesdrop, $P_\mathrm{non}^\mathrm{IC}(\mathcal{N}_\mathsf{U}, \mathcal{M}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, R_\mathrm{o})$, is derived as

$$\begin{aligned} P_\mathrm{non}^\mathrm{IC}\left(\mathcal{N}_\mathsf{U}, \mathcal{M}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, R_\mathrm{o}\right) &= 1 - \prod_{i \in \mathcal{N}_\mathsf{U}} P_{\mathrm{out},i}^\mathrm{IC}\left(\mathcal{M}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, R_\mathrm{o}\right) \\ &= 1 - \left(1 - P_\mathsf{U}^\mathrm{IC}\left(\mathcal{M}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, R_\mathrm{o}\right)\right)^{N_\mathsf{U}}, \end{aligned}$$

  where $P_\mathsf{U}^\mathrm{IC}(\mathcal{M}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, \rho, R_\mathrm{o})$ is the feedback probability of each legitimate UE when $\mathcal{M}_\mathsf{E}$ potential EVEs attempt to eavesdrop, which is given by

$$\begin{aligned} P_\mathsf{U}^\mathrm{IC}\left(\mathcal{M}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, R_\mathrm{o}\right) &= \Pr\left(\log_2\left(\frac{1 + |h_{\mathsf{B},i}|^2\rho}{1 + \max\limits_{j \in \mathcal{M}_\mathsf{E}} |h_{j,i}|^2\rho}\right) \geq R_\mathrm{o}\right) \\ &= \int_{\frac{2^{R_\mathrm{o}}-1}{\rho}}^{\infty} f_X(x) F_{\widetilde{Y}}\left(\frac{1}{\rho}\left(\frac{1 + x\rho}{2^{R_\mathrm{o}}} - 1\right)\right) dx \\ &= \sum_{m_\mathsf{E}=0}^{M_\mathsf{E}} \binom{M_\mathsf{E}}{m_\mathsf{E}} \frac{(-1)^{m_\mathsf{E}} \sigma_\mathsf{E}^2 2^{R_\mathrm{o}}}{\sigma_\mathsf{E}^2 2^{R_\mathrm{o}} + \sigma_\mathsf{B}^2 m_\mathsf{E}} \exp\left(-\frac{2^{R_\mathrm{o}} - 1}{\sigma_\mathsf{B}^2 \rho}\right), \end{aligned}$$

  where $M_\mathsf{E} = |\mathcal{M}_\mathsf{E}|$. Moreover, the SNOP when there is no potential EVE attempting to eavesdrop, denoted by $P_\mathrm{non}^\mathrm{IC}(\mathcal{N}_\mathsf{U}, \sigma_\mathsf{B}^2, \rho, R_\mathrm{o})$, is given as

$$P_\mathrm{non}^\mathrm{IC}\left(\mathcal{N}_\mathsf{U}, \sigma_\mathsf{B}^2, R_\mathrm{o}\right) = 1 - \prod_{i \in \mathcal{N}_\mathsf{U}} P_{\mathrm{out},i}^\mathrm{IC}\left(\sigma_\mathsf{B}^2, R_\mathrm{o}\right) = 1 - \left(1 - P_\mathsf{U}^\mathrm{IC}\left(\sigma_\mathsf{B}^2, R_\mathrm{o}\right)\right)^{N_\mathsf{U}},$$

  where

$$\begin{aligned} P_\mathsf{U}^\mathrm{IC}\left(\sigma_\mathsf{B}^2, R_\mathrm{o}\right) &= \Pr\left(\log_2\left(1 + |h_{\mathsf{B},i}|^2\rho\right) \geq R_\mathrm{o}\right) \\ &= \int_{\frac{2^{R_\mathrm{o}}-1}{\rho}}^{\infty} f_X(x) dx = \exp\left(-\frac{2^{R_\mathrm{o}} - 1}{\sigma_\mathsf{B}^2 \rho}\right). \end{aligned}$$

- *Worst Case:* Intuitively, this case is equivalent to performing only the first step of the proposed TOF strategy. Hence, a closed-form expression of the SOP for the WC can be written as

$$P_\mathrm{out}^\mathrm{WC}\left(\mathcal{N}_\mathsf{U}, \mathcal{N}_\mathsf{E}, R_\mathrm{o}\right) = 1 - P_{\mathrm{non},1}^\mathrm{TOF}\left(\mathcal{N}_\mathsf{U}, \mathcal{N}_\mathsf{E}, \sigma_\mathsf{B}^2, \sigma_\mathsf{E}^2, R_\mathrm{o}\right),$$

  with (16) and (18).

5.1. Secrecy outage probability (SOP)

Figs. 3–7 show the SOP performance of the proposed TOF and TOFQ strategies in uplink wireless networks with potential EVEs, where $\sigma_\mathsf{B}^2 = \sigma_\mathsf{E}^2 = 1$. We consider two channel gain thresholds $\zeta \in \{0, 2\}$ and the number of quantization bits of $L \in \{2, 4\}$ for the TOFQ. The figures show that the SOP performances of the proposed TOF and TOFQ lie between ideal and worst cases.

Fig. 3 presents the SOP performance with respect to the number of legitimate UEs N_U when the average transmit SNR $\rho = 10$[dB], the number of potential EVEs $N_\mathsf{E} = 4$, the target secrecy rate $R_\mathrm{o} = 0.5$[bps/Hz], and the eavesdropping probability $\alpha = 0.5$. First of all, we can observe that the SOP performance improves thanks to multi-user diversity as the number of legitimate UEs increases for all feedback strategies. In particular, this tendency is more noticeable in the proposed TOF and TOFQ strategies than in the conventional OF strategy based solely on the channel gain threshold; hence, when there are many legitimate UEs, the proposed TOF strategies significantly outperform the conventional OF. It is also worth noting that the TOFQ achieves comparable performance to the TOF, even though $L = 2$ or 4.

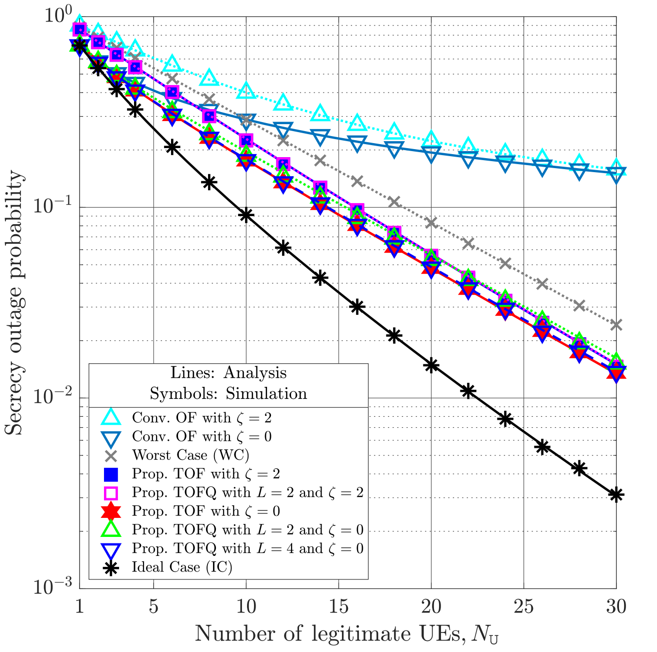


Fig. 3. SOP with respect to N_U, when $\rho = 10$[dB], $N_\mathsf{E} = 4$, $R_\mathrm{o} = 0.5$[bps/Hz], and $\alpha = 0.5$.

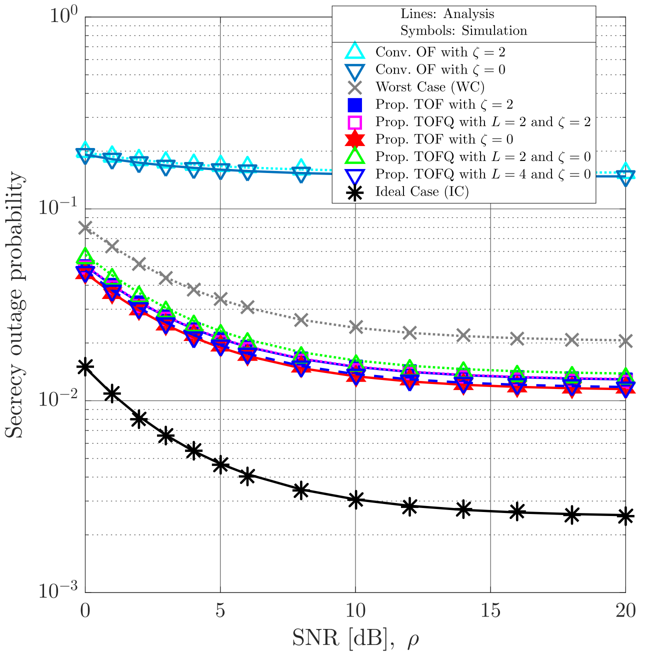


Fig. 4. SOP with respect to ρ [dB], when $N_\mathsf{U} = 30$, $N_\mathsf{E} = 4$, $R_\mathrm{o} = 0.5$[bps/Hz], and $\alpha = 0.5$.

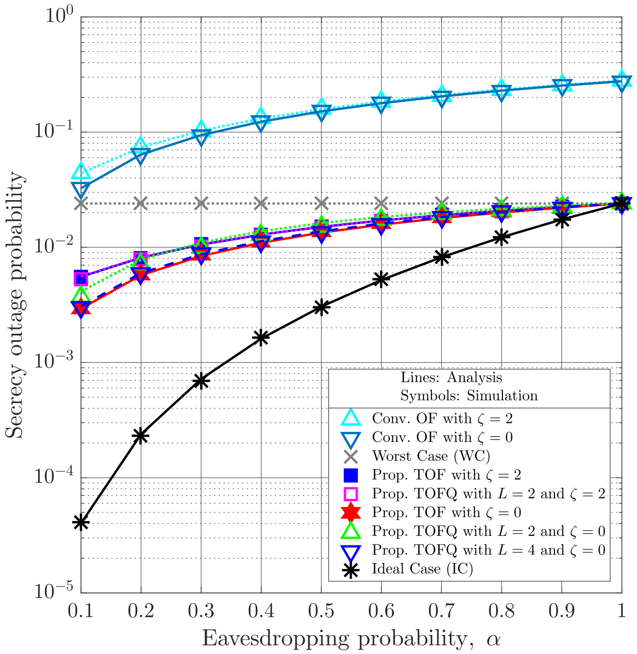


Fig. 5. SOP with respect to α, when $\rho = 10$ [dB], $N_{\mathsf{U}} = 30$, $N_{\mathsf{E}} = 4$, and $R_{\mathsf{o}} = 0.5$ [bps/Hz].

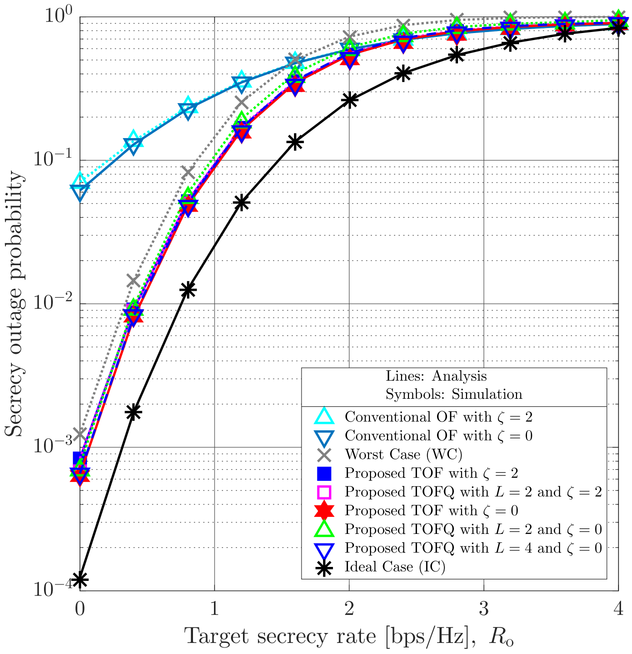


Fig. 6. SOP with respect to R_{o} [bps/Hz], when $\rho = 10$ [dB], $N_{\mathsf{U}} = 30$, $N_{\mathsf{E}} = 4$, and $\alpha = 0.5$.

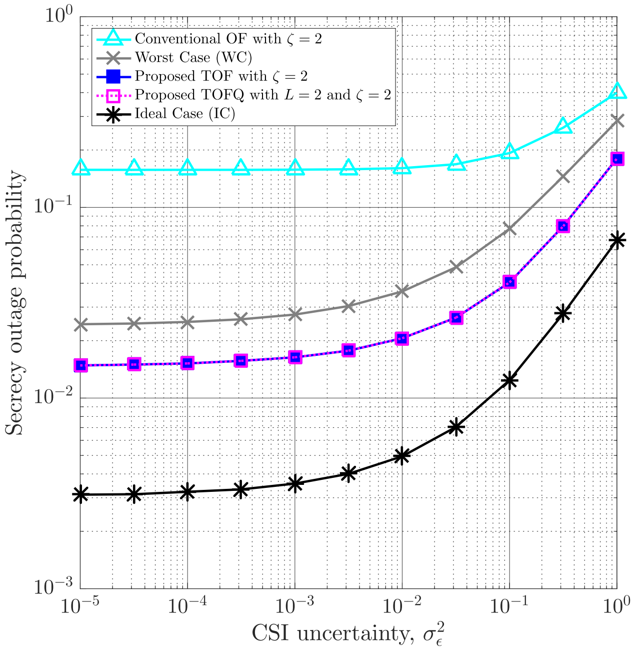


Fig. 7. SOP with respect to σ_ϵ^2, when $\rho = 10$ [dB], $N_{\mathsf{U}} = 30$, $N_{\mathsf{E}} = 4$, $R_{\mathsf{o}} = 0.5$ [bps/Hz], $\alpha = 0.5$.

Fig. 4 illustrates the SOP performance with respect to the average transmit SNR ρ when the number of legitimate UEs $N_{\mathsf{U}} = 30$, the number of potential EVEs $N_{\mathsf{E}} = 4$, the target secrecy rate $R_{\mathsf{o}} = 0.5$ [bps/Hz], and the eavesdropping probability $\alpha = 0.5$. Increasing the transmit SNR of legitimate UEs does not significantly decrease the SOP for all feedback strategies, as it also increases the received SNR not only at the legitimate BS but also at EVEs. Nevertheless, the proposed TOF and TOFQ strategies remarkably outperform the conventional OF strategy as the transmit SNR increases.

Fig. 5 depicts the SOP performance with respect to the eavesdropping probability α when the average transmit SNR $\rho = 10$[dB], the number of legitimate UEs $N_{\mathsf{U}} = 30$, the number of potential EVEs $N_{\mathsf{E}} = 4$, and the target secrecy rate $R_{\mathsf{o}} = 0.5$[bps/Hz]. Naturally, the SOP performance gradually deteriorates as the eavesdropping probability increases. In the WC, however, the SOP performance is independent of the eavesdropping probability because legitimate UEs perform conservative and careful feedback under the assumption that all potential EVEs always attempt to eavesdrop on uplink transmissions. Impressively, the proposed TOF and TOFQ strategies significantly outperform the conventional OF strategy even in the WC.

Fig. 6 shows the SOP performance with respect to the target secrecy rate R_{o} [bps/Hz] when the average transmit SNR $\rho = 10$ [dB], the number of legitimate UEs $N_{\mathsf{U}} = 30$, the number of potential EVEs $N_{\mathsf{E}} = 4$, and the eavesdropping probability $\alpha = 0.5$. The SOP increases for all feedback schemes as the target secrecy rate increases, eventually converging to 1. On the other hand, it is noteworthy that the proposed TOF and TOFQ strategies still dramatically outperform the conventional OF in the low target secrecy rate region.

On the other hand, in practical wireless communication systems, CSI may become outdated or inaccurate due to feedback delay or channel estimation errors. In the proposed TOF and TOFQ strategies, as described in Section 2, legitimate UEs acquire the CSI of potential EVEs; however, this information may be imperfect due to such impairments. A similar issue may arise when legitimate UEs estimate the CSI to the BS. To evaluate the robustness of the proposed schemes under these practical conditions, we present additional simulation results incorporating imperfect CSI, as shown in Fig. 7. In this simulation, we consider the average transmit SNR $\rho = 10$ [dB], the number of legitimate UEs $N_{\mathsf{U}} = 30$, the number of potential EVEs $N_{\mathsf{E}} = 4$, the target secrecy rate $R_{\mathsf{o}} = 0.5$ [bps/Hz], and the eavesdropping probability $\alpha = 0.5$. Specifically, the CSI uncertainties can be modeled as $\widetilde{h}_{j,i} \triangleq h_{j,i} + \epsilon_{j,i}$ and $\widetilde{h}_{\mathsf{B},i} \triangleq h_{\mathsf{B},i} + \epsilon_{\mathsf{B},i}$, where $\widetilde{h}_{j,i}$ and $\widetilde{h}_{\mathsf{B},i}$ denote the actual (or current) CSI from legitimate UE i to potential EVE j and the BS, respectively, while $h_{j,i}$ and $h_{\mathsf{B},i}$ represent the estimated (or outdated) CSI [49, 50]. The terms $\epsilon_{j,i}$ and $\epsilon_{\mathsf{B},i}$ represent the corresponding channel errors, modeled as independent and identically distributed complex Gaussian random variables with zero mean and variance σ_ϵ^2,

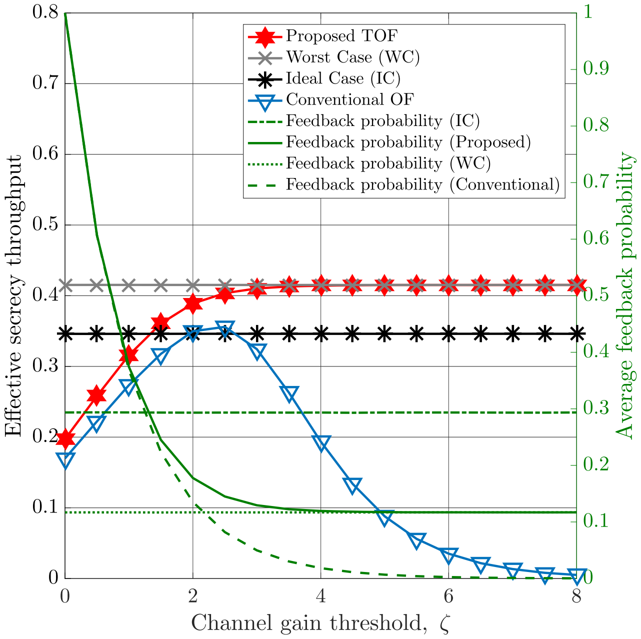


Fig. 8. EST and feedback probability for varying the channel gain threshold ζ, when $\rho = 10$ [dB], $N_{\mathrm{U}} = 30$, $N_{\mathrm{E}} = 4$, $R_{\mathrm{o}} = 0.5$ [bps/Hz], $\alpha = 0.5$, and $\beta = 0.05$.

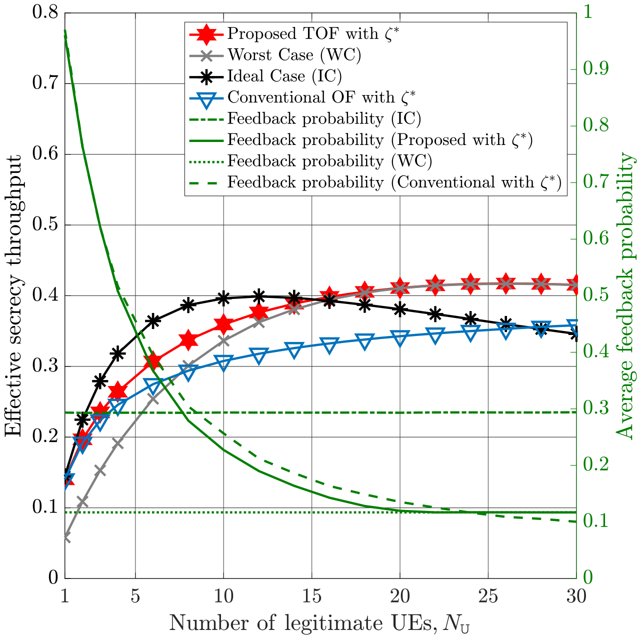


Fig. 9. EST and feedback probability for varying N_{U} with the optimal channel gain threshold ζ^*, when $\rho = 10$ [dB], $N_{\mathrm{E}} = 4$, $R_{\mathrm{o}} = 0.5$ [bps/Hz], $\alpha = 0.5$, and $\beta = 0.05$.

where the variance reflects the mean squared error (MSE) of the estimation. We can observe from Fig. 7 that the SOP increases with σ_ϵ^2. This degradation arises because a legitimate UE may refrain from sending feedback despite satisfying the target secrecy rate, or a secrecy outage may occur in the actual channel due to the feedback being based on inaccurate CSI. Nevertheless, it is noteworthy that the proposed strategies remain robust against channel uncertainties with estimation errors up to 10^{-3}.

5.2. Effective secrecy throughput (EST)

From the SOP and the feedback probability, we can derive an EST, which represents the achievable secure average throughput of feedback strategies [51,52]. Specifically, the EST is defined as

$$\Phi\left(P_{\mathrm{out}}^{\Psi}\right) = \frac{R_{\mathrm{o}}T\left(1 - P_{\mathrm{out}}^{\Psi}\right)}{\mathbb{E}\left[M_{\mathrm{U}}\right]\beta T + T} = \frac{R_{\mathrm{o}}\left(1 - P_{\mathrm{out}}^{\Psi}\right)}{N_{\mathrm{U}}P_{\mathrm{U}}^{\Psi}\beta + 1}, \tag{29}$$

where β and T denote the time slot length for uplink feedback and the frame size, respectively. Intuitively, as β increases, a larger portion of the time slot is allocated to the feedback phase, thereby reducing the duration available for data transmission. Hence, the EST decreases with increasing β. Also, $\Psi \in \{\mathrm{OF}, \mathrm{TOF}, \mathrm{TOFQ}, \mathrm{IC}, \mathrm{WC}\}$ represents the feedback strategy discussed in this paper.

Figs. 8 and 9 show the EST performance and the average feedback probability of each legitimate UE according to the channel gain threshold and the number of legitimate UEs, respectively. We have observed in 5.1 that the performance of TOF and TOFQ is almost identical even when $L = 4$, so from now on, we refer to them as a common term: *Proposed* strategy.

Fig. 8 presents the EST performance and feedback probability with respect to the channel gain threshold ζ when the average transmit SNR $\rho = 10$ [dB], the number of legitimate UEs $N_{\mathrm{U}} = 30$, the number of potential EVEs $N_{\mathrm{E}} = 4$, the target secrecy rate $R_{\mathrm{o}} = 0.5$ [bps/Hz], the eavesdropping probability $\alpha = 0.5$, and the length of time slot for uplink feedback $\beta = 0.05$. The ideal and worst cases, IC and WC, have constant ESTs and average feedback probabilities because they do not take into account channel gain thresholds. We can observe that the EST performance and feedback probability of the conventional OF strategy converge to zero as the channel gain threshold increases. This is because if the threshold is too large, legitimate UEs do not meet the feedback condition, $|h_{\mathrm{B},i}|^2 > \zeta$, with a high probability, and no UE is scheduled. Moreover, we can also observe that an optimal channel gain threshold exists that maximizes the EST performance of the conventional OF strategy. On the other hand, as the threshold increases, the proposed TOF strategy progressively takes only the first step in Section 3.1.1, so its EST performance and feedback probability converge to the WC, as discussed above. In other words, in the proposed TOF strategy, there is a difference that UEs can still perform feedback according to the first step; hence, the EST and feedback probability do not converge to zero. Finally, the proposed TOF strategy improves both the EST and the feedback probability compared to the conventional one.

Fig. 9 illustrates the EST performance and feedback probability with respect to the number of legitimate UEs N_{U} with optimal channel gain thresholds ζ^* for maximizing EST performance, when the average transmit SNR $\rho = 10$ [dB], the number of potential EVEs $N_{\mathrm{E}} = 4$, the target secrecy rate $R_{\mathrm{o}} = 0.5$ [bps/Hz], the eavesdropping probability $\alpha = 0.5$, and the length of time slot for uplink feedback $\beta = 0.05$. Here, we numerically obtained the optimal channel gain threshold ζ^*. In terms of EST performance, the IC outperforms the WC when the number of legitimate UEs is small, but it reverses as the number of UEs increases. As a result of applying optimal channel gain thresholds according to the number of legitimate UEs, we can observe that the EST performance of the proposed TOF strategy outperforms the conventional one.

We should not overlook that the minimum SOP performance is obtained when $\zeta = 0$. Specifically, the proposed TOF strategy improves the EST performance by reducing the number of feedbacks of legitimate UEs. Hence, there is a fundamental trade-off between the SOP and the EST performance according to the channel gain threshold.

5.3. System complexity

We analyze the worst-case system complexity of the considered feedback strategies—conventional OF, TOF, TOFQ, IC, and WC—in terms of the number of operations required for feedback processing and user scheduling based on selecting the user with the maximum channel gain. The system complexity of each strategy is derived as follows:

- *Conventional OF:* Each legitimate UE determines whether its own channel gain exceeds a predefined threshold via a constant-time operation, i.e., $\mathcal{O}(1)$. In the worst case, all N_{U} UEs transmit their channel gains to the BS, which then selects the UE with the highest channel gain. Therefore, the worst-case system complexity is $\mathcal{O}(N_{\mathsf{U}})$.
- *Proposed TOF(Q):* In Step I, each legitimate UE evaluates whether its worst-case secrecy rate exceeds the target R_{o}, requiring a comparison with the maximum of N_{E} EVE channel gains. Each UE satisfying the condition feeds back its channel gain. In the worst case, as in the OF scheme, up to N_{U} UEs may transmit feedback. Step II, if invoked, follows the same procedure as OF. Consequently, the worst-case system complexity is $\mathcal{O}(N_{\mathsf{E}}) + \mathcal{O}(N_{\mathsf{U}})$. Since the TOFQ differs from the TOF only in that it quantizes the feedback signals, it incurs the same system complexity.
- *Ideal Case:* Each legitimate UE is assumed to know not only the channel gains to all EVEs but also their instantaneous eavesdropping activity. The secrecy rate is computed only over the subset $\mathcal{M}_{\mathsf{E}}$ of active EVEs, where $M_{\mathsf{E}} = |\mathcal{M}_{\mathsf{E}}| \leq N_{\mathsf{E}}$. Therefore, the worst-case complexity becomes $\mathcal{O}(M_{\mathsf{E}}) + \mathcal{O}(N_{\mathsf{U}})$.
- *Worst Case:* This case corresponds to the first step of the TOF strategy; hence, the system complexity is identical to that of TOF, i.e., $\mathcal{O}(N_{\mathsf{E}}) + \mathcal{O}(N_{\mathsf{U}})$.

It is noteworthy that the proposed TOF strategies can be implemented in a distributed manner across legitimate UEs, each relying only on its local CSI. Each legitimate UE performs local computation with complexity $\mathcal{O}(N_{\mathsf{E}})$, and only those satisfying the feedback condition transmit feedback, resulting in significantly reduced system overhead in practice.

6. Conclusions

We proposed a novel two-step opportunistic feedback (TOF) strategy to enhance the physical-layer security (PLS) of uplink wireless networks against potential eavesdroppers (EVEs). To facilitate practical implementation, we also introduced a quantized variant, the TOF strategy with quantization (TOFQ), which quantizes channel gains for feedback. Unlike the conventional opportunistic feedback (OF) strategy, where legitimate user equipment (UE) feeds back channel gain information to the base station (BS) solely based on link quality, the proposed TOF strategies incorporate secrecy considerations. Specifically, each UE evaluates secrecy outage conditions before proceeding with conventional feedback. We conducted a theoretical analysis of the secrecy outage probability (SOP) and effective secrecy throughput (EST) performance of the proposed TOF strategies. Simulation results demonstrated that the TOF strategies significantly outperform the conventional OF strategy in both SOP and EST metrics. Furthermore, the TOFQ strategy achieved comparable SOP performance to the TOF strategy, even with a small number of quantization bits, underscoring its practical feasibility. Finally, although the proposed strategies are not explicitly designed to address the tradeoff between the system performance and complexity in user scheduling schemes, they can contribute to reducing computational complexity by pre-filtering UEs based on security-aware feedback before scheduling. As future work, we plan to extend the proposed user scheduling strategies to multi-antenna wireless networks with non-identical channel variances to further evaluate their applicability and performance in more complex scenarios.

CRediT authorship contribution statement

Woong Son: Writing – original draft, Software, Methodology, Investigation, Formal analysis; **Ki-Hun Lee:** Writing – review & editing, Software, Methodology, Investigation, Formal analysis; **Heejung Yu:** Writing – review & editing, Validation, Supervision, Resources, Project administration, Funding acquisition, Conceptualization; **Bang Chul Jung:** Writing – review & editing, Validation, Supervision, Resources, Project administration, Funding acquisition, Conceptualization.

Data availability

Data will be made available on request. No data was used for the research described in the article.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This work was supported in part by the National Research Foundation of Korea (NRF) through the Korean Government (MSIT) under Grant No. RS-2025-02303435, in part by the IITP Grant funded by the Korea Government (MSIP, Development of Cube Satellites Based on Core Technologies in Low Earth Orbit Satellite Communications) under Grant RS-2024-00396992, and in part by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2023-RS-2022-00164800) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation).

References

[1] D. Rupprecht, A. Dabrowski, T. Holz, E. Weippl, C. Pöpper, On security research towards future mobile network generations, IEEE Commun. Surv. Tutor 20 (3) (2018) 2518–2542. https://doi.org/10.1109/COMST.2018.2820728
[2] Y.-S. Shiu, S.Y. Chang, H.-C. Wu, C. S, H. Huang, H.-H. Chen, Physical layer security in wireless networks: a tutorial, IEEE Wireless Commun. 18 (2) (2011) 66–74. https://doi.org/10.1109/MWC.2011.5751298
[3] M.A. Siddiqi, H. Yu, J. Joung, G ultra-reliable low-latency communication implementation challenges and operational issues with IoT devices, Electronics (Basel) 5 (9) (2019). 981. https://doi.org/10.3390/electronics8090981
[4] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, K. Zeng, Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities, IEEE Internet Things J. 6 (5) (2019) 8169–8181. https://doi.org/10.1109/JIOT.2019.2927379
[5] J. Bae, W. Khalid, A. Lee, H. Lee, S. Noh, H. Yu, Overview of RIS-enabled secure transmission in 6G wireless networks, Digit. Commun. Netw. 10 (6) (2024). 1553–1565. https://doi.org/10.1016/j.dcan.2024.02.005
[6] S. Zhang, D. Zhu, Y. Liu, Artificial intelligence empowered physical layer security for 6G: State-of-the-art, challenges, and opportunities, Comput. Netw. 242 (2024) 1–27. https://doi.org/10.1016/j.comnet.2024.110255
[7] I.-R.W. 5d, Framework and overall objectives of the future development of IMT for 2030 and beyond, Technical Report, Tech. rep, 2023.
[8] F. Irram, M. Ali, M. Naeem, S. Mumtaz, Physical layer security for beyond 5G/6G networks: Emerging technologies and future directions, J. Netw. Comput. Appl. 206 (2022) 1–27. https://doi.org/10.1016/j.jnca.2022.103431
[9] Z. Wei, C. Masouros, F. Liu, S. Chatzinotas, B. Ottersten, Energy- and cost-efficient physical layer security in the era of IoT: The role of interference, IEEE Commun. Mag. 58 (4) (2020) 81–87. https://doi.org/10.1109/MCOM.001.1900716
[10] M. Bloch, et al., An overview of information-theoretic security and privacy: Metrics, limits and applications, IEEE J. Sel. Areas Inf. Theory 2 (1) (2021) 5–22. https://doi.org/10.1109/JSAIT.2021.3062755
[11] W. Khalid, H. Yu, R. Ali, R. Ullah, Advanced physical-layer technologies for beyond 5G wireless communication networks, Sensors 21 (9) (2021). 3197. https://doi.org/10.3390/s21093197
[12] P. Porambage, G. Gür, D.P.M. Osorio, M. Liyanage, A. Gurtov, M. Ylianttila, The roadmap to 6G security and privacy, IEEE Open J. Commun. Soc. 2 (2021) 1094–1122. https://doi.org/10.1109/OJCOMS.2021.3078081
[13] A.D. Wyner, The wire-tap channel, Bell Syst. Tech. J. 54 (8) (1975). 1355–1387. https://doi.org/10.1002/j.1538-7305.1975.tb02040.x
[14] S. Leung-Yan-Cheong, M. Hellman, The Gaussian wire-tap channel, IEEE Trans. Inf. Theory 24 (4) (1978) 451–456. https://doi.org/10.1109/TIT.1978.1055917
[15] M. Bloch, J. Barros, M.R.D. Rodrigues, S.W. Mclaughlin, Wireless information-theoretic security, IEEE Trans. Inf. Theory 54 (6) (2008) 2515–2534. https://doi.org/10.1109/TIT.2008.921908
[16] Y. Liang, H.V. Poor, Multiple-access channels with confidential messages, IEEE Trans. Inf. Theory 54 (3) (2008) 976–1002. https://doi.org/10.1109/TIT.2007.915978
[17] A. Khisti, G.W. Wornell, Secure transmission with multiple antennas-part II: The MIMOME wiretap channel, IEEE Trans. Inf. Theory 56 (11) (2010) 5515–5532. https://doi.org/10.1109/TIT.2010.2068852

[18] A. Khisti, G.W. Wornell, Secure transmission with multiple antennas I: the MISOME wiretap channel, IEEE Trans. Inf. Theory 56 (7) (2010) 3088–3104. https://doi.org/10.1109/TIT.2010.2048445

[19] H. Jin, W.-Y. Shin, B.C. Jung, On the multi-user diversity with secrecy in uplink wiretap networks, IEEE Commun. Lett. 17 (9) (2013). 1778–1781. https://doi.org/10.1109/LCOMM.2013.071813.131158

[20] H. Yu, T. Kim, H. Jafarkhani, Wireless secure communication with beamforming and jamming in time-varying wiretap channels, IEEE Trans. Inf. Forensics Secur. 13 (8) (2018) 2087–2100. https://doi.org/10.1109/TIFS.2018.2809695

[21] H. Yu, T. Kim, Training and data structures for AN-aided secure communication, IEEE Syst. J. 13 (3) (2019) 2869–2872. https://doi.org/10.1109/10.1109/JSYST.2018.2859446

[22] H. Yu, J. Joung, Design of the power and dimension of artificial noise for secure communication systems, IEEE Trans. Commun. 69 (6) (2021) 4001–4010. https://doi.org/10.1109/TCOMM.2021.3063446

[23] H. Yu, J. Joung, Secure IoT communications using HARQ-based beamforming for MISOSE channels, IEEE Internet Things J. 8 (23) (2021) 17211–17226. https://doi.org/10.1109/JIOT.2021.3078062

[24] M. Yang, D. Guo, Y. Huang, T.Q. Duong, B. Zhang, Physical layer security with threshold-based multiuser scheduling in multi-antenna wireless networks, IEEE Trans. Commun. 64 (12) (2016) 5189–5202. https://doi.org/10.1109/TCOMM.2016.2606396

[25] K. Guo, et al., Physical layer security for multiuser satellite communication systems with threshold-based scheduling scheme, IEEE Trans. Veh. Technol. 69 (5) (2020) 5129–5141. https://doi.org/10.1109/TVT.2020.2979496

[26] A.S.M. Badrudduza, et al., Security at the physical layer over GG fading and mEGG turbulence induced RF-UOWC mixed system, IEEE Access 9 (2021) 18123–18136. https://doi.org/10.1109/ACCESS.2021.3053323

[27] S.H. Islam, et al., Impact of correlation and pointing error on secure outage performance over arbitrary correlated Nakagami-m and $\mathcal{M}$-turbulent fading mixed RF-FSO channel, IEEE Photon. J. 13 (2) (2021) 1–17. https://doi.org/10.1109/JPHOT.2021.3059805

[28] W. Khalid, H. Yu, Security improvement with QoS provisioning using service priority and power allocation for NOMA-IoT networks, IEEE Access 9 (2021) 9937–9948. https://doi.org/10.1109/ACCESS.2021.3049258

[29] W. Khalid, H. Yu, D.-T. Do, Z. Kaleem, S. Noh, RIS-aided physical layer security with full-duplex jamming in underlay D2D networks, IEEE Access 9 (2021) 99667–99679. https://doi.org/10.1109/10.1109/ACCESS.2021.3095852

[30] L. Mucchi, et al., Physical-layer security in 6G networks, IEEE Open J. Commun. Soc. 2 (2021) 1901–1914. https://doi.org/10.1109/OJCOMS.2021.3103735

[31] S.M.S. Shahriyer, A.S.M. Badrudduza, S. Shabab, M.K. Kundu, H. Yu, Opportunistic relay in multicast channels with generalized shadowed fading effects: A physical layer security perspective, IEEE Access 9 (2021) 155726–155739. https://doi.org/10.1109/10.1109/ACCESS.2021.3128572

[32] H. Yu, I.-G. Lee, Physical layer security based on NOMA and AJ for MISOSE channels with an untrusted relay, Future Gen. Comput. Syst. 102 (2020) 611–618. https://doi.org/10.1016/j.future.2019.09.019

[33] A. Chorti, S.M. Perlaza, Z. Han, H.V. Poor, On the resilience of wireless multiuser networks to passive and active eavesdroppers, IEEE J. Sel. Areas Commun. 31 (9) (2013) 1850–1863. https://doi.org/10.1109/JSAC.2013.130917

[34] J.M. Hamamreh, H.M. Furqan, H. Arslan, Classifications and applications of physical layer security techniques for confidentiality: a comprehensive survey, IEEE Commun. Surv. Tuts 21 (2) (2019). 1773–1828. https://doi.org/10.1109/COMST.2018.2878035

[35] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, X. Gao, A survey of physical layer security techniques for 5G wireless networks and challenges ahead, IEEE J. Sel. Areas Commun. 36 (4) (2018) 679–695. https://doi.org/10.1109/JSAC.2018.2825560

[36] M.A. Abbas, H. Song, J.-P. Hong, Opportunistic scheduling for average secrecy rate enhancement in fading downlink channel with potential eavesdroppers, IEEE Trans. Inf. Forensics Secur. 14 (4) (2019) 969–980. https://doi.org/10.1109/TIFS.2018.2868494

[37] I. Bang, B.C. Jung, Secrecy rate analysis of opportunistic user scheduling in uplink networks with potential eavesdroppers, IEEE Access 7 (2019) 127078–127089. https://doi.org/10.1109/ACCESS.2019.2939048

[38] W. Son, H. Nam, W.-Y. Shin, B.C. Jung, Secrecy outage analysis of multiuser downlink wiretap networks with potential eavesdroppers, IEEE Syst. J. 15 (2) (2021) 3093–3096. https://doi.org/10.1109/JSYST.2020.3007434

[39] W. Son, H.S. Jang, B.C. Jung, A pseudo-random beamforming technique for improving physical-layer security of MIMO cellular networks, Entropy 21 (11) (2019). 1038. https://doi.org/10.3390/e21111038

[40] J. Youn, W. Son, B.C. Jung, Physical-layer security improvement with reconfigurable intelligent surfaces for 6G wireless communication systems, Sensors 21 (4) (2021). 1439. https://doi.org/10.3390/s21041439

[41] W. Son, M. Oh, H. Yu, B.C. Jung, Physical-layer security in MU-MISO downlink networks against potential eavesdroppers, Digit. Commun. Netw. 11 (2) (2025) 424–431. https://doi.org/10.1016/j.dcan.2024.02.004

[42] N. Su, F. Liu, C. Masouros, Secure radar-communication systems with malicious targets: integrating radar, communications and jamming functionalities, IEEE Trans. Wireless Commun. 20 (1) (2021) 83–95. https://doi.org/10.1109/TWC.2020.3023164

[43] M.T. Mamaghani, Y. Hong, Terahertz meets untrusted UAV relaying: Minimum secrecy energy efficiency maximization via trajectory and communication co-design, IEEE Trans. Veh. Technol. 71 (5) (2022) 4991–5006. https://doi.org/10.1109/TVT.2022.3150011

[44] K.-H. Lee, K. Lim, B.C. Jung, STEALTH: space-time encryption via constellation hiding for MIMO two-way untrusted relay systems, IEEE Internet Things J. 12 (15) (2025) 30319–30334. https://doi.org/10.1109/JIOT.2025.3571736

[45] Y. Ju, et al., Energy-efficient cooperative secure communications in mmWave vehicular networks using deep recurrent reinforcement learning, IEEE Trans. Intell. Transp. Syst. 25 (10) (2024). 14460–14475. https://doi.org/10.1109/TITS.2024.3394130

[46] N. Su, F. Liu, C. Masouros, Sensing-assisted eavesdropper estimation: an ISAC breakthrough in physical layer security, IEEE Trans. Wireless Commun. 23 (4) (2024) 3162–3174. https://doi.org/10.1109/TWC.2023.3306029

[47] M. Shen, X. Lei, X. Zhou, G.K. Karagiannidis, STAR-RIS assisted secure MIMO communication networks: transmit power minimization for perfect and imperfect CSI, IEEE Trans. Commun. 73 (3) (2025). 1487–1500. https://doi.org/10.1109/TCOMM.2024.3430971

[48] H. Xiao, X. Hu, A. Li, W. Wang, K. Yang, Robust full-space physical layer security for STAR-RIS-aided wireless networks: Eavesdropper with uncertain location and channel, IEEE Trans. Wireless Commun., 24 (9) (2025) 7206–7220. https://doi.org/10.1109/TWC.2025.3559075

[49] Y. Deng, Q. Li, Q. Zhang, L. Yang, J. Qin, Secure beamforming design in MIMO NOMA networks for Internet of Things with perfect and imperfect CSI, Comput. Netw. 187 (2021) 1–11. https://doi.org/10.1016/j.comnet.2021.107839

[50] K.-H. Lee, J.S. Yeom, J. Joung, B.C. Jung, Performance analysis of uplink NOMA with constellation-rotated STLC for IoT networks, IEEE Open J. Commun. Soc. 3 (2022) 705–717. https://doi.org/10.1109/OJCOMS.2022.3164876

[51] H. Lei, et al., On secure mixed RF-FSO systems with TAS and imperfect CSI, IEEE Trans. Commun. 68 (7) (2020) 4461–4475. https://doi.org/10.1109/TCOMM.2020.2985028

[52] M. Ibrahim, A.S.M. Badrudduza, M.S. Hossen, M.K. Kundu, I.S. Ansari, I. Ahmed, On effective secrecy throughput of underlay spectrum sharing $\alpha - \mu/$ málaga hybrid model under interference-and-transmit power constraints, IEEE Photon. J. 15 (2) (2023) 1–13. https://doi.org/10.1109/JPHOT.2023.3253020