Exploiting Impact of Eavesdropping Attacks on Secrecy Performance in WPT-based Secure Multi-hop Transmission

Kyusung Shim*, and Beongku An†
*School of Computer Engineering & Applied Mathematics, Hankyong National University, Republic of Korea
†Dept. of Software and Communications Engineering, Hongik University, Republic of Korea
Emails: *kyusung.shim@hknu.ac.kr, †beongku@hongik.ac.kr

***Abstract*—In this paper, we study the impact of various eavesdropping attacks on the secrecy performance in wireless power transfer (WPT)-based secure multi-hop transmission. Since each node has a limited power supply, each node harvests energy from the power beacon before data transmission. After then, each node fully consumes the harvested energy for data transmission. Meanwhile, according to the nature of the wireless medium, eavesdroppers can overhear the confidential message at each hop. In order to exploit the relationship between network parameters and secrecy performance, we derive the closed-form expression for secrecy outage probability (SOP) with different eavesdropping attacks, respectively. From the numerical results, we show that the Monte-Carlo simulation and analysis results are tightly matched. Additionally, we evaluate and discuss the impact of the power beacon's transmit power, the number of eavesdroppers, and time switching ratio on the secrecy performance.**

***Index Terms*—Eavesdropping attack, multi-hop transmission, physical layer security, wireless power transfer**

I. Introduction

The trend of future mobile networks is decentralization [1], [2]. Thus, each internet-of-things (IoT) device can connect and communicate without centralized nodes such as Wi-Fi and base station, which leads to the requirements of the end-to-end and multi-hop transmission [2]. However, these IoT devices are low cost, small size, and have limited power supply [3]. Thus, the node lifetime is a very big issue in future mobile networks. One of the possible solutions to extend node lifetime is wireless power transfer (WPT) that each node can harvest energy from other nodes [4], [5]. In detail, WPT can be divided into time switching-based relaying (TSR) and power splitting-based relaying (PSR). TSR architecture can harvest energy before data transmission. Thus, since TSR architecture can harvest energy for data transmission from power beacons, it can easily apply multi-hop transmission. But, it needs another kind of node, called a power beacon. Different from TSR architecture, PSR architecture can harvest energy from the received signal. Though it does not require another kind of node to supply energy, the SNR under PSR architecture degrades since each node decodes the message and harvests energy from the received signal at the same time.

According to the principle of the wireless medium, any node can overhear other users' transmission. If the malicious nodes receive an other user's message, they will abuse the wiretapped information. Thus, security is very important in the future mobile network. However, since the future mobile network is decentralized, it has some limitations to utilize encryption/decryption-based security. Thus, physical layer security (PLS) [6] is raised as one of the possible solutions to protect the message from the malicious node, named eavesdropper, by using the wild fluctuation in the wireless channel. As technology advances, the overhearing ability of eavesdroppers is also improved. Thus, the study of security in future mobile networks is required [7].

Indeed, authors in [8] proposed the node selection schemes to enhance the secrecy performance in WPT-based multi-hop transmission. However, this work did not consider the impact of eavesdropping attacks on the secrecy performance. The work in [9] exploited the optimal network design in multi-hop transmission. However, this work did not analyze the secrecy performance in the considered system model. Though this work in [10] studied active eavesdropping attacks in the advanced multiple access, it only focused on direct transmission. In [11], the authors addressed the route selection scheme to enhance the secrecy performance with WPT-based multi-hop transmission. However, this work did not study the impact of eavesdropping attacks on secrecy performance.

At the aforementioned works, the secrecy performance in various network models is studied. However, these works do not address the impact of the eavesdropping attack on the WPT-based secure multi-hop transmission. Thus, this work motivates us to study the eavesdropping attack impact on the secrecy performance in WPT-based secure multi-hop transmission. The main contribution of this paper can be summarized as follows:

- We exploit the secrecy performance on WPT-based secure multi-hop transmission. More specifically, the considered scenarios are that multiple eavesdroppers can share the eavesdropping information, called *colluding attack*, and multiple eavesdroppers work independently, called *non-colluding attack*, respectively.
- We derive the closed-form expression for secrecy outage probability (SOP) with different eavesdropping attacks, respectively. From the obtained closed-form expression for SOPs, we can capture the relationship between network parameters and secrecy performance.

- From the numerical results, we show that the colluding attack can intercept more information during multi-hop transmission compared to non-colluding attack. We investigate and discuss the impact of the power beacon's transmit power, the number of eavesdroppers, and time switching ratio.

The rest of this paper is organized as follows: Section II introduces the system and channel description under various eavesdropping attacks. Section III derives the exact closed-form expression for SOP with various wiretapping attacks, respectively. Section IV presents the illustrative numerical results and some insightful discussion. Finally, Section V concludes the paper.

II. System Model

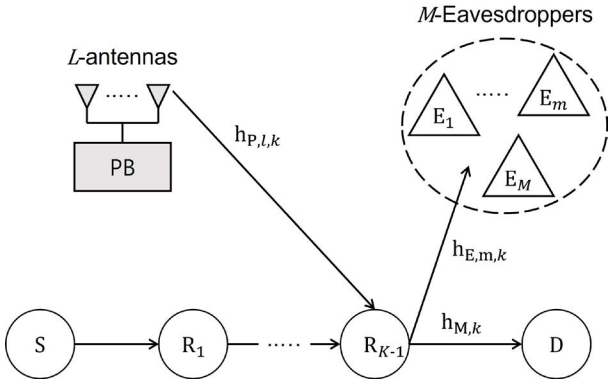

Fig. 1. The illustration of the WPT-based secure multi-hop transmission in the presence of multiple eavesdroppers

As can be seen in Fig. 1, we consider WPT-based secure multi-hop transmission under multiple eavesdroppers, where power beacon (PB) is equipped with L-antennas to transmit radio frequency signal for energy harvesting of each node. We assume that the direct link between a source node and a destination node can not be available since the limited radio range of each node, obstacle, or deep shadowing effect. Thus, $(K-1)$ nodes help data transmission from the source node to the destination node. Meanwhile, eavesdroppers can overhear the confidential message at each hop. Besides, we suppose that each node is operated in a half-duplex mode to transmit and receive signal since each node is equipped with a single antenna. All wireless links are assumed to undergo independently and identically distributed (i.i.d.) Rayleigh block flat fading.

Each node has a limited power supply; thus, they must harvest energy from the power beacons before data transmission and consume the harvested energy for data transmission. Consequently, the harvested energy during αT at k-th node can be expressed as

$$E_k = \eta \alpha T P_{\mathsf{P},l} \sum_{l=1}^{L} |h_{\mathsf{P},l,k}|^2, \tag{1}$$

where $\eta \in (0,1)$ means the energy conversion efficiency, $P_{\mathsf{P},l}$ represents the transmit power at l-th antenna. α represents the time splitting ratio with $0 < \alpha \leq 1$. $P_{\mathsf{P},l}$ is the transmit power level at l-th antenna at power beacon. $|h_{\mathsf{P},l,k}|^2$ indicates the channel gain from l-th antenna at power beacon to relay node at k-th hop transmission. In this paper, we can assume that the transmit power level is equal, i.e., $P_{\mathsf{P},l} = P_{\mathsf{P}}$, since the architecture of transmit antenna at the power beacon is same [8]. Additionally, each node has to consume the harvested energy for data transmission. Thus, the transmit power at k-th relay can be expressed as

$$P_k = \frac{E_k}{(1-\alpha)T/K} = \kappa P_{\mathsf{P}} \sum_{l=1}^{L} |h_{\mathsf{P},l,k}|^2, \tag{2}$$

where $\kappa = \frac{K\eta\alpha}{1-\alpha}$. Therefore, the received signal at (k+1)-th node can be expressed as

$$y_{\mathsf{M},k} = \sqrt{P_k} h_{\mathsf{M},k} x_{\mathsf{D}} + n_k, \tag{3}$$

where n_k indicates the additive white Gaussian noise with zero means and σ^2 variances. The instantaneous signal-to-noise ratio (SNR) can be formulated as

$$\gamma_{\mathsf{M},k} = \frac{P_k |h_{\mathsf{M},k}|^2}{\sigma^2} = \kappa \gamma_{\mathsf{P}} \sum_{l=1}^{L} |h_{\mathsf{P},l,k}|^2 |h_{\mathsf{M},k}|^2, \tag{4}$$

where $\gamma_{\mathsf{P}} = P_{\mathsf{P}}/\sigma^2$.

As can be seen in Fig. 1, when legitimate users transmit a message via radio frequency signal, eavesdroppers can overhear the confidential message. Since legitimate users adopt random-and-forward cooperative relaying protocol to protect the confidential message against eavesdropping attacks, eavesdroppers can not combine the overheard message at each hop. But, eavesdroppers can collaborate to enhance the secrecy performance. In this paper, we study the impact of eavesdropping scenarios on secrecy performance. The first scenario is that eavesdroppers can share the wiretapped message, called *colluding attack*. The second scenario is that eavesdroppers wiretap the message independently, named *non-colluding attack*.

A. Scenario 1: Colluding Attack

The overhear signal in k-th hop transmission under colluding attack can be expressed as

$$y^{\mathsf{s1}}_{\mathsf{E},m,k} = \sqrt{P_k} h^{\mathsf{s1}}_{\mathsf{E},k} x_{\mathsf{D}} + n_m, \tag{5}$$

where 's1' represents the colluding attack. The SNR in k-th hop transmission under colluding attack can be expressed as

$$\gamma^{\mathsf{s1}}_{\mathsf{E},k} = \frac{P_k}{\sigma^2} \sum_{m=1}^{M} |h_{\mathsf{E},m,k}|^2 = \kappa \gamma_{\mathsf{P}} \sum_{l=1}^{L} |h_{\mathsf{P},l,k}|^2 \sum_{m=1}^{M} |h_{\mathsf{E},m,k}|^2. \tag{6}$$

$$\Delta_1 = \left(\frac{1}{\lambda_{\mathsf{E},k}}\right)^M \frac{1}{\Gamma(M)} \int_0^\infty y^{M-1} e^{-\frac{1}{\lambda_{\mathsf{E},k}} y} dy - \left(\frac{1}{\lambda_{\mathsf{E},k}}\right)^M \frac{1}{\Gamma(M)} e^{-\frac{1}{\lambda_{\mathsf{M},k}}\left(\frac{\gamma_{\rm th}-1}{\kappa\gamma_{\mathsf{P}}}\frac{1}{z}\right)} \int_0^\infty y^{M-1} e^{-\left(\frac{1}{\lambda_{\mathsf{E},k}}+\frac{\gamma_{\rm th}}{\lambda_{\mathsf{M},k}}\right)y} dy. \quad (16)$$

$$\Delta = \left(\frac{1}{\lambda_{\mathsf{P},k}}\right)^L \frac{1}{\Gamma(L)} \int_0^\infty z^{L-1} e^{-\frac{1}{\lambda_{\mathsf{P},k}} z} dz - \left(\frac{1}{\lambda_{\mathsf{P},k}}\right)^L \left(\frac{1}{\lambda_{\mathsf{E},k}}\right)^M \frac{\beta}{\Gamma(L)} \int_0^\infty z^{L-1} e^{-\frac{\gamma_{\rm th}-1}{\kappa\gamma_{\mathsf{P}}\lambda_{\mathsf{M},k}}\frac{1}{z} - \frac{1}{\lambda_{\mathsf{P},k}} z} dz. \quad (18)$$

$$P_{\rm out}^{\mathsf{s1}} = 1 - \prod_{k=1}^{K} \left[\left(\frac{1}{\lambda_{\mathsf{P},k}}\right)^L \left(\frac{1}{\lambda_{\mathsf{E},k}}\right)^M \frac{2\beta}{\Gamma(L)} \left(\frac{(\gamma_{\rm th}-1)\lambda_{\mathsf{P},k}}{\kappa\gamma_{\mathsf{P}}\lambda_{\mathsf{M},k}}\right)^{L/2} K_L\left(2\sqrt{\frac{\gamma_{\rm th}-1}{\kappa\gamma_{\mathsf{P}}\lambda_{\mathsf{M},k}\lambda_{\mathsf{P},k}}}\right) \right], \quad (19)$$

B. Scenario 2: Non-colluding Attack

In the non-colluding attack, the overhear signal in k-th hop transmission can be expressed as

$$y_{\mathsf{E},m,k}^{\mathsf{s2}} = \sqrt{P_k} h_{\mathsf{E},k}^{\mathsf{s2}} x_{\mathsf{D}} + n_m, \quad (7)$$

where 's2' indicates the non-colluding attack. The SNR in k-th hop transmission under colluding attack can be expressed as

$$\begin{aligned} \gamma_{\mathsf{E},k}^{\mathsf{s2}} =& \frac{P_k}{\sigma^2} \max_{m\in M}\{|h_{\mathsf{E},m,k}|^2\} \\ =& \kappa\gamma_{\mathsf{P}} \sum_{l=1}^{L} |h_{\mathsf{P},l,k}|^2 \max_{m\in M}\{|h_{\mathsf{E},m,k}|^2\}. \end{aligned} \quad (8)$$

III. Secrecy Outage Performance Analysis

In this context, the secrecy outage probability (SOP) is one of performance measurement metrics, which can be defined as

$$P_{\rm out} = \Pr\left[\frac{1-\alpha}{K} \min_{k\in K}\left\{\log_2\left(\frac{1+\gamma_{\mathsf{M},k}}{1+\gamma_{\mathsf{E},k}}\right)\right\} < R_{\rm th}\right]. \quad (9)$$

After energy harvested phase, each node can transmit message using the harvested energy during K hop. Thus, the secrecy capacity is divided by $(1-\alpha)/K$. For the sake of simplicity, $X_k \triangleq |h_{\mathsf{M},k}|^2$, $Y_{1,k} \triangleq \sum_{m=1}^{M} |h_{\mathsf{E},m,k}|^2$, $Y_{2,k} \triangleq \max_{m\in M}\{|h_{\mathsf{E},m,k}|^2\}$, $Z_k \triangleq \sum_{l=1}^{L} |h_{\mathsf{P},l,k}|^2$ and $R_{\rm th}^{\mathsf{s1}} = R_{\rm th}^{\mathsf{s2}} = R_{\rm th}$. The following lemma will help to calculate the closed-form expression for SOP with the considered eavesdropper scenarios.

Lemma 1. *The CDF and PDF of Z_k can be expressed as*

$$F_{Z_k}(z) = 1 - \sum_{l=0}^{L-1} \frac{1}{l!}\left(\frac{z}{\lambda_{\mathsf{P},k}}\right)^l e^{-\frac{1}{\lambda_{\mathsf{P},k}} z}, \quad (10)$$

$$f_{Z_k}(z) = \left(\frac{1}{\lambda_{\mathsf{P},k}}\right)^L \frac{z^{L-1}}{\Gamma(L)} e^{-\frac{1}{\lambda_{\mathsf{P},k}} z}, \quad (11)$$

where $\Gamma(\cdot)$ represents the Gamma function [12].

Proof: See [13], [14]. ∎

A. Scenario 1: Colluding Attack

From (9), $P_{\rm out}^{\mathsf{s1}}$ can be further expressed as

$$P_{\rm out}^{\mathsf{s1}} = 1 - \prod_{k=1}^{K} \Big[1 - \underbrace{\Pr\left(\frac{1+\gamma_{\mathsf{M},k}}{1+\gamma_{\mathsf{E},k}^{\mathsf{s1}}} < \gamma_{\rm th}\right)}_{\triangleq\Delta} \Big], \quad (12)$$

where $\gamma_{\rm th} \triangleq 2^{\frac{KR_{\rm th}}{1-\alpha}}$. Δ in (12) can be re-written as

$$\begin{aligned} \Delta =& \Pr\left[X_k < \frac{\gamma_{\rm th}-1}{\kappa\gamma_{\mathsf{P}} Z_k} + \gamma_{\rm th} Y_{1,k}\right] \\ =& \int_0^\infty \underbrace{\int_0^\infty \left[1 - e^{-\frac{1}{\lambda_{\mathsf{M},k}}\left(\frac{\gamma_{\rm th}-1}{\kappa\gamma_{\mathsf{P}} z} + \gamma_{\rm th} y\right)}\right] f_{Y_{1,k}}(y) dy}_{\triangleq\Delta_1} f_{Z_k}(z) dz. \end{aligned} \quad (13)$$

The following lemma will help to calculate the closed-form expression for SOP under colluding attack.

Lemma 2. *The CDF and PDF of $Y_{1,k}$ can be expressed as*

$$F_{Y_{1,k}}(y) = 1 - \sum_{m=0}^{M-1} \frac{1}{m!}\left(\frac{y}{\lambda_{\mathsf{E},k}}\right)^m e^{-\frac{1}{\lambda_{\mathsf{E},k}} y}, \quad (14)$$

$$f_{Y_{1,k}}(y) = \left(\frac{1}{\lambda_{\mathsf{E},k}}\right)^M \frac{y^{M-1}}{\Gamma(M)} e^{-\frac{1}{\lambda_{\mathsf{E},k}} y}. \quad (15)$$

Proof: See [13], [14]. ∎

By plugging (15) into Δ_1 in (13), Δ_1 can be further expressed as (16). Relying on [12, eq. 3.381.4], (16) can be further formulated as

$$\Delta_1 = 1 - \beta\left(\frac{1}{\lambda_{\mathsf{E},k}}\right)^M e^{-\frac{\gamma_{\rm th}-1}{\kappa\gamma_{\mathsf{P}}\lambda_{\mathsf{M},k}}\frac{1}{z}}, \quad (17)$$

where $\beta = 1/(\frac{1}{\lambda_{\mathsf{E},k}} + \frac{\gamma_{\rm th}}{\lambda_{\mathsf{M},k}})^M$. By plugging (11) and (17) into (13), Δ can be re-written as (18). Again, by using [12, eq. 3.381.4] and [12, eq. 3.471.9] and some manipulation steps, the closed-form expression for SOP with colluding attack ($P_{\rm out}^{\mathsf{s1}}$) can be obtained as (19), where $K_\nu(\cdot)$ is the modified Bessel function of the second kind with order ν [12, Eq. 8.342.6].

$$\begin{aligned}\Phi_1 =&\frac{M}{\lambda_{\mathsf{E},k}}\sum_{m=0}^{M-1}\binom{M-1}{m}(-1)^m\int_0^\infty e^{-\frac{m+1}{\lambda_{\mathsf{E},k}}y}dy-\frac{M}{\lambda_{\mathsf{E},k}}\sum_{m=0}^{M-1}\binom{M-1}{m}(-1)^m e^{-\frac{\gamma_{\rm th}-1}{\kappa\gamma_{\mathsf{P}}\lambda_{\mathsf{M},k}}\frac{1}{z}}\int_0^\infty e^{-\left(\frac{\gamma_{\rm th}}{\lambda_{\mathsf{M},k}}+\frac{m+1}{\lambda_{\mathsf{E},k}}\right)y}dy\\ =&\sum_{m=0}^{M-1}\binom{M-1}{m}(-1)^m\frac{M}{m+1}-\sum_{m=0}^{M-1}\binom{M-1}{m}(-1)^m\frac{M\lambda_{\mathsf{M},k}}{(m+1)\lambda_{\mathsf{M},k}+\gamma_{\rm th}\lambda_{\mathsf{E},k}}e^{-\frac{\gamma_{\rm th}-1}{\kappa\gamma_{\mathsf{P}}\lambda_{\mathsf{M},k}}\frac{1}{z}}dy\end{aligned} \tag{25}$$

$$\begin{aligned}\Phi=&\sum_{m=0}^{M-1}\binom{M-1}{m}(-1)^m\frac{M}{m+1}\left(\frac{1}{\lambda_{\mathsf{P},k}}\right)^L\frac{1}{\Gamma(L)}\underbrace{\int_0^\infty z^{L-1}e^{-\frac{1}{\lambda_{\mathsf{P},k}}z}dz}_{\Phi_2}\\ &-\sum_{m=0}^{M-1}\binom{M-1}{m}(-1)^m\left(\frac{1}{\lambda_{\mathsf{P},k}}\right)^L\frac{M\lambda_{\mathsf{M},k}}{((m+1)\lambda_{\mathsf{M},k}+\gamma_{\rm th}\lambda_{\mathsf{E},k})\Gamma(L)}\underbrace{\int_0^\infty z^{L-1}e^{-\frac{\gamma_{\rm th}-1}{\kappa\gamma_{\mathsf{P}}\lambda_{\mathsf{M},k}}\frac{1}{z}-\frac{1}{\lambda_{\mathsf{P},k}}z}dz}_{\Phi_3}\end{aligned} \tag{26}$$

$$\begin{aligned}P_{\rm out}^{\mathsf{s2}}=1-\prod_{k=1}^{K}\Bigg[1-&\sum_{m=0}^{M-1}\binom{M-1}{m}(-1)^m\frac{M}{m+1}+\sum_{m=0}^{M-1}\binom{M-1}{m}(-1)^m\left(\frac{1}{\lambda_{\mathsf{P},k}}\right)^L\\ &\times\frac{2M\lambda_{\mathsf{M},k}}{((m+1)\lambda_{\mathsf{M},k}+\gamma_{\rm th}\lambda_{\mathsf{E},k})\Gamma(L)}\left(\frac{(\gamma_{\rm th}-1)\lambda_{\mathsf{P},k}}{\kappa\gamma_{\mathsf{P}}\lambda_{\mathsf{M},k}}\right)^{L/2}K_L\left(2\sqrt{\frac{\gamma_{\rm th}-1}{\kappa\gamma_{\mathsf{P}}\lambda_{\mathsf{M},k}\lambda_{\mathsf{P},k}}}\right)\Bigg]\end{aligned} \tag{29}$$

B. Scenario 2: Non-colluding Attack

Form (9), $P_{\rm out}^{\mathsf{S2}}$ can be further written as

$$P_{\rm out}^{\mathsf{s2}}=1-\prod_{k=1}^{K}\Bigg[1-\underbrace{\Pr\left(\frac{1+\gamma_{\mathsf{M},k}}{1+\gamma_{\mathsf{E},k}^{\mathsf{s2}}}<\gamma_{\rm th}\right)}_{\triangleq\Phi}\Bigg]. \tag{20}$$

Φ in (20) can be re-expressed as

$$\begin{aligned}\Phi=&\Pr\left[X_k<\frac{\gamma_{\rm th}-1}{\kappa\gamma_{\mathsf{B}}Z_k}+\gamma_{\rm th}Y_{2,k}\right]\\ =&\int_0^\infty\underbrace{\int_0^\infty\left[1-e^{-\frac{1}{\lambda_{\mathsf{M},k}}\left(\frac{\gamma_{\rm th}-1}{\kappa\gamma_{\mathsf{P}}z}+\gamma_{\rm th}y\right)}\right]f_{Y_{2,k}}(y)dy}_{\triangleq\Phi_1}f_{Z_k}(z)dz.\end{aligned} \tag{21}$$

The following lemma will help to further obtain the closed-form expression for SOP with non-colluding attack.

Lemma 3. *The CDF and PDF of $Y_{2,k}$ can be expressed as*

$$F_{Y_{2,k}}(y)=\sum_{m=0}^{M}\binom{M-1}{m}(-1)^m e^{-\frac{1}{\lambda_{\mathsf{E},k}}y}, \tag{22}$$

$$f_{Y_{2,k}}(y)=\frac{M}{\lambda_{\mathsf{E},k}}\sum_{m=0}^{M-1}\binom{M-1}{m}(-1)^m e^{-\frac{m+1}{\lambda_{\mathsf{E},k}}y}. \tag{23}$$

Proof: The CDF of $Y_{2,k}$ can be re-expressed as

$$\begin{aligned}F_{Y_{2,k}}(y)=&\Pr\left[\max_{m\in M}\{|h_{\mathsf{E},m,k}|^2\}<y\right]\\ =&\prod_{k=1}^{K}\Big[\Pr\left[|h_{\mathsf{E},m,k}|^2<y\right]\Big].\end{aligned} \tag{24}$$

By relying on binomial theorem, the CDF of $Y_{2,k}$ can be obtained as (22). After some algebraic manipulations, the PDF of $Y_{2,k}$ can be obtained as (23). The proof of Lemma 3 is concluded. ■

By substituting (23) into Φ_1 in (21) and using the fact [12, eq. 3.310], Φ_1 can be further obtained as (25). Again, by plugging (11) and (25) into Φ in (21), Φ can be re-expressed as (26). By relying on the fact [12, Eq. 3.381.4] and [12, Eq. 3.471.9], Φ_2 in (26) and Φ_3 in (26) can be further, respectively, calculated as

$$\Phi_2=\int_0^\infty z^{L-1}e^{-\frac{1}{\lambda_{\mathsf{P},k}}z}dz=\frac{1}{(1/\lambda_{\mathsf{P},k})^L}\Gamma(L), \tag{27}$$

$$\begin{aligned}\Phi_3=&\int_0^\infty z^{L-1}e^{-\frac{\gamma_{\rm th}-1}{\kappa\gamma_{\mathsf{P}}\lambda_{\mathsf{M},k}}\frac{1}{z}-\frac{1}{\lambda_{\mathsf{P},k}}z}dz\\ =&2\left(\frac{(\gamma_{\rm th}-1)\lambda_{\mathsf{P},k}}{\kappa\gamma_{\mathsf{P}}\lambda_{\mathsf{M},k}}\right)^{L/2}K_L\left(2\sqrt{\frac{\gamma_{\rm th}-1}{\kappa\gamma_{\mathsf{P}}\lambda_{\mathsf{P},k}\lambda_{\mathsf{M},k}}}\right).\end{aligned} \tag{28}$$

By plugging (27) and (28) into (26) and after some calculation steps, the closed-form expression for SOP with non-colluding attack can be obtained as (29).

IV. Performance Evaluations

In this section, we present representative numerical results to illustrate the achieved secrecy performance with various eavesdropping attacks. Unless otherwise stated, the simulation parameters can be summarized in Table I.

TABLE I
SIMULATION PARAMETERS

Parameters	**Value**
The distance between S and D, d_{SD}	10 m
The reference distance, d_0	1 m
The position of S	(0, 0)
The position of R_k	(k/K, 0)
The position of D	(10, 0)
The position of PB_m	(7.5 ,5.5)
The position of E	(-5 ,5)
The secrecy target data rate, R_{th}	0.1 bps/Hz
Pathloss exponent, β	2.7
Pathloss at reference distance, $\mathcal{L}$ at d_0	-30 dB
Energy conversion efficiency, η	0.7
Time switching ratio, α	0.15

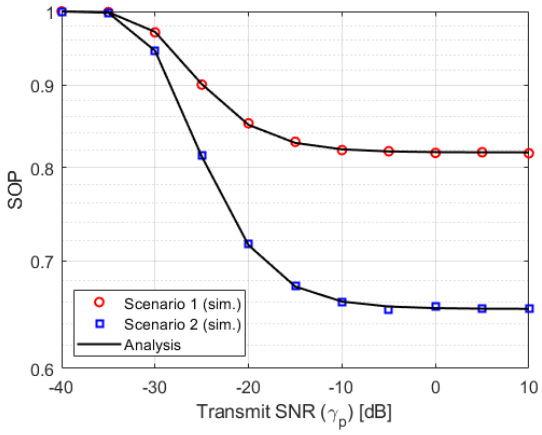

Fig. 2. The impact of transmit SNR (γ_{P}) on the SOP with L=5, K=4, M=3

Fig. 2 represents the impact of transmit SNR at power beacon (γ_{P}) on SOP with different eavesdropping attack. When γ_{P} increases, the SOP is decreased. Additionally, SOP reaches the performance floor at the high SNR region. From this phenomenon, we can know that the considered system model has secrecy performance threshold in the viewpoint of γ_{P}. Additionally, eavesdroppers with scenario 1, i.e.,*colluding attack*, can intercept more information than that with scenario 2. One of possible reasons is that the eavesdropper with scenario 1 can collect more information since eavesdropper are collaborated. Monte-Carlo simulation and analysis results are tightly matched.

The effect of the number of eavesdroppers on the SOP is represented as Fig. 3. As can be seen, the SOP increases when the number of eavesdroppers is increased. It means that the considered system is more vulnerable when the number of eavesdropper increases. Additionally, when the number of hop (K) increases, the SOP is decreased. It can be explained by

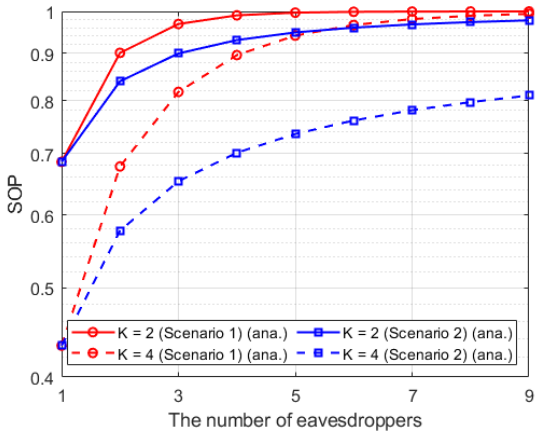

Fig. 3. The SOP versus the number of eavesdropper with L=5, γ_{P}=10dB

that the advantage of distance reducing is strongly affect on the secrecy performance compared to the impact of the number of hop. The secrecy performance gap between scenario 1 and scenario 2 increases when the number of hop is increased.

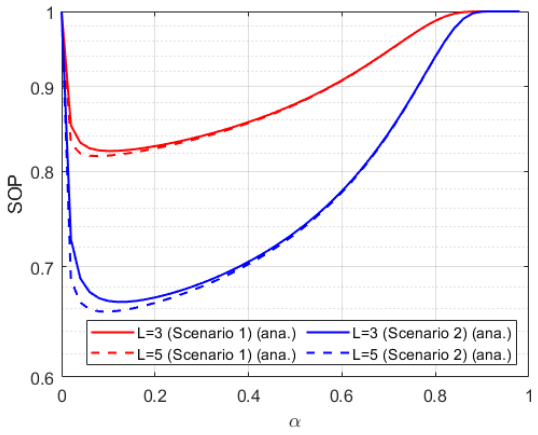

Fig. 4. The impact of α on the SOPs with K=4, M=3, and γ_{P}=-10dB

Now, we turn our attention to energy harvesting parameters on secrecy performance. As can be seen in Fig. 4, when time switching rate (α) increases, SOPs show convex pattern, respectively. Thus, the proper time switching ratio can minimize the SOP, which leads to the secrecy performance improvement. It can be explained by that, as can be seen in (19) and (29), α has a complicated impact on secrecy performance. Besides, when the number of power beacon's antennas increases, SOPs are decreased. From this result, the increased number of power beacon antennas affects on secrecy performance positively.

V. Conclusions

We exploited the impact of eavesdropping attack on secrecy performance in secure multi-hop transmission. In the first scenario, called colluding attack, eavesdroppers could collaborate to improve the overhearing ability. The non-colluding attack did not share the wiretapped information to hide their

existence. In order to find the relationship between network parameters and secrecy performance, we derived the closed-form expression for SOP with different eavesdropping attacks, respectively. From the performance evaluations, we evaluated and discussed the impact of the transmit power, the number of eavesdroppers and time switching ratio on the secrecy performance.

ACKNOWLEDGMENTS

This work was supported by a research grant from Hankyong National University in the year of 2023.

REFERENCES

[1] S. Chen, J. Zhang, Y. Jin, and B. Ai, "Wireless powered IoE for 6G: Massive access meets scalable cell-free massive MIMO," *China Communications*, vol. 17, no. 12, pp. 92–109, 2020.

[2] M. Noor-A-Rahim, Z. Liu, H. Lee, M. O. Khyam, J. He, D. Pesch, K. Moessner, W. Saad, and H. V. Poor, "6G for Vehicle-to-Everything (V2X) Communications: Enabling Technologies, Challenges, and Opportunities," *Proceedings of the IEEE*, vol. 110, no. 6, pp. 712–734, 2022.

[3] G. Pan, H. Lei, Y. Yuan, and Z. Ding, "Performance Analysis and Optimization for SWIPT Wireless Sensor Networks," *IEEE Transactions on Communications*, vol. 65, no. 5, pp. 2291–2302, 2017.

[4] X. Zhou, R. Zhang, and C. K. Ho, "Wireless Information and Power Transfer: Architecture Design and Rate-Energy Tradeoff," *IEEE Transactions on Communications*, vol. 61, no. 11, pp. 4754–4767, 2013.

[5] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying Protocols for Wireless Energy Harvesting and Information Processing," *IEEE Transactions on Wireless Communications*, vol. 12, no. 7, pp. 3622–3636, 2013.

[6] H. V. Poor and R. F. Schaefer, "Wireless Physical Layer Security," *Proc. National Academy of Sciences*, vol. 114, no. 1, pp. 19–26, 2017.

[7] T. M. Hoang, L. T. Dung, B. C. Nguyen, X. N. Tran, and T. Kim, "Secrecy Outage Performance of FD-NOMA Relay System with Multiple Non-Colluding Eavesdroppers," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 12, pp. 12 985–12 997, 2021.

[8] K. Shim, T.-V. Nguyen, and B. An, "Exploiting Opportunistic Scheduling Schemes and WPT-Based Multi-Hop Transmissions to Improve Physical Layer Security in Wireless Sensor Networks," *Sensors*, vol. 19, no. 24, p. 5456, Dec. 2019.

[9] J. Yao, X. Zhou, Y. Liu, and S. Feng, "Secure Transmission in Linear Multihop Relaying Networks," *IEEE Transactions on Wireless Communications*, vol. 17, no. 2, pp. 822–834, 2018.

[10] K. Shim, T. N. Do, T.-V. Nguyen, D. B. d. Costa, and B. An, "Enhancing PHY-Security of FD-Enabled NOMA Systems Using Jamming and User Selection: Performance Analysis and DNN Evaluation," *IEEE Internet of Things Journal*, vol. 8, no. 24, pp. 17 476–17 494, 2021.

[11] T. D. Hieu, T. T. Duy, and B.-S. Kim, "Performance Enhancement for Multihop Harvest-to-Transmit WSNs With Path-Selection Methods in Presence of Eavesdroppers and Hardware Noises," *IEEE Sensors Journal*, vol. 18, no. 12, pp. 5173–5186, 2018.

[12] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products (7th edition)*. Academic Press is an imprint of Elsevier, 2007.

[13] K. Shim, T.-V. Nguyen, and B. An, "Exploiting Opportunistic Scheduling Schemes to Improve Physical-Layer Security in MU-MISO NOMA Systems," *IEEE Access*, vol. 7, no. no, pp. 180 867–180 886, 2019.

[14] N. T. Van, T. N. Do, V. N. Q. Bao, and B. An, "Performance Analysis of Wireless Energy Harvesting Multihop Cluster-Based Networks Over Nakagami- m Fading Channels," *IEEE Access*, vol. 6, no. no, pp. 3068–3084, 2018.