Short Papers

Secrecy Outage Analysis of Multiuser Downlink Wiretap Networks With Potential Eavesdroppers

Woong Son, *Student Member, IEEE*, Hyunwoo Nam, *Student Member, IEEE*, Won-Yong Shin, *Senior Member, IEEE*, and Bang Chul Jung, *Senior Member, IEEE*

***Abstract*—We investigate the secrecy outage probability (SOP) of a downlink wiretap network consisting of a single legitimate base station (BS), multiple legitimate mobile stations (MSs), and multiple *potential* eavesdroppers (EVEs), where each EVE randomly attempts to overhear the data transmission with a certain probability. In particular, we consider an opportunistic feedback (OF) strategy in which each legitimate MS feeds their channel gain back to the BS for data reception only when its gain is greater than a certain threshold. We analyze a closed-form expression of the SOP under this strategy. As our main result, we demonstrate that the SOP of the OF strategy approaches that of the full feedback strategy as the number of legitimate MSs becomes large. It is worth noting that, for the first time, we mathematically characterize the SOP in this practical wiretap network setting having multiple potential EVEs.**

***Index Terms*—Multiuser diversity, opportunistic feedback, physical-layer security (PLS), potential eavesdropper, secrecy energy efficiency (SEE), secrecy outage probability (SOP).**

I. Introduction

Physical-layer security (PLS) has steadily gained attention from both academia and industry, where the PLS is built upon a notion of information-theoretic secrecy exploiting the randomness of wireless channels [1]. Many technical aspects of various 5G wireless networks such as massive multiple-input multiple-output, nonorthogonal multiple access, full-duplex, millimeter wave communications, heterogeneous networks, and so forth have been extensively investigated in terms of PLS [2].

Existing studies on the PLS in the literature have been carried out under the following three different eavesdropping scenarios: passive, active, and potential eavesdropping cases [3]–[6].

Passive eavesdroppers (EVEs) only overhear and attempt to decode the packet of legitimate nodes; thus, the channel state information (CSI) of the passive EVEs is usually assumed to be unavailable at legitimate nodes [3]. On the other hand, active EVEs are regarded as being registered in the associated network and pretend to be legitimate nodes. The active EVEs not only attempt to decode the private message of legitimate nodes, but also induce the network to malfunction through pilot contamination or false feedback information [3]. Recently, the concept of potential eavesdropping was introduced in [5] and [6]. In [5], all unscheduled legitimate nodes in a certain cell are defined as potential EVEs, while some of the unscheduled legitimate nodes in a certain cell are defined as potential EVEs in [6]. The term of *potential* is used in the sense that EVEs can also participate in their own legitimate communications.

In this paper, we investigate the effect of intermittent operation of potential EVEs on the secrecy outage probability (SOP) [7] in a multiuser downlink wiretap network, which consists of a single legitimate BS, multiple legitimate MSs, and multiple *potential* noncolluding EVEs. Furthermore, we propose an *opportunistic feedback* (OF) strategy such that each legitimate MS feeds its channel gain back to the BS only when the gain is greater than a certain threshold, which enables us to perform energy-efficient communications.

The rest of this paper is organized as follows. In Section II, the proposed technique are explained and compared with existing schemes and its SOP is mathematically analyzed. Numerical results are shown in Section III and concluding remarks are drawn in Section IV.

II. Multiuser Downlink Wiretap Networks With Potential Eavesdroppers

A. System Model

We consider a single-cell downlink wiretap network consisting of a legitimate BS, legitimate MSs, and potential EVEs as illustrated in Fig. 1. In this paper, we assume that the potential EVEs belong to other cells as legitimate MSs, but they can attempt to overhear legitimate communications of other cells.[1] All devices are assumed to be equipped with a single antenna. We also consider noncolluding potential EVEs, each of which does not share eavesdropping data with other EVEs [5], [6]. System parameters are summarized in Table I. The received signals at the ith legitimate MS and the jth potential EVE are given by

$$r_{\mathsf{MS},i} = h_{\mathsf{MS},i}x + z_{\mathsf{MS},i}, \quad r_{\mathsf{E},j} = h_{\mathsf{E},j}x + z_{\mathsf{E},j} \tag{1}$$

respectively, where $z_{\mathsf{MS},i}$, $z_{\mathsf{E},j} \sim \mathcal{CN}(0, N_0)$ and x denotes the transmit signal at the BS with the power constraint $\mathbb{E}[|x|^2] = P$. All wireless channels are assumed to follow independent and identically distributed

Manuscript received February 5, 2020; revised May 16, 2020 and June 23, 2020; accepted July 1, 2020. Date of publication July 17, 2020; date of current version June 7, 2021. This work was supported in part by the NRF through the Basic Science Research Program funded by the Ministry of Science and ICT under Grant NRF2019R1A2B5B01070697 and in part by the Yonsei University Research Fund of 2020 under Grant 2020-22-0101. *(Corresponding authors: Won-Yong Shin; Bang Chul Jung.)*

Woong Son and Bang Chul Jung are with the Department of Electronics Engineering, Chungnam National University, Daejeon 34134, South Korea (e-mail: woongson@cnu.ac.kr; bcjung@cnu.ac.kr).

Hyunwoo Nam is with the School of Electrical Engineering Korea Advanced Institute of Science and Technology, Daejeon 34141, South Korea (e-mail: hw.nam@kaist.ac.kr).

Won-Yong Shin is with the Department of Computational Science and Engineering, Yonsei University, Seoul 03722, South Korea (e-mail: wy.shin@yonsei.ac.kr).

Digital Object Identifier 10.1109/JSYST.2020.3007434

[1]The definition of potential EVEs in this paper follows the definition and context of existing papers [5], [6], but it can be considered as a more advanced and generalized concept.

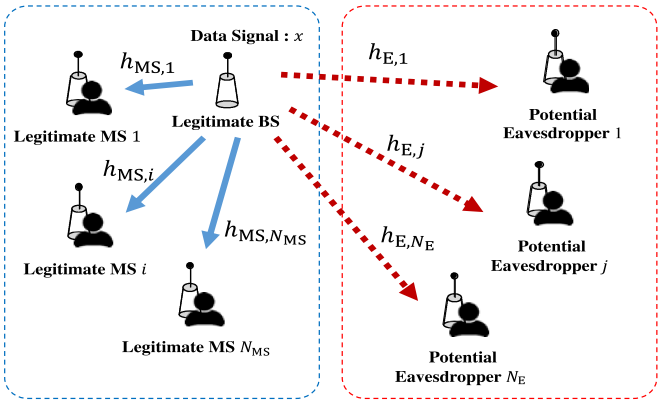

Fig. 1. Illustration of a downlink wiretap network with multiple legitimate MSs and multiple EVEs.

TABLE I
SYSTEM PARAMETERS

Parameters	Definitions
N_{MS} / N_{E}	Number of legitimate MSs / potential EVEs
$\mathcal{N}_{\mathsf{MS}}$ / $\mathcal{N}_{\mathsf{E}}$	Set of all of legitimate MSs / potential EVEs
$\mathcal{M}_{\mathsf{MS}}$ / $\mathcal{M}_{\mathsf{E}}$	Set of legitimate MSs that feed their channel gain back to the BS / potential EVEs that attempt to overhear
$h_{\mathsf{MS},i}$ / $h_{\mathsf{E},j}$	Wireless channel coefficient from the legitimate BS to the i-th legitimate MS / to the j-th potential EVE
$z_{\mathsf{MS},i}$ / $z_{\mathsf{E},j}$	AWGN at the i-th legitimate MS / at the j-th potential EVE

(i.i.d.) circular Gaussian complex random variables with different variances, i.e., $h_{\mathsf{MS},i} \sim \mathcal{CN}(0, 1/\lambda_{\mathsf{MS}})$ and $h_{\mathsf{E},j} \sim \mathcal{CN}(0, 1/\lambda_{\mathsf{E}})$, where $\forall i \in \mathcal{N}_{\mathsf{MS}} \triangleq \{1, 2, \ldots, N_{\mathsf{MS}}\}$ and $\forall j \in \mathcal{N}_{\mathsf{E}} \triangleq \{1, 2, \ldots, N_{\mathsf{E}}\}$.[2]

B. Proposed Technique

We describe the overall procedure of our method, which includes OF at the legitimate MSs and random intermittent operation at the potential EVEs.

1) Pilot Broadcast: The BS broadcasts a pilot signal, which enable all legitimate MSs and potential EVEs to estimate the wireless channel coefficients $h_{\mathsf{MS},i}$ and $h_{\mathsf{E},j}$ for all i and j.

2) Opportunistic Feedback (OF): Only a few legitimate MSs among all MSs feed their channel gain back to the BS to reduce the signaling overhead and improve energy efficiency. Specifically, the ith legitimate MS feeds its channel gain $\gamma_{\mathsf{MS},i} = |h_{\mathsf{MS},i}|^2 \sim \exp(\lambda_{\mathsf{MS}})$ back to the BS only when $\gamma_{\mathsf{MS},i} > \zeta_{\mathsf{MS}}$, where ζ_{MS} indicates a certain positive threshold. The probability density function (PDF) and cumulative distribution function (CDF) of $\gamma_{\mathsf{MS},i}$ are given as $f_{\gamma_{\mathsf{MS}}}(y) = \lambda_{\mathsf{MS}} e^{-\lambda_{\mathsf{MS}} y}$ and $F_{\gamma_{\mathsf{MS}}}(y) = 1 - e^{-\lambda_{\mathsf{MS}} y}$ when $y \geq 0$, respectively. Then, the feedback probability is $P_{\mathsf{MS}} = \Pr(Y \geq \zeta_{\mathsf{MS}}) = \int_{\zeta_{\mathsf{MS}}}^{\infty} f_{\gamma_{\mathsf{MS}}}(y) dy = e^{-\lambda_{\mathsf{MS}} \zeta_{\mathsf{MS}}} \in [0, 1]$, which depends on both λ_{MS} and the channel threshold ζ_{MS}. In particular, when $\zeta_{\mathsf{MS}} = 0$ as a special case of OF, it follows that $P_{\mathsf{MS}} = 1$; thus, all of legitimate MSs operate in full feedback (FF) strategy.

3) Random Eavesdropping (RE): Each EVE attempts to overhear the data transmission with eavesdropping probability $P_{\mathsf{E}} \in [0, 1]$, which can be determined by its own traffic load and communication protocol. When $P_{\mathsf{E}} = 1$ as a special case of RE, EVEs operate as the full eavesdropping (FE) strategy like conventional EVEs.

4) Scheduling and Transmission: The BS selects one legitimate MS with the maximum channel gain and starts transmission.

The instantaneous achievable secrecy rate is given by

$$R_{\mathsf{s}}\left(|\mathcal{M}_{\mathsf{MS}}|, \lambda_{\mathsf{MS}}, \zeta_{\mathsf{MS}}, |\mathcal{M}_{\mathsf{E}}|, \lambda_{\mathsf{E}}, \rho\right) = \log_2\left(\frac{1 + \max\limits_{i \in \mathcal{M}_{\mathsf{MS}}} \gamma_{\mathsf{MS},i}\rho}{1 + \max\limits_{j \in \mathcal{M}_{\mathsf{E}}} \gamma_{\mathsf{E},j}\rho}\right)$$

where $\rho = P/N_0$, $\gamma_{\mathsf{E},m_{\mathsf{E}}} = |h_{\mathsf{E},m_{\mathsf{E}}}|^2 \sim \exp(\lambda_{\mathsf{E}})$, and $|\cdot|$ indicates the cardinality of set.

C. Performance Analysis

1) SOP: For the OF and RE strategies, we derive a closed-form expression of the SOP in this section.

Theorem 1: For a given target secrecy rate R_{o}, the SOP is expressed as

$$\begin{aligned} &P_{\mathsf{outage}}^{\mathsf{OFRE}}(N_{\mathsf{MS}}, \lambda_{\mathsf{MS}}, \zeta_{\mathsf{MS}}, N_{\mathsf{E}}, \lambda_{\mathsf{E}}, P_{\mathsf{E}}, \rho, R_{\mathsf{o}}) \\ &= 1 - \sum_{|\mathcal{M}_{\mathsf{MS}}|=1}^{N_{\mathsf{MS}}} \binom{N_{\mathsf{MS}}}{|\mathcal{M}_{\mathsf{MS}}|} P_{\mathsf{MS}}^{|\mathcal{M}_{\mathsf{MS}}|}(1 - P_{\mathsf{MS}})^{N_{\mathsf{MS}} - |\mathcal{M}_{\mathsf{MS}}|} \\ &\quad \times \left[\sum_{|\mathcal{M}_{\mathsf{E}}|=1}^{N_{\mathsf{E}}} \binom{N_{\mathsf{E}}}{|\mathcal{M}_{\mathsf{E}}|} P_{\mathsf{E}}^{|\mathcal{M}_{\mathsf{E}}|}(1 - P_{\mathsf{E}})^{N_{\mathsf{E}} - |\mathcal{M}_{\mathsf{E}}|} \right. \\ &\qquad \times \Psi_{\mathsf{non}}^{\mathsf{OFRE}}(|\mathcal{M}_{\mathsf{MS}}|, \lambda_{\mathsf{MS}}, \zeta_{\mathsf{MS}}, |\mathcal{M}_{\mathsf{E}}|, \lambda_{\mathsf{E}}, \rho, R_{\mathsf{o}}) \\ &\qquad \left. + (1 - P_{\mathsf{E}})^{N_{\mathsf{E}}} \Psi_{\mathsf{non}}^{\mathsf{OF}}(|\mathcal{M}_{\mathsf{MS}}|, \lambda_{\mathsf{MS}}, \zeta_{\mathsf{MS}}, \rho, R_{\mathsf{o}}) \right] \end{aligned} \tag{2}$$

where $\Psi_{\mathsf{non}}^{\mathsf{OFRE}}(|\mathcal{M}_{\mathsf{MS}}|, \lambda_{\mathsf{MS}}, \zeta_{\mathsf{MS}}, |\mathcal{M}_{\mathsf{E}}|, \lambda_{\mathsf{E}}, \rho, R_{\mathsf{o}})$ and $\Psi_{\mathsf{non}}^{\mathsf{OF}}(|\mathcal{M}_{\mathsf{MS}}|, \lambda_{\mathsf{MS}}, \zeta_{\mathsf{MS}}, \rho, R_{\mathsf{o}})$ denote the secrecy nonoutage probability in case of the OF and RE strategies, and the secrecy nonoutage probability in case of the OF and all-inactive eavesdropping strategy, respectively.

Proof: Refer to Appendix A. ■

It is possible to derive the SOP with other feedback and eavesdropping strategies. For example, the SOP in FF and RE strategy $P_{\mathsf{outage}}^{\mathsf{FFRE}}(N_{\mathsf{MS}}, \lambda_{\mathsf{MS}}, \zeta_{\mathsf{MS}}, N_{\mathsf{E}}, \lambda_{\mathsf{E}}, P_{\mathsf{E}}, \rho, R_{\mathsf{o}})$ under the FF and RE strategies can be obtained by setting $\zeta_{\mathsf{MS}} = 0$. Similarly, $P_{\mathsf{outage}}^{\mathsf{OFFE}}(N_{\mathsf{MS}}, \lambda_{\mathsf{MS}}, \zeta_{\mathsf{MS}}, N_{\mathsf{E}}, \lambda_{\mathsf{E}}, P_{\mathsf{E}}, \rho, R_{\mathsf{o}})$ under the OF and FE strategies can be obtained by setting $P_{\mathsf{E}} = 1$.

2) Secrecy Energy Efficiency: We also obtain secrecy energy efficiency (SEE) [8]. From (2), the SEE for the OF and RE strategies is given by

$$\begin{aligned} \eta^{\mathsf{OFRE}} &= \mathbb{E}\left[\frac{R_{\mathsf{o}}(1 - P_{\mathsf{outage}}^{\mathsf{OFRE}}(N_{\mathsf{MS}}, \lambda_{\mathsf{MS}}, \zeta_{\mathsf{MS}}, N_{\mathsf{E}}, \lambda_{\mathsf{E}}, P_{\mathsf{E}}, \rho, R_{\mathsf{o}})}{P(1 + \beta \sum_{i=1}^{N_{\mathsf{MS}}} I_{\mathsf{MS}}(i))}\right] \\ &= \frac{R_{\mathsf{o}}(1 - P_{\mathsf{outage}}^{\mathsf{OFRE}}(N_{\mathsf{MS}}, \lambda_{\mathsf{MS}}, \zeta_{\mathsf{MS}}, N_{\mathsf{E}}, \lambda_{\mathsf{E}}, P_{\mathsf{E}}, \rho, R_{\mathsf{o}}))}{P} \\ &\quad \times \sum_{i=1}^{N_{\mathsf{MS}}} \binom{N_{\mathsf{MS}}}{i} \frac{1}{1 + \beta \cdot i} P_{\mathsf{MS}}^{i}(1 - P_{\mathsf{MS}})^{N_{\mathsf{MS}} - i} \end{aligned}$$

where β denotes the ratio of the power consumption at the legitimate MS to P and $I_{\mathsf{MS}}(i)$ is given by

$$I_{\mathsf{MS}}(i) = \begin{cases} 1, & \text{if } |h_{\mathsf{MS},i}|^2 > \zeta_{\mathsf{MS}} \\ 0, & \text{otherwise.} \end{cases}$$

[2]We do not explicitly consider the spatial distribution of both legitimate MSs and potential EVEs in this paper, but the physical distances from the BS to the legitimate MSs and potential EVEs can be regarded as implicitly reflected in the variances of wireless channel coefficients, λ_{MS} and λ_{E}.

TABLE II
COMPARISON WITH EXISTING SCHEMES

Ref	Networks	Type of EVEs	Strategies	CSI Req
[3] (Sec.IV)	DL	Passive	FF / FE	MS
[5]	DL	Potential	FF / FE	EVE, MS
[6] (Sec.IV)	UL	Potential	OF / FE	MS
[7] (Sec.III)	UL	Passive	FF / FE	MS
Proposed	DL	Potential	OF / RE	MS

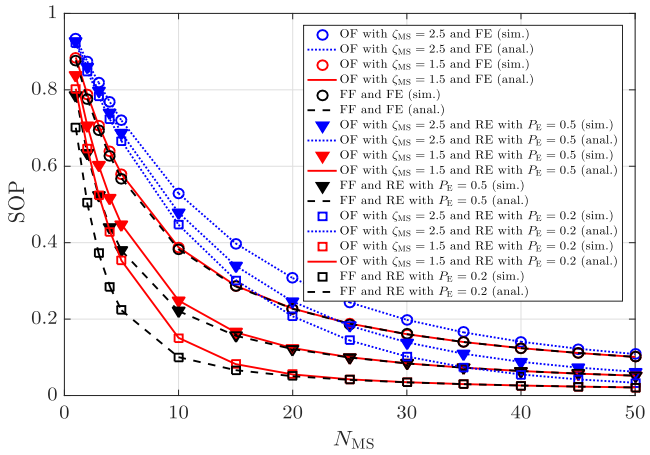

Fig. 2. SOP with respect to N_{MS}, when $\rho = 0$ [dB], $\zeta_{\mathsf{MS}} \in \{0, 1.5, 2.5\}$, and $P_{\mathsf{E}} \in \{0.2, 0.5, 1\}$.

D. Comparison

Table II summarizes the comparison of the proposed technique with existing schemes in terms of the network model, type of EVEs, feedback, and eavesdropping strategies, and CSI requirements at the BS. All existing schemes except for [6] do not consider OF at legitimate MSs, and thus all MSs feed their CSI values back to the BS. Furthermore, all existing schemes assume that all EVEs always attempt to overhear, i.e., the FE strategy. It is worth noting that the proposed technique requires the instantaneous CSI of only a few legitimate MSs not all MSs.

III. NUMERICAL RESULTS

This section evaluates the performance in terms of SOP when the OF and RE strategies are employed in our downlink wiretap network under various system parameters. In all simulations, we assume that $\lambda_{\mathsf{MS}} = 1$, $\lambda_{\mathsf{E}} = 2$, and $R_{\mathsf{o}} = 1$ [bps/Hz]. In addition, as noted in Section II-A, we assume the i.i.d. fading channels from the BS to the legitimate MSs and to the potential EVEs. Thus, in the OF and RE strategies, both $|\mathcal{M}_{MS}|$ and $|\mathcal{M}_{E}|$ become random variables following a binomial distribution with parameters P_{MS} and P_{E}, respectively. We use these two random variables in our simulations. In Figs. 2–4, we validate our analysis by showing that the derived SOP in (2) coincides the simulation results.

Fig. 2 illustrates the SOP for varying N_{MS} when $\rho = 0$ [dB], $\zeta_{\mathsf{MS}} \in \{0, 1.5, 2.5\}$, and $P_{\mathsf{E}} \in \{0.2, 0.5, 1\}$. Here, $\zeta_{\mathsf{MS}} = 0$ corresponds to the FF case where all legitimate MSs feed back their effective channel gains to the BS, while $P_{\mathsf{E}} = 1$ corresponds to the FE case where all EVEs always overhear the legitimate links. The FF strategy always outperforms the OF strategy in terms of SOP, since in the OF strategy some legitimate MSs do not participate in sending their channel gain in the OF strategy. Thus, there would be more legitimate MS candidates to be scheduled at the BS by the FF strategy. However, the performance gap between FF and OF strategies becomes negligible as the number of legitimate MSs increases due to widely studied the multiuser diversity gain, in various opportunistic communication scenarios. Moreover, it is observed that the SOP decreases as P_E decreases due to more intermittent information leakage at potential EVEs for given ζ_{MS}.

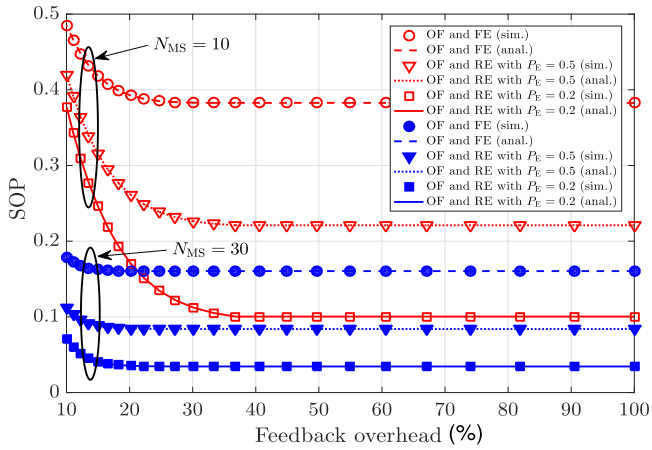

Fig. 3. SOP with respect to feedback overhead, when $\rho = 0$ [dB], $N_{\mathsf{MS}} \in \{10, 30\}$, and $P_{\mathsf{E}} \in \{0.2, 0.5, 1\}$.

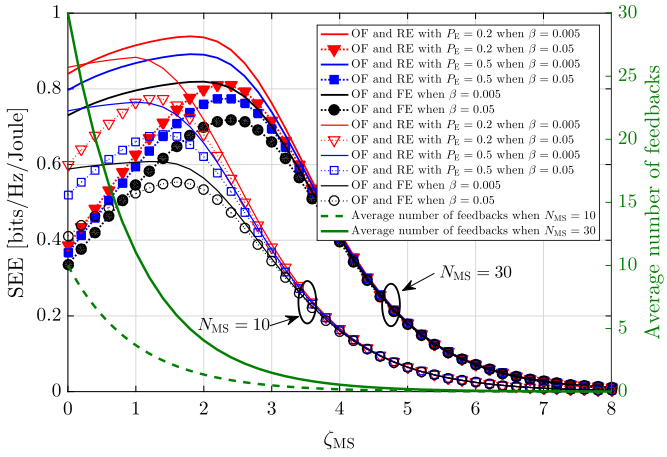

Fig. 4. SEE and the average number of MSs with feedback for varying the ζ_{MS} when $\rho = 0$ [dB], $N_{\mathsf{MS}} \in \{10, 30\}$, and $P_{\mathsf{E}} \in \{0.2, 0.5, 1\}$.

Fig. 3 illustrates the SOP versus feedback overhead for uplink when $\rho = 0$ [dB], $N_{\mathsf{MS}} \in \{10, 30\}$, and $P_{\mathsf{E}} \in \{0.2, 0.5, 1\}$. The feedback overhead is defined as $\mathbb{E}[|\mathcal{M}_{MS}|/N_{MS}] = P_{MS}$. As expected, as the feedback overhead increases, the SOP decreases for given N_{MS} and P_{E}, and approaches that SOP of the FF strategy. It is worth noting that the SOP of the OF strategy is almost identical to that of the FF strategy as long as the feedback overhead is larger than 40% and 20% when $N_{\mathsf{MS}} = 10$ and $N_{\mathsf{MS}} = 30$, respectively. The feedback overhead in the OF strategy required to maintain the SOP of the FF strategy becomes reduced as N_{MS} increases because of the effect of the multiuser diversity.

Fig. 4 illustrates the SEE and the average number of MSs with feeding their CSI values back according to the threshold ζ_{MS} when $\rho = 0$ [dB], $N_{\mathsf{MS}} \in \{10, 30\}$, and $P_{\mathsf{E}} \in \{0.2, 0.5, 1\}$. The proposed OF strategy improves the energy efficiency by suppressing the amount of feedback from legitimate MSs with small channel gain values, which enables us to establish a fundamental tradeoff between the SOP and SEE that can be observed by varying the values of ζ_{MS}. As shown in

Fig. 4, there exists the optimal feedback threshold ζ_{MS} to maximize the SEE for given system parameters. Note that the optimal SEE of the OF strategy is always larger than that of the FF strategy, i.e., $\zeta_{\mathsf{MS}} = 0$, for all system parameters.

IV. Conclusion

We analyzed the secrecy outage probability (SOP) of a multiuser downlink wiretap network with multiple potential eavesdroppers (EVEs) randomly attempting to overhear the data transmission with a certain probability, which is the first theoretical result in the literature to the best our knowledge and generalizes the conventional wiretap network settings. We employed the opportunistic feedback (OF) strategy at the legitimate MSs to reduce the signal overhead and improve SEE. It was demonstrated that our numerical results via computer simulations coincide with the analytical ones. It is desirable to set ζ_{MS} appropriately in order to achieve the same SOP as the FF case while reducing the feedback overhead and to maximize the SEE. We leave the SOP analysis for the case of colluding potential EVEs as a further study.

Appendix A
Proof of Theorem 1

When $|\mathcal{M}_{\mathsf{MS}}|$ legitimate MSs among N_{MS} feed their channel gain back to the BS and $|\mathcal{M}_{\mathsf{E}}|$ EVEs among N_{E} attempt to overhear, the secrecy nonoutage probability is given by

$$\begin{aligned}
&\Psi_{\mathsf{non}}^{\mathsf{OFRE}}(|\mathcal{M}_{\mathsf{MS}}|, \lambda_{\mathsf{MS}}, \zeta_{\mathsf{MS}}, |\mathcal{M}_{\mathsf{E}}|, \lambda_{\mathsf{E}}, \rho, R_{\mathsf{o}}) \\
&\quad = \mathsf{Pr}\Big(R_{\mathsf{s}}(|\mathcal{M}_{\mathsf{MS}}|, \lambda_{\mathsf{MS}}, \zeta_{\mathsf{MS}}, |\mathcal{M}_{\mathsf{E}}|, \lambda_{\mathsf{E}}, \rho) > R_{\mathsf{o}}\Big) \\
&\quad = \mathsf{Pr}\left(\begin{array}{c}\max_{m_{\mathsf{MS}}\in\mathcal{M}_{\mathsf{MS}}} \gamma_{\mathsf{MS},m_{\mathsf{MS}}} \\ > 2^{R_{\mathsf{o}}} \max_{m_{\mathsf{E}}\in\mathcal{M}_{\mathsf{E}}} \gamma_{\mathsf{E},m_{\mathsf{E}}} + \rho^{-1}(2^{R_{\mathsf{o}}}-1)\end{array}\right) \\
&\quad = \mathsf{Pr}\Big(X > 2^{R_{\mathsf{o}}} Y + \rho^{-1}(2^{R_{\mathsf{o}}}-1)\Big) \qquad (3)
\end{aligned}$$

where X and Y are random variables indicating $\max_{m_{\mathsf{MS}}\in\mathcal{M}_{\mathsf{MS}}} \gamma_{\mathsf{MS},m_{\mathsf{MS}}}$ for $|\mathcal{M}_{\mathsf{MS}}|$ legitimate MSs and the maximum channel gain $\max_{m_{\mathsf{E}}\in\mathcal{M}_{\mathsf{E}}} \gamma_{\mathsf{E},m_{\mathsf{E}}}$ for $|\mathcal{M}_{\mathsf{E}}|$ EVEs, respectively. Now, we are ready to establish the following theorem representing our main analytical result. The CDF and PDF of random variable X are given by

$$\begin{aligned}
F_X^{\mathsf{OF}}(x) &= \left(1 - e^{-\lambda_{\mathsf{MS}}(x-\zeta_{\mathsf{MS}})}\right)^{|\mathcal{M}_{\mathsf{MS}}|} \\
&= \sum_{m_{\mathsf{MS}}=0}^{|\mathcal{M}_{\mathsf{MS}}|} \binom{|\mathcal{M}_{\mathsf{MS}}|}{m_{\mathsf{MS}}} (-1)^{m_{\mathsf{MS}}} e^{-\lambda_{\mathsf{MS}} m_{\mathsf{MS}}(x-\zeta_{\mathsf{MS}})} \\
f_X^{\mathsf{OF}}(x) &= \lambda_{\mathsf{MS}}|\mathcal{M}_{\mathsf{MS}}| e^{-\lambda_{\mathsf{MS}}(x-\zeta_{\mathsf{MS}})} \left(1 - e^{-\lambda_{\mathsf{MS}}(x-\zeta_{\mathsf{MS}})}\right)^{|\mathcal{M}_{\mathsf{MS}}|-1} \\
&= \lambda_{\mathsf{MS}}|\mathcal{M}_{\mathsf{MS}}| \sum_{m_{\mathsf{MS}}=0}^{|\mathcal{M}_{\mathsf{MS}}|-1} \binom{|\mathcal{M}_{\mathsf{MS}}|-1}{m_{\mathsf{MS}}} (-1)^{m_{\mathsf{MS}}} e^{-\lambda_{\mathsf{MS}}(m_{\mathsf{MS}}+1)(x-\zeta_{\mathsf{MS}})}
\end{aligned}$$

respectively. Similarly, the CDF and PDF of random variable Y can be derived as

$$\begin{aligned}
F_Y^{\mathsf{RE}}(y) &= \sum_{m_{\mathsf{E}}=0}^{|\mathcal{M}_{\mathsf{E}}|} \binom{|\mathcal{M}_{\mathsf{E}}|}{m_{\mathsf{E}}} (-1)^{m_{\mathsf{E}}} e^{-\lambda_{\mathsf{E}} m_{\mathsf{E}} y} \\
f_Y^{\mathsf{RE}}(y) &= \lambda_{\mathsf{E}}|\mathcal{M}_{\mathsf{E}}| \sum_{m_{\mathsf{E}}=0}^{|\mathcal{M}_{\mathsf{E}}|-1} \binom{|\mathcal{M}_{\mathsf{E}}|-1}{m_{\mathsf{E}}} (-1)^{m_{\mathsf{E}}} e^{-\lambda_{\mathsf{E}}(m_{\mathsf{E}}+1) y}
\end{aligned}$$

respectively. Consequently, (3) can be rewritten as

$$\begin{aligned}
&\Psi_{\mathsf{non}}^{\mathsf{OFRE}}(|\mathcal{M}_{\mathsf{MS}}|, \lambda_{\mathsf{MS}}, \zeta_{\mathsf{MS}}, |\mathcal{M}_{\mathsf{E}}|, \lambda_{\mathsf{E}}, \rho, R_{\mathsf{o}}) \\
&\quad = \int_{\theta}^{\infty} \int_{0}^{2^{-R_{\mathsf{o}}} x + \rho^{-1}(2^{-R_{\mathsf{o}}}-1)} f_{XY}^{\mathsf{OFRE}}(x,y) dy dx \\
&\quad = \int_{\theta}^{\infty} f_X^{\mathsf{OF}}(x) \int_{0}^{2^{-R_{\mathsf{o}}} x + \rho^{-1}(2^{-R_{\mathsf{o}}}-1)} f_Y^{\mathsf{RE}}(y) dy dx \\
&\quad = \sum_{m_{\mathsf{MS}}=0}^{|\mathcal{M}_{\mathsf{MS}}|-1} \sum_{m_{\mathsf{E}}=0}^{|\mathcal{M}_{\mathsf{E}}|} \binom{|\mathcal{M}_{\mathsf{MS}}|-1}{m_{\mathsf{MS}}} \binom{|\mathcal{M}_{\mathsf{E}}|}{m_{\mathsf{E}}} \\
&\qquad \times (-1)^{m_{\mathsf{MS}}+m_{\mathsf{E}}} \lambda_{\mathsf{MS}}|\mathcal{M}_{\mathsf{MS}}| e^{\lambda_{\mathsf{MS}}(m_{\mathsf{MS}}+1)\zeta_{\mathsf{MS}}} \\
&\qquad \times \left[\frac{e^{-\lambda_{\mathsf{E}} m_{\mathsf{E}} \rho^{-1}(2^{-R_{\mathsf{o}}}-1)} e^{-(\lambda_{\mathsf{MS}}(m_{\mathsf{MS}}+1)+\lambda_{\mathsf{E}} m_{\mathsf{E}} 2^{-R_{\mathsf{o}}})\theta}}{\lambda_{\mathsf{MS}}(m_{\mathsf{MS}}+1) + \lambda_{\mathsf{E}} m_{\mathsf{E}} 2^{-R_{\mathsf{o}}}}\right. \\
&\qquad \left. - \frac{e^{-\lambda_{\mathsf{MS}}(m_{\mathsf{MS}}+1)\theta}}{\lambda_{\mathsf{MS}}(m_{\mathsf{MS}}+1)}\right] \qquad (4)
\end{aligned}$$

where $f_{XY}(x,y)$ indicates the joint PDF of random variables X and Y and the second equality holds since X and Y are independent. Here, θ represents

$$\theta = \begin{cases} \rho^{-1}(2^{R_o}-1), & \text{if } \zeta_{\mathsf{MS}} < \rho^{-1}(2^{R_{\mathsf{o}}}-1) \\ \zeta_{\mathsf{MS}}, & \text{otherwise.} \end{cases} \qquad (5)$$

In addition, when $|\mathcal{M}_{\mathsf{MS}}|$ legitimate MSs among N_{MS} are available and none EVE is active (i.e., $|\mathcal{M}_{\mathsf{E}}| = 0$), the secrecy nonoutage probability is given by

$$\begin{aligned}
&\Psi_{\mathsf{non}}^{\mathsf{OF}}(|\mathcal{M}_{\mathsf{MS}}|, \lambda_{\mathsf{MS}}, \zeta_{\mathsf{MS}}, \rho, R_{\mathsf{o}}) \\
&\quad = 1 - \int_{0}^{\theta} f_X^{\mathsf{OF}}(x) dx = 1 - \left(1 - e^{-\lambda_{\mathsf{MS}}(\theta-\zeta_{\mathsf{MS}})}\right)^{|\mathcal{M}_{\mathsf{MS}}|}. \qquad (6)
\end{aligned}$$

Therefore, $P_{\mathsf{outage}}^{\mathsf{OFRE}}(N_{\mathsf{MS}}, \lambda_{\mathsf{MS}}, \zeta_{\mathsf{MS}}, N_{\mathsf{E}}, \lambda_{\mathsf{E}}, P_{\mathsf{E}}, \rho, R_{\mathsf{o}})$ can be obtained by plugging (4), (5) and (6) into (2).

References

[1] Y.-S. Shiu *et al.*, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

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

[3] A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor, "On the resilience of wireless multiuser networks to passive and active eavesdroppers," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1850–1863, Sep. 2013.

[4] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[5] M. A. Abbas, H. Song, and J.-P. Hong, "Opportunistic scheduling for average secrecy rate enhancement in fading downlink channel with potential eavesdroppers," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 4, pp. 969–980, Apr. 2019.

[6] I. Bang and B. C. Jung, "Secrecy rate analysis of opportunistic user scheduling in uplink networks with potential eavesdroppers," *IEEE Access*, vol. 7, pp. 127 078–127 089, 2019.

[7] X. Ge, H. Jin, J. Zhu, J. Cheng, and V. C. M. Leung, "Exploiting opportunistic scheduling in uplink wiretap networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 4886–4897, Jun. 2017.

[8] J. Farhat *et al.*, "On the secure energy efficiency of TAS/MRC with relaying and jamming strategies," *IEEE Signal Process. Lett.*, vol. 24, no. 8, pp. 1228–1232, Aug. 2017.