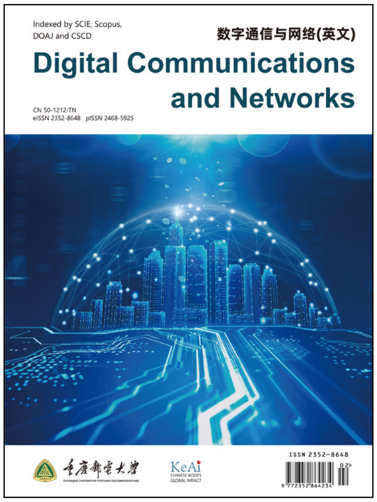


Physical-layer security in MU-MISO downlink networks against potential eavesdroppers

Woong Son, Minkyu Oh, Heejung Yu and Bang Chul Jung

PII: S2352-8648(24)00022-1
DOI: https://doi.org/10.1016/j.dcan.2024.02.004
Reference: DCAN 727

To appear in: *Digital Communications and Networks*

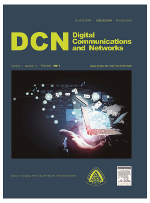
Received date: 26 September 2022
Revised date: 20 February 2024
Accepted date: 26 February 2024

Digital Communications and Networks(DCN)

Available online at www.sciencedirect.com

ScienceDirect

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



Physical-layer security in MU-MISO downlink networks against potential eavesdroppers

Woong Son[a], Minkyu Oh[b], Heejung Yu[c,*], Bang Chul Jung[b,*]

[a]C4I R & D Lab., LIG Nex1 Co. Ltd., Yongin, 16911, South Korea
[b]Department of Electronics Engineering, Chungnam National University, Daejeon, 34134, South Korea
[c]Department of Electronics and Information Engineering, Korea University, Sejong, 30019, South Korea

Abstract

Recently, wireless security has been highlighted as one of the most important techniques for 6G mobile communication systems. Many researchers have tried to improve the Physical-Layer Security (PLS) performance such as Secrecy Outage Probability (SOP) and Secrecy Energy-Efficiency (SEE). The SOP indicates the outage probability that the data transmission between legitimate devices does not guarantee a certain reliability level, and the SEE is defined as the ratio between the achievable secrecy-rate and the consumed transmit power. In this paper, we consider a Multi-User Multi-Input Single-Output (MU-MISO) downlink cellular network where a legitimate Base Station (BS) equipped with multiple transmit antennas sends secure information to multiple legitimate Mobile Stations (MSs), and multiple *potential* eavesdroppers (EVEs) equipped with a single receive antenna try to eavesdrop on this information. Each potential EVE tries to intercept the secure information, i.e., the private message, from the legitimate BS to legitimate MSs with a certain eavesdropping probability. To securely receive the private information, each legitimate MS feeds back its effective channel gain to the legitimate BS only when the effective channel gain is higher than a certain threshold, i.e., the legitimate MSs adopt an *Opportunistic* Feedback (OF) strategy. In such eavesdropping channels, both SOP and SEE are analyzed as performance measures of PLS and their closed-form expressions are derived mathematically. Based on the analytical results, it is shown that the SOP of the OF strategy approaches that of a Full Feedback (FF) strategy as the number of legitimate MSs or the number of antennas at the BS increases. Furthermore, the trade-off between SOP and SEE as a function of the channel feedback threshold in the OF strategy is investigated. The analytical results and related observations are verified by numerical simulations.

KEYWORDS:
Physical-layer security, opportunistic feedback, potential eavesdroppers, secrecy outage probability, secrecy energy-efficiency.

1. Introduction

Security in wireless networks has become one of the most important issues since various private and confidential information has been exchanged over wireless networks, especially cellular networks. Although various encryption schemes, such as shared key and private key schemes, have been developed, robust security at the network layer is based on the assumption that eavesdroppers have limited computational capabilities. Therefore, security cannot be guaranteed against adversaries with ultimate computational power. Physical-Layer Security (PLS) has been introduced as an alternative to providing substantial secrecy, PLS exploits the broadcast nature of a wireless channel [1, 2]. In PLS, the physical signal transmitted over wireless channels is controlled so that the signal is decoded only by legitimate users. Therefore, PLS has been considered as one of the promising

*Corresponding authors

[1]Email addresses: woong.son@lignex1.com (W. Son), minkyuoh@o.cnu.ac.kr (M. Oh), heejungyu@korea.ac.kr (H. Yu), bcjung@cnu.ac.kr (B. C. Jung)

Table 1
Comparison between the proposed technique with existing studies for multiple potential eavesdroppers in a single-cell downlink network (S: Simulation, A: Mathematical closed-form analysis).

Reference	[20]	[21]	Proposed
Antenna	SISO	SISO	MISO
Strategy	FF, FE	OF, RE	OF, RE
CSI Req.	MS, EVE	MS	MS
Metric	SR	SOP, SEE	SOP, SEE
Evaluation	S, A	S, A	S, A

techniques to ensure secure communication in wireless networks. The secrecy performance was analyzed under various channel models, e.g., discrete memoryless wire-tap channel [1], Gaussian wire-tap channel [3], quasi-static fading channel [4], Gaussian multiple access wire-tap channel [5], and wire-tap channels with multiple antennas [6, 7]. Moreover, practical PLS schemes have been proposed to enhance legitimate links and/or to deteriorate eavesdropping links for various communication systems [8, 9, 10, 11]. Recently, PLS in millimeter-wave (mmWave) and terahertz (THz)-band communication, massive Multi-Input Multi-Output (massive MIMO), Reconfigurable Intelligent Surface (RIS), Non-Orthogonal Multiple Access (NOMA), relay and backscatter communication have been studied [12, 13, 14, 15, 16, 17, 18, 19].

As well-known measures of the PLS against malicious and intrusive eavesdroppers (EVEs), Secrecy Rate (SR) and Secrecy Outage Probability (SOP) have been widely adopted. To consider the energy-efficient PLS, Secrecy Energy-Efficiency (SEE), defined by a ratio of secrecy rate to power consumption, has also been introduced as another performance metric. Different types of eavesdropping attack scenarios have been investigated depending on the capability and operational scenario of EVEs. In many previous studies, *passive* eavesdropping scenarios where EVEs attempt to eavesdrop on private messages of legitimate users without performing any other operations, such as jamming the signal transmission, have been considered [22, 23, 24, 25, 26, 8, 11]. In the *active* eavesdropping scenario, EVEs not only eavesdrop on the information of legitimate users, but also transmit a jamming signal to degrade legitimate links or feed back false information to legitimate users to induce malfunction [27, 28, 29]. Recently, a new eavesdropping scenario, i.e., *potential* eavesdropping, has been investigated. For example, unscheduled Mobile Stations (MSs) in the same cell can be a candidate for potential EVEs since they cannot eavesdrop on the other MSs' information when sending their own information to a Base Station (BS). In another scenario, a potential EVE does not eavesdrop the information of the other users when it is in sleep mode onserve battery power. In [30] and [20, 31, 21, 32], potential eavesdropping was studied in multi-user uplink and downlink networks, respectively. Table 1 compares the proposed technique with existing studies in the literature which considers multiple potential eavesdroppers in a single-cell downlink network. The CSI req. in Table 1 indicates Channel State Information (CSI) requirement at the legitimate transmitter or BS. In aerial networks with Unmanned Aerial Vehicles (UAVs), an untrusted UAV relay, which can operate as a potential EVE while act as a relay, has been considered [33]. The authors of [33] investigated a maximization problem of minimum SEE in terms of UAV's trajectory and velocity, scheduling, and transmission power allocation. In [34], PLS has been studied for a Multi-input Multi-Output (MIMO) joint radar communication system that transmits downlink signals to MSs and tracks radar targets simultaneously. Here, the radar targets act as potential EVEs.

For PLS in multi-antenna systems, a beamforming technology has been adopted to improve the quality of legitimate links or degrade that of eavesdropping links [8, 11, 31, 32]. To further improve the secrecy rate, the concept of Artificial Noise (AN) has been introduced [9, 10, 35]. However, to the best of our knowledge, the effects on multiple antennas and intermittent operation of potential EVEs in potential eavesdropping attack scenarios have not been investigated by mathematical analysis. Therefore, this paper investigates the effects of beamforming gain at the legitimate BS and intermittent eavesdropping of multiple potential EVEs on the SOP and SEE performance in multi-user multi-input single-output (MU-MISO) downlink cellular networks with multiple potential EVEs. Under such a system model, an *opportunistic* feedback (OF) strategy is proposed to improve secrecy performance with low feedback overhead. It is shown that the proposed OF scheme achieves a high level of security, i.e., high SEE and low SOP, when the number of legitimate MSs or the number of transmit antennas at a BS is large enough. Furthermore, the closed-form expressions for SOP and SEE are derived. They are compared with numerical results under different system parameters in our multi-user downlink cellular networks.

The rest of this paper is organized as follows: the system and signal models are introduced in Section 2, the general procedure of the proposed technique is explained in Section 3, closed-form expressions of PLS performance are derived in Section 4, mathematical analysis and computer simulations are included in Section 5, and the conclusions are summerized in Section 6.

1.1. Notations

Vectors and matrices are written in boldface with matrices in capitals. All vectors are column vectors. For a vector $\mathbf{x}$, $\mathbf{x}^H$ indicates the conjugate transpose of a vector $\mathbf{x}$. We use $\|\mathbf{x}\|$ for the 2-norm of a vector $\mathbf{x}$. $\mathbf{I}_K$ denote an identity matrix with size $K \times K$. For a random vector $\mathbf{x}$, $\mathbf{x} \sim \mathcal{CN}(\mu, \mathbf{\Sigma})$ means that $\mathbf{x}$ is complex

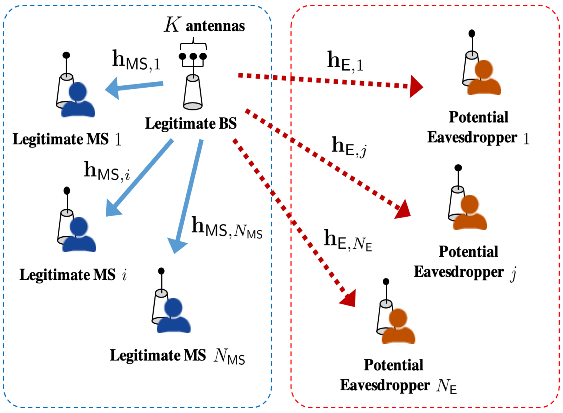

K antennas
$\mathsf{h}_{\mathsf{MS},1}$
Legitimate MS 1
Legitimate BS
$\mathsf{h}_{\mathsf{MS},i}$
Legitimate MS i
$\mathsf{h}_{\mathsf{MS},N_{\mathsf{MS}}}$
Legitimate MS N_{MS}
$\mathsf{h}_{\mathsf{E},1}$
Potential Eavesdropper 1
$\mathsf{h}_{\mathsf{E},j}$
Potential Eavesdropper j
$\mathsf{h}_{\mathsf{E},N_{\mathsf{E}}}$
Potential Eavesdropper N_{E}

Fig. 1. A multi-user MISO downlink cellular network with multiple potential EVEs.

Gaussian distributed with mean vector μ and covariance matrix $\mathbf{\Sigma}$. $X \sim \mathsf{Exp}(\lambda)$ and $X \sim \mathsf{Erlang}(k, \lambda)$ mean that a random variable X follows an exponential distribution with rate λ and an Erlang distribution with shape k and rate λ. $\mathbb{E}[X]$ denotes the expectation of a random variable X. For a set $\mathcal{A}$, $|\mathcal{A}|$ is a cardinality of $\mathcal{A}$, i.e., the number of elements in $\mathcal{A}$.

2. System and signal models

As shown in Figure 1, we consider a multi-user MISO downlink cellular network where a BS equipped with K multiple transmit antennas, N_{MS} legitimate Mobile Stations (MSs) with a single antenna, and multiple N_{E} non-colluding potential EVEs with a single antenna are deployed. This system model is a typical model considered in existing studies for an eavesdropping scenario in a downlink cellular network with multiple potential EVEs [20, 21]. In this network, a channel vector of the legitimate link from the BS to the i-th legitimate MS is denoted by $\mathbf{h}_{\mathsf{MS},i} = [h_{\mathsf{MS},i,1}, h_{\mathsf{MS},i,2}, \cdots, h_{\mathsf{MS},i,K}] \in \mathbb{C}^{1\times K}$ for $i \in \mathcal{N}_{\mathsf{MS}}$ where $\mathcal{N}_{\mathsf{MS}}$ is a set of indices of the legitimate MSs, i.e., $\mathcal{N}_{\mathsf{MS}} = \{1, 2, \cdots, N_{\mathsf{MS}}\}$. Similarly, a channel vector of the eavesdropping link from the BS to the j-th potential EVE is given by $\mathbf{h}_{\mathsf{E},j} = \left[h_{\mathsf{E},j,1}, h_{\mathsf{E},j,2}, \cdots, h_{\mathsf{E},j,K}\right] \in \mathbb{C}^{1\times K}$ for $j \in \mathcal{N}_{\mathsf{E}} \triangleq \{1, 2, \cdots, N_{\mathsf{E}}\}$. Note that individual average path loss from the BS to each legitimate MS (potential EVE) does not considered. This means that the distance from the BS to all legitimate MSs (potential EVEs) is identical. Then, the legitimate and eavesdropping channel vectors are assumed to be zero-mean complex Gaussian random vector with covariance matrices of $\sigma^2_{\mathsf{MS}}\mathbf{I}_K$ and $\sigma^2_{\mathsf{E}}\mathbf{I}_K$, i.e., $\mathbf{h}_{\mathsf{MS},i} \sim \mathcal{CN}(\mathbf{0}, \sigma^2_{\mathsf{MS}}\mathbf{I}_K)$ and $\mathbf{h}_{\mathsf{E},j} \sim \mathcal{CN}(\mathbf{0}, \sigma^2_{\mathsf{E}}\mathbf{I}_K)$, respectively. In addition, quasi-static block fading channel coefficients are assumed, i.e. they do not change during data transmission.

It is assumed that the CSI of the eavesdropping links as well as the CSI of the legitimate links are available at the BS, since unscheduled MSs in the same cell as the legitimate MSs may operate as potential EVEs and may try to eavesdrop on the secret information of the legitimate MSs. However, the current operation of the potential EVE (whether eavesdropping or not) is assumed to be unknown to the BS. To improve channel quality of the legitimate links based on the feedback CSI, the Maximum Ratio Transmission (MRT) beamforming technique is adopted to maximize Signal-to-Noise Ratio (SNR) at a target legitimate receiver. If the i-th legitimate MS is selected to be served by the BS, the MRT beam vector is given by

$$\mathbf{v}_{\mathsf{MS},i} = \frac{\mathbf{h}^H_{\mathsf{MS},i}}{||\mathbf{h}_{\mathsf{MS},i}||}$$

Therefore, the transmit signal vector form the BS to the scheduled i-th legitimate MS is expressed by

$$\begin{aligned}\mathbf{s}_{\mathsf{MS},i} &= \sqrt{P}\mathbf{v}_{\mathsf{MS},i}s_{\mathsf{MS},i} \\ &= \sqrt{P}\frac{\mathbf{h}^H_{\mathsf{MS},i}}{||\mathbf{h}_{\mathsf{MS},i}||}s_{\mathsf{MS},i} \in \mathbb{C}^{K\times 1}\end{aligned}$$

where $s_{\mathsf{MS},i}$ is a transmit symbol and P is transmit signal power, i.e., $\mathbb{E}[||\mathbf{s}_{\mathsf{MS},i}||^2] = P$.

Then, the received signals at the i-th legitimate MS and the j-th potential EVE can be represented as

$$\begin{aligned}r_{\mathsf{MS},i} &= \mathbf{h}_{\mathsf{MS},i}\mathbf{s}_{\mathsf{MS},i} + z_{\mathsf{MS},i} \\ &= \sqrt{P}||\mathbf{h}_{\mathsf{MS},i}||s_{\mathsf{MS},i} + z_{\mathsf{MS},i} \qquad (1)\end{aligned}$$

and

$$\begin{aligned}r_{\mathsf{E},j} &= \mathbf{h}_{\mathsf{E},j}\mathbf{s}_{\mathsf{MS},i} + z_{\mathsf{E},j} \\ &= \sqrt{P}(\mathbf{h}_{\mathsf{E},j}\mathbf{h}^H_{\mathsf{MS},i}/||\mathbf{h}_{\mathsf{MS},i}||)s_{\mathsf{MS},i} + z_{\mathsf{E},j} \qquad (2)\end{aligned}$$

respectively. $z_{\mathsf{MS},i} \sim \mathcal{CN}(0, \sigma^2_z)$ and $z_{\mathsf{E},j} \sim \mathcal{CN}(0, \sigma^2_z)$ are additive white Gaussian noise at the i-th legitimate MS and j-th potential EVE, respectively. Based on (1) and (2), the SNRs can be evaluated as

$$\Gamma_{\mathsf{MS},i} = \frac{P||\mathbf{h}_{\mathsf{MS},i}||^2}{\sigma^2_z} = \rho||\mathbf{h}_{\mathsf{MS},i}||^2 \qquad (3)$$

and

$$\Gamma_{\mathsf{E},j} = \frac{P|\mathbf{h}_{\mathsf{E},j}\mathbf{h}^H_{\mathsf{MS},i}|^2}{||\mathbf{h}_{\mathsf{MS},i}||^2\sigma^2_z} = \rho\frac{|\mathbf{h}_{\mathsf{E},j}\mathbf{h}^H_{\mathsf{MS},i}|^2}{||\mathbf{h}_{\mathsf{MS},i}||^2} \qquad (4)$$

respectively, where $\rho = P/\sigma^2_z$.

3. Secure transmission with opportunistic feedback against potential EVEs

In a multi-user MISO downlink channel, a secure transmission scenario against multiple potential EVEs attempting to eavesdrop on the secure information with a certain probability is proposed. By adopting OF and scheduling schemes, we can reduce the feedback overhead while achieving reasonable secrecy performance if the number of legitimate MSs or the number of antennas at a BS is large enough. The detailed operation scenario of the proposed secure transmission is explained the following subsections.

3.1. Broadcasting reference signal

First, a BS transmits a reference signal for downlink channel estimation to all devices including all of legitimate MSs and potential EVEs. With the received reference signal, all devices can estimate their CSI from the BS. Although the potential EVEs can estimate their channel, the CSI of the potential EVEs is not required in the overall scenario.

3.2. Opportunistic CSI feedback

If the all legitimate MSs feed back their CSI to the BS, the uplink overhead increases with the number of legitimate MSs and the number of antennas at the BS. Therefore, the overall system performance considering both uplink and downlink may be degraded. Therefore, to reduce the uplink overhead of CSI feedback, an opportunistic CSI feedback strategy is proposed in our operation scenario. In the proposed OF strategy, only when the i-th legitimate MS's channel gain $||\mathbf{h}_{\mathsf{MS},i}||^2$ is larger than a certain threshold ζ, the i-th legitimate MS feeds its channel information back to the BS. This means that the selected legitimate MSs, which have better channel quality than the other MSs, can be candidates for scheduling and transmission. For convenience, we define a set of the selected legitimate MSs as $\mathcal{M}_{\mathsf{MS}}$, which is a subset of $\mathcal{N}_{\mathsf{MS}}$, i.e., $\mathcal{M}_{\mathsf{MS}} \subseteq \mathcal{N}_{\mathsf{MS}}$. Depending on ζ, therefore, $|\mathcal{M}_{\mathsf{MS}}|$, i.e., the number of selected MSs, and uplink feedback overhead can be determined. As a special case of OF, when $\zeta = 0$, all the legitimate MSs feed their CSI, i.e., $\mathcal{M}_{\mathsf{MS}} = \mathcal{N}_{\mathsf{MS}}$, and this case is called a full feedback (FF) strategy.

3.3. Random eavesdropping of potential EVEs

In this paper, we consider a potential eavesdropping scenario where EVEs attempt to eavesdrop on private information sent by legitimate MSs depending on their state, e.g., their scheduling and power saving conditions. Such a potential eavesdropping scenario can then be modelled as Random Eavesdropping (RE) with a certain probability. In the RE strategy, the j-th potential EVE attempts to eavesdrop private message for the scheduled legitimate MS with a certain eavesdropping probability $P_{\mathsf{E},j}$. For simplicity, we assume that $P_{\mathsf{E},j} = P_{\mathsf{E}}$ for all $j \in \mathcal{N}_{\mathsf{E}}$. Therefore, a subset of the potential EVEs, which is denoted by $\mathcal{M}_{\mathsf{E}}(\subseteq \mathcal{N}_{\mathsf{E}})$, try to eavesdrop secure message. As a special case of an RE strategy with $P_{\mathsf{E}} = 1$, all potential EVEs attempt to eavesdrop legitimate information. This case is called a conventional Full Eavesdropping (FE) strategy.

3.4. Legitimate MS scheduling for secure transmission

Based on the CSI feedback from a part of the legitimate MSs, the BS selects the best legitimate MS, which has the maximum channel gain, and transmits a signal vector $\mathbf{s}_{\mathsf{MS},\widehat{i}}$, where $\widehat{i}$ denotes the index of the scheduled (i.e., selected) legitimate MS, that is, $\widehat{i} = \arg\max_{i\in\mathcal{M}_{\mathsf{MS}}} ||\mathbf{h}_{\mathsf{MS},i}||^2$. After scheduling one legitimate MS, the BS sends secret information with an MRT beam vectors,

$$\mathbf{s}_{\mathsf{MS},\widehat{i}} = \sqrt{P}\frac{\mathbf{h}^H_{\mathsf{MS},\widehat{i}}}{||\mathbf{h}_{\mathsf{MS},\widehat{i}}||}x_{\mathsf{MS},\widehat{i}} \tag{5}$$

4. Secrecy performance analysis

To define secrecy performance measures, such as SOP and SEE, we first evaluate instantaneous secrecy rate for a given legitimate MS and active potential EVEs. The instantaneous achievable secrecy rate can be calculated by replacing achievable rate of the scheduled legitimate MS and that of the potential EVE with the maximum effective channel gain from the BS. For a given set of potential EVEs attempting to eavesdrop, $\mathcal{M}_{\mathsf{E}}$, the instantaneous achievable secrecy rate for the selected (i.e., scheduled) $\widehat{i}$-th legitimate MS as a function of $\mathcal{M}_{\mathsf{E}}$, σ^2_{MS}, σ^2_{E}, K and ρ is expressed by

$$\begin{aligned} &R_{\mathsf{s}}(\mathcal{M}_{\mathsf{E}}, \sigma^2_{\mathsf{MS}}, \sigma^2_{\mathsf{E}}, K, \rho) \\ &= \log_2\left(1 + \Gamma_{\mathsf{MS},\widehat{i}}\right) - \log_2\left(1 + \max_{j\in\mathcal{M}_{\mathsf{E}}} \Gamma_{\mathsf{E},j}\right) \\ &= \log_2\left(1 + ||\mathbf{h}_{\mathsf{MS},\widehat{i}}||^2\rho\right) \\ &\quad - \log_2\left(1 + \max_{j\in\mathcal{M}_{\mathsf{E}}}\left|\frac{\mathbf{h}_{\mathsf{E},j}\mathbf{h}^H_{\mathsf{MS},\widehat{i}}}{||\mathbf{h}_{\mathsf{MS},\widehat{i}}||}\right|^2\rho\right) \end{aligned} \tag{6}$$

In (6), the effective channel power of the j-th potential EVE follows an exponential distribution, i.e., $\left|(\mathbf{h}_{\mathsf{E},j}\mathbf{h}^H_{\mathsf{MS},\widehat{i}})/||\mathbf{h}_{\mathsf{MS},\widehat{i}}||\right|^2 \sim \mathsf{Exp}(\sigma^{-2}_{\mathsf{E}})$, because $\mathbf{v}_{\mathsf{MS},\widehat{i}} = \mathbf{h}^H_{\mathsf{MS},\widehat{i}}/||\mathbf{h}_{\mathsf{MS},\widehat{i}}||$ is a unit-norm vector and $\mathbf{h}_{\mathsf{E},j}$ is a complex Gaussian random vector, i.e., $\mathbf{h}_{\mathsf{E},j} \sim \mathcal{CN}(\mathbf{0}, \sigma^2_{\mathsf{E}})\mathbf{I}_K$.

In addition, a CSI feedback probability for each legitimate MS should be evaluated. As explained in subsection 3.2, the legitimate MSs opportunistically feed their CSI back to the BS depending on the corresponding channel gain and channel feedback threshold ζ. The expression of the feedback probability can be obtain as follows:

Lemma 1. *When the number of antennas at a BS is K, the channel variance of a legitimate link is σ_{MS^2} and the channel feedback threshold is given by ζ, the feedback probability of each legitimate MS is expressed by*

$$P_{\mathsf{MS}}(\sigma^2_{\mathsf{MS}}, K, \zeta) = e^{-\sigma^{-2}_{\mathsf{MS}}\zeta}\sum_{l=0}^{K-1}\frac{(\sigma^{-2}_{\mathsf{MS}}\zeta)^l}{l!} \tag{7}$$

Proof. Let X_i be a random variable denoting the channel power of the i-th legitimate link, i.e., $X_i \triangleq ||\mathbf{h}_{\mathsf{MS},i}||^2$. Because $||\mathbf{h}_{\mathsf{MS},i}||^2 = \sum_{k=1}^{K}\left|h_{\mathsf{MS},i}(k)\right|^2$ where $h_{\mathsf{MS},i}(k)$ is the k-th element of the legitimate channel vector $\mathbf{h}_{\mathsf{MS},i}$, the random variable X_i is regarded as the sum of K number of independent and identically distributed (i.i.d.) exponential distribution with rate $\sigma_{\mathsf{MS}}^{-2}$. Therefore, the distribution of X_i is given by $X_i \sim \mathsf{Erlang}(K, \sigma_{\mathsf{MS}}^{-2})$. With this distribution, we show that

$$
\begin{aligned}
P_{\mathsf{MS}}(\sigma_{\mathsf{MS}}^2, K, \zeta) &= \Pr\left(X_i \geq \zeta\right) \\
&= 1 - F_{X_i}(\zeta) \\
&= e^{-\sigma_{\mathsf{MS}}^{-2}\zeta} \sum_{l=0}^{K-1} \frac{(\sigma_{\mathsf{MS}}^{-2}\zeta)^l}{l!}
\end{aligned}
$$

where $F_{X_i}(\cdot)$ denotes the commutative distribution function (CDF) of a random variable X_i. □

Based on Lemma 1, we can also derive the average number of legitimate MSs which feed their CSI back to the BS, i.e., $\mathbb{E}[|\mathcal{M}_{\mathsf{MS}}|]$, as follows:

Corollary 1. *For a given number of legitimate MSs, $|\mathcal{N}_{\mathsf{MS}}|$, the average number of legitimate MSs participating in OF is given by*

$$
\mathbb{E}[|\mathcal{M}_{\mathsf{MS}}|] = |\mathcal{N}_{\mathsf{MS}}| e^{-\sigma_{\mathsf{MS}}^{-2}\zeta} \sum_{l=0}^{K-1} \frac{(\sigma_{\mathsf{MS}}^{-2}\zeta)^l}{l!} \tag{8}
$$

when K, σ_{MS^2} and ζ are given.

Proof. Because the channel vectors of legitimate links are i.i.d. complex Gaussian random vectors, the average number of legitimate MSs with CSI feedback is obtained by

$$
\begin{aligned}
\mathbb{E}[|\mathcal{M}_{\mathsf{MS}}|] &= |\mathcal{N}_{\mathsf{MS}}| P_{\mathsf{MS}}(\sigma_{\mathsf{MS}}^2, K, \zeta) \\
&= |\mathcal{N}_{\mathsf{MS}}| e^{-\sigma_{\mathsf{MS}}^{-2}\zeta} \sum_{l=0}^{K-1} \frac{(\sigma_{\mathsf{MS}}^{-2}\zeta)^l}{l!}
\end{aligned}
$$

The second equality holds by Lemma 1. □

4.1. Secrecy outage probability

As a measure of eavesdropping performance that the effects of channel fading, a SOP, which is defined as the probability that an instantaneously achievable eavesdropping rate is less than a given target eavesdropping rate, has been widely used [9, 21]. To derive the SOP in a MU-MISO eavesdropping channel with the OF strategy against RE of potential EVEs, we considered two different cases: one is a case where $|\mathcal{M}_{\mathsf{E}}|$ number of potential EVEs actually participate in eavesdropping and the other is a case where all potential EVEs do not eavesdrop the secure message of a legitimate MS. For the first case, the SOP is derived as follows:

Lemma 2. *When $|\mathcal{M}_{\mathsf{MS}}|$ number of legitimate MSs (out of $|\mathcal{N}_{\mathsf{MS}}|$ legitimate MSs) feed their CSI back to the BS according to the proposed OF strategy and $|\mathcal{M}_{\mathsf{E}}|$ number of potential EVEs (out of $|\mathcal{N}_{\mathsf{E}}|$ potential EVEs) attempt to eavesdrop based on the RE strategy with a given eavesdropping probability P_{E}, the SOP can be derived as*

$$
\begin{aligned}
P_{\mathrm{out}}^{\mathsf{OFRE}} = 1 &- \sum_{m_{\mathsf{MS}}=0}^{|\mathcal{M}_{\mathsf{MS}}|-1} \sum_{m_{\mathsf{E}}=0}^{|\mathcal{M}_{\mathsf{E}}|} \sum_{l=0}^{m_{\mathsf{MS}}(K-1)} \binom{|\mathcal{M}_{\mathsf{MS}}|-1}{m_{\mathsf{MS}}} \binom{|\mathcal{M}_{\mathsf{E}}|}{m_{\mathsf{E}}} \\
&\times \frac{(-1)^{m_{\mathsf{MS}}+m_{\mathsf{E}}} |\mathcal{M}_{\mathsf{MS}}| \sigma_{\mathsf{MS}}^{-2K} (K-1)!^{m_{\mathsf{MS}}}}{\left(\sigma_{\mathsf{MS}}^{-2}(m_{\mathsf{MS}}+1) + \sigma_{\mathsf{E}}^{-2} m_{\mathsf{E}} 2^{-R_{\mathsf{o}}}\right)^{K+l}} \\
&\times \frac{\Gamma\left((K+l), \left(\sigma_{\mathsf{MS}}^{-2}(m_{\mathsf{MS}}+1) + \sigma_{\mathsf{E}}^{-2} m_{\mathsf{E}} 2^{-R_{\mathsf{o}}}\right)\theta\right)}{\Gamma\left(K, \sigma_{\mathsf{MS}}^{-2}\zeta\right)^{m_{\mathsf{MS}}+1}} \\
&\times e^{-\sigma_{\mathsf{E}}^{-2} m_{\mathsf{E}} \rho^{-1} \left(2^{-R_{\mathsf{o}}}-1\right)} c_l
\end{aligned} \tag{9}
$$

where

$$
\theta = \begin{cases} \rho^{-1}(2^{R_{\mathsf{o}}} - 1) & \textit{if } \zeta < \rho^{-1}(2^{R_{\mathsf{o}}} - 1) \\ \zeta & \textit{otherwise} \end{cases}
$$

and $c_l = \sum_{t=1}^{l} (t(m_{\mathsf{MS}}+1) - l) \sigma_{\mathsf{MS}}^{-2t} (t!l)^{-1} c_{l-t}$ and $c_0 = 1$, respectively.

Proof. By the definition of SOP with a target secrecy rate R_{o}, the SOP with OF and RE strategies where $|\mathcal{M}_{\mathsf{E}}| > 0$ is given by

$$
\begin{aligned}
&P_{\mathrm{out}}^{\mathsf{OFRE}}\left(|\mathcal{M}_{\mathsf{MS}}|, |\mathcal{M}_{\mathsf{E}}|, \sigma_{\mathsf{MS}}^2, \sigma_{\mathsf{E}}^2, K, \zeta, \rho, R_{\mathsf{o}}\right) \\
&= \Pr\left(\log_2\left(\frac{1 + \|\mathbf{h}_{\mathsf{MS},\widehat{i}}\|^2 \rho}{1 + \max_{j \in \mathcal{M}_{\mathsf{E}}} \left|\frac{\mathbf{h}_{\mathsf{E},j} \mathbf{h}_{\mathsf{MS},\widehat{i}}^H}{\|\mathbf{h}_{\mathsf{MS},\widehat{i}}\|}\right|^2 \rho}\right) \leq R_{\mathsf{o}}\right) \\
&= 1 - \Pr\left(\log_2\left(\frac{1 + \widehat{X}\rho}{1 + \widehat{Y}\rho}\right) \geq R_{\mathsf{o}}\right)
\end{aligned} \tag{10}
$$

where $\widehat{X} \triangleq \|\mathbf{h}_{\mathsf{MS},\widehat{i}}\|^2 = \max_{i \in \mathcal{M}_{\mathsf{MS}}} \|\mathbf{h}_{\mathsf{MS},i}\|^2$ such that $\|\mathbf{h}_{\mathsf{MS},i}\|^2 \geq \zeta$ and $\widehat{Y} \triangleq \max_{j \in \mathcal{M}_{\mathsf{E}}} \left|\frac{\mathbf{h}_{\mathsf{E},j} \mathbf{h}_{\mathsf{MS},\widehat{i}}^H}{\|\mathbf{h}_{\mathsf{MS},\widehat{i}}\|}\right|^2$. To obtain a closed form expression, the distributions of $\widehat{X}$ and $\widehat{Y}$ need to be investigated. To find the distribution of $\widehat{X}$, we first derive the truncated CDF and probability density function (PDF) of a random variable $\bar{X}_i \triangleq \|\mathbf{h}_{\mathsf{MS},i}\|^2$ such that $\|\mathbf{h}_{\mathsf{MS},i}\|^2 \geq \zeta$ are given by

$$
\begin{aligned}
F_{\bar{X}_i}(x) &= \frac{\Pr(x \geq X_i \geq \zeta)}{\Pr(X \geq \zeta)} \\
&= \frac{\int_{\zeta}^{x} f_{X_i}(x)dx}{\int_{\zeta}^{\infty} f_{X_i}(x)dx} \\
&= 1 - \frac{(K-1)! e^{-\sigma_{\mathsf{MS}}^{-2}x}}{\Gamma(K, \sigma_{\mathsf{MS}}^{-2}\zeta)} \sum_{l=0}^{K-1} \frac{(\sigma_{\mathsf{MS}}^{-2}x)^l}{l!}
\end{aligned} \tag{11}
$$

and

$$
\begin{aligned}
f_{\bar{X}_i}(x) &= \frac{f_{X_i}(x)}{\Pr(X_i \geq \zeta)} \\
&= \frac{f_{X_i}(x)}{\int_{\zeta}^{\infty} f_{X_i}(x)dx} \\
&= \frac{\sigma_{\mathsf{MS}}^{-2K} x^{K-1} e^{-\sigma_{\mathsf{MS}}^{-2}x}}{\Gamma(K, \sigma_{\mathsf{MS}}^{-2}\zeta)} \qquad (12)
\end{aligned}
$$

respectively. In the third equalities of (11) and (12), we use $X_i \triangleq \|\mathbf{h}_{\mathsf{MS},i}\|^2 \sim \mathsf{Erlang}(K, \sigma_{\mathsf{MS}}^{-2})$. By using the order statistics, we further obtain the PDF of $\widehat{X}$ as follows:

$$
\begin{aligned}
f_{\widehat{X}}(x) &= |\mathcal{M}_{\mathsf{MS}}| f_{\bar{X}}(x) F_{\bar{X}}(x)^{|\mathcal{M}_{\mathsf{MS}}|-1} \\
&= \sum_{m_{\mathsf{MS}}=0}^{|\mathcal{M}_{\mathsf{MS}}|-1} \sum_{l=0}^{m_{\mathsf{MS}}(K-1)} \binom{|\mathcal{M}_{\mathsf{MS}}|-1}{m_{\mathsf{MS}}} \\
&\quad \times \frac{(-1)^{m_{\mathsf{MS}}} |\mathcal{M}_{\mathsf{MS}}| \sigma_{\mathsf{MS}}^{-2K} (K-1)!^{m_{\mathsf{MS}}} c_l}{\Gamma\left(K, \sigma_{\mathsf{MS}}^{-2}\zeta\right)^{m_{\mathsf{MS}}+1}} \\
&\quad \times x^{K+l-1} e^{-\sigma_{\mathsf{MS}}^{-2}(m_{\mathsf{MS}}+1)x} \qquad (13)
\end{aligned}
$$

To find the distribution of $\widehat{Y}$, we define a random variable for a channel power of the eavesdropping links with $Y_j = \left|\frac{\mathbf{h}_{\mathsf{E},j}\mathbf{h}_{\mathsf{MS},\widehat{i}}^H}{\|\mathbf{h}_{\mathsf{MS},\widehat{i}}\|}\right|^2$. As discussed previously, the CDF of Y_j is given by

$$
F_{Y_j}(y) = 1 - e^{-\sigma_{\mathsf{E}}^{-2}y}
$$

because $Y_j \sim \mathsf{Exp}(\sigma_{\mathsf{E}}^{-2})$ and Y_j's are i.i.d. Based on the order statistics, the distribution of $\widehat{Y}$ with $|\mathcal{M}_{\mathsf{E}}|$ number of active potential EVEs in a RE policy is also derived by

$$
\begin{aligned}
F_{\widehat{Y}}(y) &= F_{Y_j}(y)^{|\mathcal{M}_{\mathsf{E}}|} \\
&= \sum_{m_{\mathsf{E}}=0}^{|\mathcal{M}_{\mathsf{E}}|} \binom{|\mathcal{M}_{\mathsf{E}}|}{m_{\mathsf{E}}} (-1)^{m_{\mathsf{E}}} e^{-\sigma_{\mathsf{E}}^{-2} m_{\mathsf{E}} y} \qquad (14)
\end{aligned}
$$

With (13) and (14), we can evaluate

$$
\begin{aligned}
&\Pr\left(\log_2\left(\frac{1+\widehat{X}\rho}{1+\widehat{Y}\rho}\right) \geq R_{\mathsf{o}}\right) \\
&= \int_{\theta}^{\infty} f_{\widehat{X}}(x) F_{\widehat{Y}}\left(2^{-R_{\mathsf{o}}}x + \rho^{-1}\left(2^{-R_{\mathsf{o}}}-1\right)\right) dx \\
&= \sum_{m_{\mathsf{MS}}=0}^{|\mathcal{M}_{\mathsf{MS}}|-1} \sum_{m_{\mathsf{E}}=0}^{|\mathcal{M}_{\mathsf{E}}|} \sum_{l=0}^{m_{\mathsf{MS}}(K-1)} \binom{|\mathcal{M}_{\mathsf{MS}}|-1}{m_{\mathsf{MS}}} \binom{|\mathcal{M}_{\mathsf{E}}|}{m_{\mathsf{E}}} \\
&\quad \times \frac{(-1)^{m_{\mathsf{MS}}+m_{\mathsf{E}}} |\mathcal{M}_{\mathsf{MS}}| \sigma_{\mathsf{MS}}^{-2K} (K-1)!^{m_{\mathsf{MS}}}}{\left(\sigma_{\mathsf{MS}}^{-2}(m_{\mathsf{MS}}+1) + \sigma_{\mathsf{E}}^{-2} m_{\mathsf{E}} 2^{-R_{\mathsf{o}}}\right)^{K+l}} \\
&\quad \times \frac{\Gamma\left((K+l), \left(\sigma_{\mathsf{MS}}^{-2}(m_{\mathsf{MS}}+1) + \sigma_{\mathsf{E}}^{-2} m_{\mathsf{E}} 2^{-R_{\mathsf{o}}}\right)\theta\right)}{\Gamma\left(K, \sigma_{\mathsf{MS}}^{-2}\zeta\right)^{m_{\mathsf{MS}}+1}} \\
&\quad \times e^{-\sigma_{\mathsf{E}}^{-2} m_{\mathsf{E}} \rho^{-1}\left(2^{-R_{\mathsf{o}}}-1\right)} c_l \qquad (15)
\end{aligned}
$$

where the $c_l = \sum_{t=1}^{l}(t(m_{\mathsf{MS}}+1) - l)\sigma_{\mathsf{MS}}^{-2t}(t!l)^{-1}c_{l-t}$ and $c_0 = 1$ [36, Equation 0.314], respectively. In addition, the θ is given by

$$
\theta = \begin{cases} \rho^{-1}(2^{R_{\mathsf{o}}}-1) & \text{if } \zeta < \rho^{-1}(2^{R_{\mathsf{o}}}-1) \\ \zeta & \text{otherwise} \end{cases}
$$

where the first line considers the case where the data-rate of R_{o} or less is achieved even if the instantaneous channel gain of a legitimate MS is greater than the channel threshold ζ and the second line considers the case where the instantaneous channel gain achieves the data-rate of R_{o} or more and is greater than the channel threshold ζ. □

There is a possibility that a potential EVE will not attempt to eavesdrop on the secret information of legitimate MSs, depending on an eavesdropping probability in an RE strategy. In this case, a general failure probability can be considered as a secrecy failure probability, since there is no eavesdropping link and it can be obtained as follows:

Lemma 3. *When $|\mathcal{M}_{\mathsf{MS}}|$ number of legitimate MSs (out of N_{MS} legitimate MSs) feed their CSI back to a BS according to the OF strategy and no potential EVE tries to eavesdrop in the RE strategy with a given eavesdropping probability P_{E} (i.e., $|\mathcal{M}_{\mathsf{E}}| = 0$), the SOP can be derived as*

$$
P_{\mathsf{out}}^{\mathsf{OF}} = \left(1 - \frac{(K-1)! e^{-\sigma_{\mathsf{MS}}^{-2}x}}{\Gamma(K, \sigma_{\mathsf{MS}}^{-2}\zeta)} \sum_{l=0}^{K-1} \frac{(K\sigma_{\mathsf{MS}}^{-2}x)^l}{l!}\right)^{|\mathcal{M}_{\mathsf{MS}}|}. \qquad (16)
$$

Proof. As discussed at the beginning of this subsection, a general failure probability that considers only the achievable rate of legitimate links can be considered as a secrecy failure probability and it can be defined as

$$
\begin{aligned}
&P_{\mathsf{out}}^{\mathsf{OF}}\left(|\mathcal{M}_{\mathsf{MS}}|, \sigma_{\mathsf{MS}}^2, K, \zeta, \rho, R_{\mathsf{o}}\right) \\
&= \Pr(\log_2(1+\widehat{X}\rho) \leq R_{\mathsf{o}}) \\
&= F_{\widehat{X}}(\theta) \\
&= F_{\bar{X}}(\theta)^{|\mathcal{M}_{\mathsf{MS}}|} \\
&= \left(1 - \frac{(K-1)! e^{-\sigma_{\mathsf{MS}}^{-2}x}}{\Gamma(K, \sigma_{\mathsf{MS}}^{-2}\zeta)} \sum_{l=0}^{K-1} \frac{(\sigma_{\mathsf{MS}}^{-2}x)^l}{l!}\right)^{|\mathcal{M}_{\mathsf{MS}}|} \qquad (17)
\end{aligned}
$$

In the third equality, we use the fact $\widehat{X} = \max_{i \in \mathcal{M}_{\mathsf{MS}}} \bar{X}_i$ and X_i's are i.i.d. □

Now, we can derive the total failure probability using with Lemmas 1, 2 and 3 as follows:

Theorem 1. *For given N_{MS}, N_{E}, σ_{MS}^2, σ_{E}^2, K, ζ, ρ and R_{o}, the SOP in a MU-MISO wiretap channel can* *be derived as*

$$
\begin{aligned}
&P_{\mathsf{out}}(|\mathcal{N}_{\mathsf{MS}}|, |\mathcal{N}_{\mathsf{E}}|, \sigma^2_{\mathsf{MS}}, \sigma^2_{\mathsf{E}}, K, \zeta, \rho, R_{\mathsf{o}}) \\
&= 1 - \sum_{|\mathcal{M}_{\mathsf{MS}}|=1}^{|\mathcal{N}_{\mathsf{MS}}|} \binom{|\mathcal{N}_{\mathsf{MS}}|}{|\mathcal{M}_{\mathsf{MS}}|} P_{\mathsf{MS}}(\sigma^2_{\mathsf{MS}}, K, \zeta)^{|\mathcal{M}_{\mathsf{MS}}|} \\
&\quad \times (1 - P_{\mathsf{MS}}(\sigma^2_{\mathsf{MS}}, K, \zeta))^{|\mathcal{N}_{\mathsf{MS}}|-|\mathcal{M}_{\mathsf{MS}}|} \\
&\quad \times \Bigg(\sum_{|\mathcal{M}_{\mathsf{E}}|=1}^{|\mathcal{N}_{\mathsf{E}}|} \binom{|\mathcal{N}_{\mathsf{E}}|}{|\mathcal{M}_{\mathsf{E}}|} P_{\mathsf{E}}^{|\mathcal{M}_{\mathsf{E}}|}(1 - P_{\mathsf{E}})^{|\mathcal{N}_{\mathsf{E}}|-|\mathcal{M}_{\mathsf{E}}|} \\
&\quad \times \Big(1 - P^{\mathsf{OFRE}}_{\mathsf{out}}(|\mathcal{M}_{\mathsf{MS}}|, |\mathcal{M}_{\mathsf{E}}|, \sigma^2_{\mathsf{MS}}, \sigma^2_{\mathsf{E}}, K, \zeta, \rho, R_{\mathsf{o}})\Big) \\
&\quad + (1 - P_{\mathsf{E}})^{|\mathcal{N}_{\mathsf{E}}|} \Big(1 - P^{\mathsf{OF}}_{\mathsf{out}}(|\mathcal{M}_{\mathsf{MS}}|, \sigma^2_{\mathsf{MS}}, K, \zeta, \rho, R_{\mathsf{o}}))\Big)\Bigg)
\end{aligned}
\tag{18}
$$

Proof. By plugging in the feedback probability, the SOPs for both cases, i.e., with and without active potential EVEs, we obtain

$$
\begin{aligned}
P_{\mathsf{out}} &= \Pr\Big(R_{\mathsf{s}}(|\mathcal{N}_{\mathsf{MS}}|, |\mathcal{N}_{\mathsf{E}}|, \sigma^2_{\mathsf{MS}}, \sigma^2_{\mathsf{E}}, K, \zeta, \rho) \leq R_{\mathsf{o}}\Big) \\
&= 1 - \Pr\Big(R_{\mathsf{s}}(|\mathcal{N}_{\mathsf{MS}}|, |\mathcal{N}_{\mathsf{E}}|, \sigma^2_{\mathsf{MS}}, \sigma^2_{\mathsf{E}}, K, \zeta, \rho) \geq R_{\mathsf{o}}\Big),
\end{aligned}
$$

where

$$
\begin{aligned}
&\Pr\Big(R_{\mathsf{s}}(|\mathcal{N}_{\mathsf{MS}}|, |\mathcal{N}_{\mathsf{E}}|, \sigma^2_{\mathsf{MS}}, \sigma^2_{\mathsf{E}}, K, \zeta, \rho) \geq R_{\mathsf{o}}\Big) \\
&= \sum_{|\mathcal{M}_{\mathsf{MS}}|=1}^{|\mathcal{N}_{\mathsf{MS}}|} \binom{|\mathcal{N}_{\mathsf{MS}}|}{|\mathcal{M}_{\mathsf{MS}}|} P_{\mathsf{MS}}(\sigma^2_{\mathsf{MS}}, K, \zeta)^{|\mathcal{M}_{\mathsf{MS}}|} \\
&\quad \times (1 - P_{\mathsf{MS}}(\sigma^2_{\mathsf{MS}}, K, \zeta))^{|\mathcal{N}_{\mathsf{MS}}|-|\mathcal{M}_{\mathsf{MS}}|} \\
&\quad \times \Bigg(\sum_{|\mathcal{M}_{\mathsf{E}}|=1}^{|\mathcal{N}_{\mathsf{E}}|} \binom{|\mathcal{N}_{\mathsf{E}}|}{|\mathcal{M}_{\mathsf{E}}|} P_{\mathsf{E}}^{|\mathcal{M}_{\mathsf{E}}|}(1 - P_{\mathsf{E}})^{|\mathcal{N}_{\mathsf{E}}|-|\mathcal{M}_{\mathsf{E}}|} \\
&\quad \times \Big(1 - P^{\mathsf{OFRE}}_{\mathsf{out}}(|\mathcal{M}_{\mathsf{MS}}|, |\mathcal{M}_{\mathsf{E}}|, \sigma^2_{\mathsf{MS}}, \sigma^2_{\mathsf{E}}, K, \zeta, \rho, R_{\mathsf{o}})\Big) \\
&\quad + (1 - P_{\mathsf{E}})^{|\mathcal{N}_{\mathsf{E}}|} \Big(1 - P^{\mathsf{OF}}_{\mathsf{out}}(|\mathcal{M}_{\mathsf{MS}}|, \sigma^2_{\mathsf{MS}}, K, \zeta, \rho, R_{\mathsf{o}}))\Big)\Bigg)
\end{aligned}
$$

We use the binomial expansion formula [36] to account for all the cases where all legitimate MSs and potential EVEs operate.

□

4.2. Secrecy energy-efficiency

As another measure of secrecy performance with respect to energy efficiency, the SEE has been widely used [21, 37, Sec.II-C-2)]. The SEE is generally defined as the ratio of secrecy throughput to power consumption. By exploiting the fading effects of wireless channels, the secrecy throughput in the definition of SEE can be calculated as the product of a target secrecy rate and non-outage probability. That is, SEE, η, is defined as

$$
\begin{aligned}
&\eta(|\mathcal{N}_{\mathsf{MS}}|, |\mathcal{N}_{\mathsf{E}}|, \sigma^2_{\mathsf{MS}}, \sigma^2_{\mathsf{E}}, K, \zeta, \rho, R_{\mathsf{o}}) \\
&\triangleq \frac{R_{\mathsf{o}}(1 - P_{\mathsf{out}}(|\mathcal{N}_{\mathsf{MS}}|, |\mathcal{N}_{\mathsf{E}}|, \sigma^2_{\mathsf{MS}}, \sigma^2_{\mathsf{E}}, K, \zeta, \rho, R_{\mathsf{o}}))}{P(1 + \beta\mathbb{E}[|\mathcal{M}_{\mathsf{MS}}|])}
\end{aligned}
\tag{19}
$$

where P is power consumption for a BS to transmit data and β is a ratio of power consumption for a single legitimate MS to that for a BS. Therefore, $P(\beta\mathbb{E}[|\mathcal{N}_{\mathsf{MS}}|])$ in (19) means the average power consumption for the legitimate MSs of which channel power is higher than a threshold ζ, i.e., $\mathbb{E}[|\mathcal{M}_{\mathsf{MS}}|]$ number of legitimate MSs on average, to feed their CSI back to the BS.

The average number of legitimate MSs participating in OF decreases and the SOP increases as the channel feedback threshold ζ increases. Therefore, there is a trade-off between secrecy throughput and average power consumption in SEE. It means that the optimal channel feedback threshold ζ that maximizes SEE can be found. However, this optimal solution is difficult to find analytically because SEE as a function of a feedback threshold, $\eta(|\mathcal{N}_{\mathsf{MS}}|, |\mathcal{N}_{\mathsf{E}}|, \sigma^2_{\mathsf{MS}}, \sigma^2_{\mathsf{E}}, K, \zeta, \rho, R_{\mathsf{o}})$ in (19), is in a very complicated form. Instead, the existence of the optimal ζ and its result are numerically verified in Section 5.

5. Numerical results

In this section, the SOP and SEE performance in multi-user MISO downlink cellular networks with different system parameters are evaluated through 10 million Monte Carlo simulations using MATLAB. Furthermore, to derive a mathematical closed-form expression of the SOP, we assume the independent and identically distributed (i.i.d.) Rayleigh fading channels from the legitimate BS to all legitimate MSs and to all potential EVEs. The terms $|\mathcal{M}_{\mathsf{MS}}|$ and $|\mathcal{M}_{\mathsf{E}}|$ are assumed to be random variables following a binomial distribution with parameters the feedback probability P_{MS} and the eavesdropping probability P_{E}, respectively. We use these two random variables in our simulations for verifying the closed-form expression of SOP performance. As explained in Section 2, it is assumed that all channel coefficients are independent complex Gaussian random variables, i.e., Rayleigh fading channels are assumed. The channel variances for legitimate and eavesdropping links are given by $\sigma^2_{\mathsf{MS}} = 1$ and $\sigma^2_{\mathsf{E}} = 0.5$ to reflect physical distance from a BS to legitimate MSs and potential EVEs, respectively. Depending on the channel realizations, both $|\mathcal{M}_{\mathsf{MS}}|$ and $|\mathcal{M}_{\mathsf{E}}|$ become random variables of which characteristics is determined by the feedback probability $P_{\mathsf{MS}}(\sigma^2_{\mathsf{MS}}, K, \zeta)$ and the eavesdropping P_{E}, respectively. In the numerical simulations to evaluate the SOP, the target secrecy rate is set to be $R_{\mathsf{o}} = 1$ [bps/Hz]. As benchmarks to show the effectiveness of the proposed OF scheme, the FF and FE strategies, i.e., a channel threshold $\zeta = 0$ in an OF strategy and a random eavesdropping probability $P_{\mathsf{E}} = 1$ in an RE strategy, are considered. As another benchmark, a single-antenna case in [21] is considered. In particular, we only consider a FF strategy in the benchmark of [21] (i.e., $K = 1$ and $\zeta = 0$) because

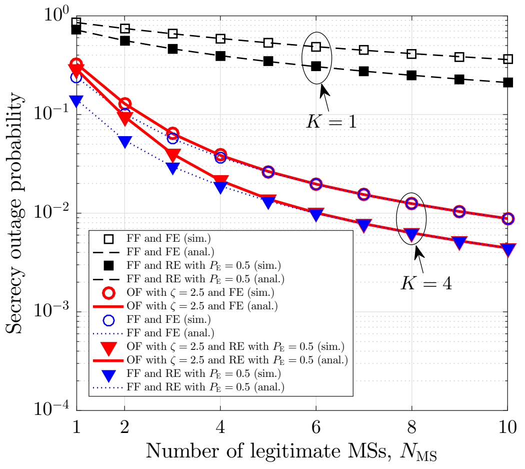


Fig. 2. SOP with respect to N_{MS}, when $\rho = 5$ [dB], $K \in \{1, 4\}$, $N_{\mathsf{E}} = 4$ and $P_{\mathsf{E}} \in \{0.5, 1\}$.

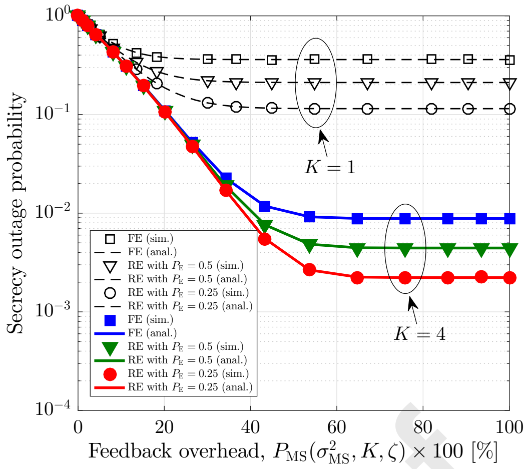


Fig. 3. SOP with respect to feedback overhead, when $\rho = 5$ [dB], $K \in \{1, 4\}$, $N_{\mathsf{MS}} = 10$ and $P_{\mathsf{E}} \in \{0.25, 0.5, 1\}$.

the FF strategy always shows better performance than an OF strategy in terms of SOP.

Figure 2 illustrates the SOP performance with respect to the number of legitimate MSs N_{MS}, when $\rho = 5$ [dB], $K \in \{1, 4\}$, $N_{\mathsf{E}} = 4$ and $P_{\mathsf{E}} \in \{0.5, 1\}$. As the number of legitimate MSs N_{MS} or the number of transmit antennas K increases, the SOP decreases monotonically due to multi-user diversity or antenna gain, i.e., beamforming gain. Moreover, as the eavesdropping probability P_{E} decreases, the SOP decreases because the average number of potential EVEs attempting to eavesdrop $\mathbb{E}[|\mathcal{M}_{\mathsf{E}}|]$ decreases. It is shown that the FF strategy always outperforms the OF strategy in terms of SOP because not all legitimate MSs in the OF strategy feed their CSI back to the BS. Furthermore, the performance difference between FF and OF strategies can be neglected when the number of legitimate MSs is large enough. For example, the SOP gap can be neglected when $N_{\mathsf{MS}} \geq 12$ in the cases of $K = 4$, $\zeta = 1$, and $P_{\mathsf{E}} = \{0.5, 1\}$. When $K = 4$ and $\zeta = 2.5$, the feedback probability can be calculated as $P_{\mathsf{MS}}(\sigma^2_{\mathsf{MS}}, K, \zeta) \approx 0.7576$ with Lemma 1. This means that the feedback overhead of the proposed OF strategy can be reduced by approximately 75.76% compared to that of the FF strategy while obtaining negligible SOP performance gap.

When $\rho = 5$ [dB], $K \in \{1, 4\}$, $N_{\mathsf{MS}} = 10$, $N_{\mathsf{E}} = 4$ and $P_{\mathsf{E}} \in \{0.25, 0.5, 1\}$, SOP with respect to feedback overhead $P_{\mathsf{MS}}(\sigma^2_{\mathsf{MS}}, K, \zeta)$ is shown in Figure 3. As the feedback overhead increases, the multi-antenna case with $K = 4$ case shows lower SOP than the single-antenna case with $K = 1$ thanks to MRT beamforming gain. In addition, when the feedback overhead exceeds a certain level because a given N_{MS}, the SOP performance gain is saturated. The saturated level, i.e., the converged SOP, is the minimal SOP which is obtained by the OF strategy under the given condition and it can be regarded as the SOP of the FF strategy. Therefore, it can be shown that we can roughly achieve the lowest SOP even with an OF strategy. This means that we can maximize overall system performance taking into account both the downlink secure transmission and the uplink CSI feedback overhead with an OF strategy with an appropriate feedback threshold ζ. The relationship between feedback overhead and the channel threshold ζ is shown as in the next figure.

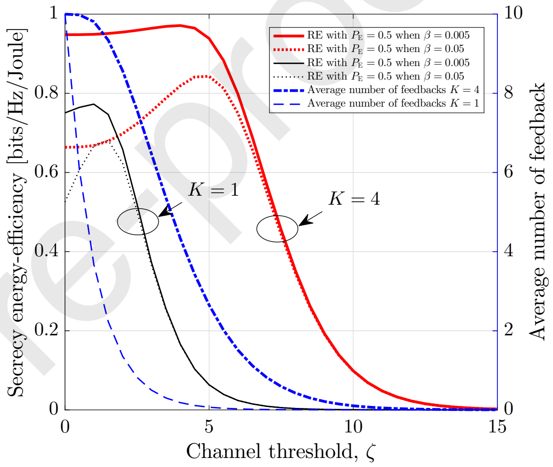


Fig. 4. SEE and the average number of MSs with feedback for varying the ζ when $\rho = 5$ [dB], $K \in \{1, 4\}$, $N_{\mathsf{MS}} = 10$, $N_{\mathsf{E}} = 4$, $\beta \in \{0.005, 0.05\}$ and $P_{\mathsf{E}} = 0.5$.

Figure 4 illustrates the SEE performance with respect to the feedback threshold ζ, when $K \in \{1, 4\}$, $\rho = 5$ [dB], $N_{\mathsf{MS}} = 10$, $N_{\mathsf{E}} = 4$, and $P_{\mathsf{E}} \in \{0.5, 1\}$. Since the feedback threshold ζ increases or the ratio of the power consumption at the legitimate MS β decreases, the average number of feedbacks $\mathbb{E}[|\mathcal{M}_{\mathsf{MS}}|]$ decreases monotonically, but the SEE performance has the optimal point to maximize the SEE performance. There is a fundamental trade-off between the SOP and SEE by varying the channel threshold ζ.

6. Conclusions

In this paper, we mathematically analyzed the Secrecy Outage Probability (SOP) and Secrecy Energy-

Efficiency (SEE) performance of a Multi-User Multi-Input Single-Output (MU-MISO) downlink cellular networks consisting of one legitimate Base Station (BS), multiple legitimate Mobile Station (MSs) and multiple potential eavesdroppers (EVEs). In our system model, each potential EVE tries to eavesdrop with a certain random eavesdropping probability for the Random Eavesdropping (RE) strategy. In addition, each legitimate MS opportunistically feeds back the effective channel gain to the legitimate BS for data reception for the proposed Opportunistic Feedback (OF) strategy which can reduce the signal overhead for user feedback and improve SEE performance. Using computer simulations, we have shown that our results are in agreement with our numerical results depending on various system parameters. Furthermore, we find that the effects and the trade-offs on the SOP and SEE depend on the channel threshold for the OF strategy. To the best of our knowledge, this work is the worst-first SOP and SEE performance analysis in MU-MISO downlink cellular networks with multiple potential EVEs. For the case of MU-MIMO cellular networks with multiple potential EVEs and colluding potential EVEs, we leave the SOP performance analysis to further.

Acknowledgements

This work is supported in part by the National Research Foundation of Korea (NRF) funded by the Korea government (MSIT) under Grant NRF-2022R1I1A3073740 and in part by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (2022-0-00704, Development of 3D-NET Core Technology for High-Mobility Vehicular Service).

References

[1] A. D. Wyner, The wire-tap channel, The Bell System Technical Journal 54 (8) (1975) 1355–1387.

[2] Y. Zou, J. Zhu, X. Wang, L. Hanzo, A survey on wireless security: Technical challenges, recent advances, and future trends, Proceedings of the IEEE 104 (9) (2016) 1727–1765.

[3] S. K. Leung-Yan-Cheong, M. E. Hellman, The Gaussian wire-tap channel, IEEE Transactions on Information Technology IT-24 (4) (1978) 451–456.

[4] M. Bloch, J. Barros, M. R. D. Rodrigues, S. W. McLaughlin, Wireless information-theoretic security, IEEE Transactions on Information Technology 54 (6) (2008) 2515–2534.

[5] Y. Liang, H. V. Poor, Multiple-access channels with confidential messages, IEEE Transactions on Information Technology 54 (3) (2008) 976–1002.

[6] A. Khisti, G. W. Wornell, Secure transmission with multiple antennas I: The MISOME wiretap channel, IEEE Transactions on Information Technology 56 (7) (2010) 3088–3104.

[7] A. Khisti, G. W. Wornell, Secure transmissionwith multiple antennas—Part II: The MIMOME wiretap channel, IEEE Transactions on Information Technology 56 (11) (2010) 5515–5532.

[8] H. Yu, J. Joung, Secure IoT communications using HARQ-based beamforming for MISOSE channels, IEEE Internet of Things Journal 8 (23) (2021) 17211–17226.

[9] H. Yu, J. Joung, Design of the power and dimension of artificial noise for secure communication systems, IEEE Transactions on Communications 69 (6) (2021) 4001–4010.

[10] H. Yu, T. Kim, Training and data structures for AN-aided secure communication, IEEE Systems Journal 13 (3) (2019) 2869–2872.

[11] H. Yu, T. Kim, H. Jafarkhani, Wireless secure communication with beamforming and jamming in time-varying wiretap channels, IEEE Transactions on Information Forensics and Security 13 (8) (2018) 2087–2100.

[12] L. Mucchi, S. Jayousi, S. Caputo, E. Panayirci, S. Shahabuddin, J. Bechtold, I. Morales, R.-A. Stoica, G. Abreu, H. Haas, Physical-layer security in 6G networks, IEEE Open Journal of the Communications Society 2 (2021) 1901–1914.

[13] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, M. Ylianttila, The roadmap to 6G security and privacy, IEEE Open Journal of the Communications Society 2 (2021) 1094–1122.

[14] 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.

[15] 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.

[16] H. Yu, I.-G. Lee, Physical layer security based on NOMA and AJ for MISOSE channels with an untrusted relay, Future Generation Computer Systems 102 (2020) 611–618.

[17] 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.

[18] S. H. Islam, A. S. M. Badrudduza, S. M. R. Islam, F. I. Shahid, I. S. Ansari, M. K. Kundu, H. Yu, 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 Photonics Journal 13 (2) (2021) 1–17.

[19] A. S. M. Badrudduza, M. Ibrahim, S. M. R. Islam, M. S. Hossen, M. K. Kundu, I. S. Ansari, H. Yu, Security at the physical layer over GG fading and mEGG turbulence induced RF-UOWC mixed system, IEEE Access 9 (2021) 18123–18136.

[20] M. A. Abbas, H. Song, J.-P. Hong, Opportunistic scheduling for average secrecy rate enhancement in fading downlink channel with potential eavesdroppers, IEEE Transactions on Information Forensics and Security 14 (4) (2019) 969–980.

[21] W. Son, H. Nam, W.-Y. Shin, B. C. Jung, Secrecy outage analysis of multiuser downlink wiretap networks with potential eavesdroppers, IEEE Systems Journal 15 (2) (2021) 3093–3096.

[22] H. Jin, W.-Y. Shin, B. C. Jung, On the multi-user diversity with secrecy in uplink wiretap networks, IEEE Communication Letters 17 (9) (2013) 1778–1781.

[23] H. He, X. Luo, J. Weng, K. Wei, Secure transmission in multiple access wiretap channel: Cooperative jamming without sharing CSI, IEEE Transactions on Information Forensics and Security 16 (2021) 3401–3411.

[24] A. Hamyani, F. E. Bouanani, Y. Miftah, Jamming-assisted multi-user multi-eavesdropper broadcast network: PHY layer security analysis, IEEE Access 9 (2021) 118051–118064.

[25] J. Choi, J. Joung, B. C. Jung, Space-time line code for enhancing physical layer security of multiuser MIMO uplink transmission, IEEE Systems Journal 15 (3) (2021) 3336–3347.

[26] Z. Tang, L. Sun, X. Tian, D. Niyato, Y. Zhang, Artificial-noise-aided coordinated secure transmission design in multi-cell multi-antenna networks with limited feedback, IEEE Transactions on Vehicular Technology 71 (2) (2022) 1750–1765.

[27] 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 Journal on Selected Ar-

eas in Communications 36 (4) (2018) 679–695.

[28] J. M. Hamamreh, H. M. Furqan, H. Arslan, Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey, IEEE Communications Surveys and Tutorials 21 (2) (2019) 1773–1828.

[29] J. Qiu, K. Xu, X. Xia, Z. Shen, W. Xie, D. Zhang, M. Wang, Secure transmission scheme based on fingerprint positioning in cell-free massive MIMO systems, IEEE Transactions on Signal and Information Processing over Networks 8 (2022) 92–105.

[30] I. Bang, B. C. Jung, Secrecy rate analysis of opportunistic user scheduling in uplink networks with potential eavesdroppers, IEEE Access 7 (2019) 127078–127089.

[31] W. Son, H. S. Jang, B. C. Jung, A pseudo-random beamforming technique for improving physical-layer security of MIMO cellular networks, MDPI Entropy 21 (11) (2019) 1038.

[32] J. Youn, W. Son, B. C. Jung, Physical-layer security improvement with reconfigurable intelligent surfaces for 6G wireless communication systems, MDPI Sensors 21 (4) (2021) 1439.

[33] M. T. Mamaghani, Y. Hong, Terahertz meets untrusted UAV-relaying: Minimum secrecy energy efficiency maximization via trajectory and communication co-design, IEEE Transactions on Vehicular Technology 71 (5) (2022) 4991–5006.

[34] N. Su, F. Liu, C. Masouros, Secure radar-communication systems with malicious targets: Integrating radar, communications and jamming functionalities, IEEE Transaction on Wireless Communications 20 (1) (2021) 83–95.

[35] J. Joung, J. Choi, B. C. Jung, S. Yu, Artificial noise injection and its power loading methods for secure space-time line coded systems, MDPI Entropy 21 (5) (2019) 515.

[36] I. S. Gradshteyn, I. M. Ryzhik, Table of Integrals, Series and Products, Seventh ed., Academic, 2007.

[37] J. Farhat, G. Brante, R. D. Souza, On the secure energy efficiency of TAS/MRC with relaying and jamming strategies, IEEE Signal Processsing Letters 24 (8) (2017) 1228–1232.

Declaration of interests

☒ 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.

☒The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: