EAI Endorsed Transactions
on Industrial Networks and Intelligent Systems

Research Article EAI.EU

On the Performance of the Relay Selection in Multi-hop Cluster-based Wireless Networks with Multiple Eavesdroppers Under Equally Correlated Rayleigh Fading

Pham Minh Nam[1], Ngo Dinh Phong[2,*], Nguyen Luong Nhat[2], Lam-Thanh Tu[3], Thuong Le-Tien [4]

[1]Faculty of Electronics Technology, Industrial University of HoChiMinh City, VietNam; phamminhnam@iuh.edu.vn
[2]Faculty of Electrical Engineering, Posts and Telecommunications Institute of Technology, Vietnam; phongnd@ptit.edu.vn, nhatnl@ptit.edu.vn
[3]Communication and Signal Processing Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam; tulamthanh@tdtu.edu.vn
[4]Ho Chi Minh City University of Technology, VNU-HCM, HoChiMinh city, Vietnam; thuongle@hcmut.edu.vn

Abstract

The performance of multi-hop cluster-based wireless networks under multiple eavesdroppers is investigated in the present work. More precisely, we derive the outage probability (OP) of the considered networks under two relay selection schemes: the channel-gain-based scheme and the random scheme. Although equally correlated Rayleigh fading is taken into consideration, the derived mathematical framework remains tractable. Specifically, we represent the exact expression of the OP under the channel-based scheme in series form, while the OP under the random scheme is computed in a closed-form expression. Additionally, we propose a novel power allocation for each transmitter that strictly satisfies the given intercept probability. Numerical results based on the Monte Carlo method are provided to verify the correctness of the derived framework. These results are also used to identify the influences of various parameters, such as the number of clusters, the number of relays per cluster, and the transmit power..

Received on 31 December 2023; accepted on 25 March 2024; published on 02 May 2024

Keywords: Eavesdroppers, Equally Correlated Rayleigh Fading, Multi-hop Wireless Networks, Power Allocation, Outage Probability

doi:10.4108/eetinis.v11i3.4728

1. Introduction

Multi-hop communication is one of the most effective ways to enhance spectral efficiency (S E) an d energy efficiency (EE). By shortening the transmission distance, one can improve reliability while reducing transmit power. Adopting the decode-and-forward (DF) protocol also helps eliminate the adverse effects of background noise [1, 2]. To further boost system performance, multi-hop cluster-based wireless networks can be considered, where several relay nodes are employed for each immediate hop instead of a single relay [3]. This approach significantly e nhances s ystem performance, especially in terms of reliability. However, multi-hop wireless networks are vulnerable to security risks, particularly when the eavesdropper receives multiple replicas of the source information in the case of adopting the DF protocol. This vulnerability makes multi-hop cluster-based wireless networks less attractive if the security problem is not adequately addressed. In

[*]Corresponding author: Ngo Dinh Phong
Email: ndphong@ptit.edu.vn

addition to security risks, the performance of multi-hop cluster-based wireless networks degrades severely in the presence of correlated fading. The main reason is that under correlated fading conditions, the diversity gain is no longer maximized, rendering an increase in the number of relays less beneficial. Although extreme networks of this nature have not yet been extensively explored in the literature, the present manuscript aims to investigate their performance.

Before delving into the main contributions and novelties of the manuscript, let us review relevant works in the literature. The performance of multi-hop networks and correlated fading has been extensively studied in several papers [4–24]. In particular, [4] investigated the reliability-security trade-off for harvest-to-jam multi-hop cluster-based multiple input multiple output (MIMO) networks. However, this study did not consider correlated fading or power allocation. In [5], Tin and co-authors addressed the reliability-security trade-off in non-orthogonal multiple access (NOMA)-based multi-hop relay networks, deriving outage probability (OP) and intercept probability (IP). Nevertheless, correlated fading was not taken into account. The use of Fountain codes (FCs) in multi-hop cooperative networks was explored in [6], focusing on OP under partial relay selection. In contrast, the present manuscript investigates channel-gain-based and random relay selection approaches. The power allocation in dual-hop NOMA networks was studied in [7], albeit under fixed power allocation and in NOMA networks. The relationship between reliability and security through OP and IP was revisited in [8]. Spectrum sharing and power allocation optimization were addressed in [9], but correlated fading was not considered. The performance of correlated fading in MIMO systems was explored in [11], with a focus on ergodic capacity, while the present work concentrates on OP. Finally, the study of oversampling correlation receivers in direct sequence code division multiple access (DS-CDMA) was conducted in [12]. Van *et al.* [13] investigated the performance of short packet multi-hop Internet of Things (IoT) networks, focusing on the derivation of the secrecy block error rate under both perfect and imperfect channel state information (CSI). In a related study, Lu et al. [14] explored the performance of multi-hop ad-hoc networks using reinforcement learning techniques. Tran *et al.* [15] addressed the secrecy performance with relay selection in the presence of co-channel interference. Miao and his colleagues focused on maximizing secrecy energy efficiency (SEE) in unmanned aerial vehicle (UAV)-assisted multi-hop relay systems [16]. Letafati *et al.*, on the other hand, studied the impact of three-hop untrusted relay networks with hardware impairments and channel estimation errors, deriving the lower bound of the average secrecy rate [17]. The authors in [18] examined physical layer security (PLS) versus covert communications in multi-hop UAV-aided scenarios, while [19] explored the security-reliability trade-off of multi-hop reconfigurable intelligent surfaces (RIS)-assisted Fountain codes. The secrecy performance of the multi-hop DF and cognitive radio networks were investigated in [20, 21]. The impact of friendly jamming in multi-hop LEACH networks was addressed in [22]. Additionally, Dang *et al.* [23] examined the outage probability and intercept probability in multi-hop cooperative jamming scenarios with FCs, while Tin *et al.* [24] analyzed the influence of the harvest-to-transmit protocol on secrecy performance.

While previous works have extensively examined secrecy performance in multi-hop wireless networks, they often overlook certain crucial factors such as receiver correlation and scenarios involving multiple eavesdroppers. Furthermore, the consideration of multi-hop cluster-based architectures remains largely unexplored. Addressing these gaps, this paper focuses on investigating the performance of multi-hop cluster-based wireless networks in the presence of multiple eavesdroppers, accounting for equal correlation Rayleigh fading. We provide Table 1 to highlight the main differences b etween t he p resent w ork a nd the state-of-the-art. The principal contributions and novelties of the manuscript are summarized below:

- We consider multi-hop cluster-based wireless networks with multiple eavesdroppers, adopting equally correlated Rayleigh fading for all transmissions.
- Two relay selection schemes, namely, channel gain-based and random selections, are explored in our analysis.
- We introduce a novel transmit power scheme at each transmitter that not only strictly satisfies the intercept probability threshold but also enhances the reliability of the considered networks.
- The exact framework of the outage probability is derived under the channel gain-based approach in an infinite series form, and the closed-form expression for the random selection scheme is provided.
- Numerous numerical results are presented to corroborate the accuracy of the derived framework and to gain insights into the performance of the networks.

The organization of the current paper is as follows: The system model is presented in Section 2, while the outage probability performance under two relay selection schemes is detailed in Section 3. Simulation results are discussed in Section 4. Finally, Section 5 concludes the manuscript.

Table 1. Comparison of the present works with state-of-the-art; TP = throughput, NZSP = non-zero secrecy probability, EC = ergodic capacity, SBLER = secrecy block-error rate, STP = secrecy throughput, SCP = secure connection probability, SOP = secrecy outage probability, SC = secrecy capacity, NZSC = non-zero secrecy capacity, SR = secrecy rate.

References	Multi-hop	Selection	Correlated fading	Multiple Eavesdroppers	Clusted-based	Metrics
This work	✓	Relay	✓	✓	✓	OP
[4]	✓	Antennas Jammers			✓	OP, IP
[5]	✓				✓	OP, IP, TP
[6]	✓					OP, IP
[8]		Relay				IP, NZSP
[9]	✓					EC
[10]						IP, OP
[13]	✓	Relay		✓	✓	SBLER, STP
[14]	✓			✓		SCP
[15]		Relay			✓	SOP, SC, NZSC
[16]	✓	UAV				SEE
[17]	✓					SR
[18]	✓					SR
[19]	✓					OP, IP
[20]	✓			✓		NZSC
[21]		Antennas				SOP, SC
[22]	✓	Relay			✓	SOP
[23]	✓	Relay			✓	OP, IP
[24]	✓	Antennas				SOP
[25]		Sources			✓	OP, IP

2. System model

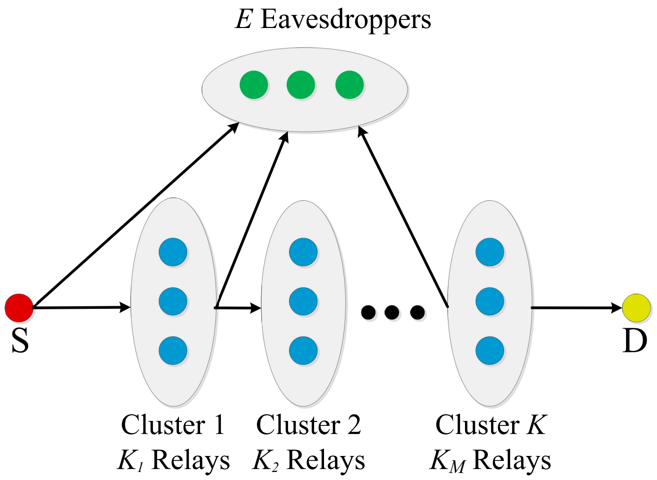

Figure 1. The considered multi-hop cluster-based wireless networks with multiple eavesdroppers.

Let us consider a multi-hop wireless network comprising a source node (S), a destination (D), and $K > 1$ immediate hops, as illustrated in Fig. 1. Additionally, there are $E > 1$ eavesdroppers attempting to wiretap secure information transmitted from S to D. For each middle hop, we assume there are $K_M \in \mathbb{N}$, available relays. It is further assumed that each node in the considered network is equipped with a single antenna, leaving the consideration of multi-antennas at the source, destination, relays, and/or eavesdroppers for future work.

2.1. Channel modeling

A generic transmission link from the transmitter to the receiver experiences both large-scale path-loss and small-scale fading. The effects of shadowing are not considered in the present work. The description of small-scale fading and large-scale path-loss is provided below.

Small scale fading. In contrast to prior works in the literature that assume uncorrelated fading between nodes in the cluster, our approach in this work considers equally correlated fading. This choice is motivated by the proximity of all relays to each other, which implies a high probability that they are not independent. More precisely, denoting $h_{m,n}$ as the channel coefficient from transmitter n at the k-th hop $k \in \{1, \ldots, K\}$ to receiver m at the $(k+1)$-th hop, it can be formulated as follows [26]:

$$h_{m,n} = \sqrt{1-\rho}X_{m,n} + \sqrt{\rho}X_n + j\left(\sqrt{1-\rho}Y_{m,n} + \sqrt{\rho}Y_n\right), \forall m \quad (1)$$

In (1), $X_{m,n}$, $Y_{m,n}$, X_n, and Y_n follow Gaussian distributions with zero mean and Ω variance. Upon direct inspection of (1), it is evident that all links from transmitter n are correlated due to the shared random variables X_n and Y_n. It is essential to highlight that the adopted equal-correlated fading channel is consid-ered the worst case compared to other correlated chan-nels, such as the distance-based approach [27]. Consequently, the system performance is affected accordingly. Moreover, the derived mathematical framework becomes more challenging as all variables share the same random variables. This necessitates the need for the joint probability density function (PDF) of all random variables to derive the system performance. Here, $\rho \in [0, 1]$ represents the correlation coefficient. When $\rho \to 1$, it indicates that all links experience the same fading, resulting in no spatial diversity gain from the cluster. Conversely, as $\rho \to 0$, a full degree of freedom is achieved from all relays in each cluster. Additionally, it is assumed that the fading changes independently between each transmission.

2.2. Large-scale path-loss

Let $H_{m,n}$ represent the large-scale path-loss from transmitter n to receiver m, formulated as follows [28]:

$$H_{m,n} = Z_0 \max\left\{1, d_{m,n}^{\delta}\right\}, \tag{2}$$

where Z_0 denotes the path-loss constant, computed based on the free-space path-loss model (FSPL) at 1 meter, i.e., $Z_0 = \left(\frac{4\pi f_c}{c}\right)^2$, where c [meters per second] is the speed of light, and f_c [Hz] is the carrier frequency. The variable $d_{m,n}$ represents the transmission distance from transmitter n to receiver m, and $\delta \geq 2$ is the path-loss exponent, dependent on the transmission environment. For instance, in urban areas, δ is generally greater than 3.5, whereas in rural areas, δ typically approaches 2. The term $\max\{.\}$ denotes the maximum function.

Remark 1. The adopted large-scale path-loss model addresses the singularity issue inherent in popular unbounded path-loss models. Specifically, as the transmission distance $d_{m,n} \to 0$, the value of $H_{m,n}$ approaches Z_0, ensuring that the received power converges to a constant value. In contrast, if an unbounded path-loss model were employed, the received power would approach infinity under the same conditions. Therefore, the employed model provides a more realistic representation, preventing the divergence of received power to infinity.

2.3. Received signals

The received signals at receiver m in cluster k, denoted by $y_{m,n}$, are defined as follows:

$$y_{m,n} = \sqrt{P_n H_{m,n}^{-1}} h_{m,n} x_n + \eta_m. \tag{3}$$

Here P_n represents the transmit power of transmitter n in cluster k, as provided in Lemma 1. The variable x_n denotes the transmit signals from transmitter n with unit power, i.e., $\mathbb{E}\left\{|x_n|^2\right\} = 1$ for all n and k. The expectation operator, $\mathbb{E}\{.\}$, is applied here. η_m represents the additive white Gaussian noise (AWGN) with a noise variance of $\sigma^2 = -174 + \mathrm{NF} + 10\log_{10}(\mathrm{BW})$ [dBm], where BW [Hz] is the transmission bandwidth, and NF [dB] is the noise figure of the receiver. Without loss of generality, it is assumed that all receivers have a similar noise figure, and the system employs a single signal transmission bandwidth.

Similarly, the received signals at the e-th eavesdropper, denoted by $y_{e,n}$, are formulated as follows:

$$y_{e,n} = \sqrt{P_n H_{e,n}^{-1}} h_{e,n} x_n + \eta_e, \tag{4}$$

where η_e represents the additive white Gaussian noise (AWGN) at the e-th eavesdropper. $H_{e,n}^{-1}$ and $h_{e,n}$ are the path-loss and channel coefficient from transmitter n to the e-th eavesdropper, respectively.

2.4. Signal-to-noise-ratio (SNR) at receivers

From (3) and (4), the signal-to-noise-ratios (SNRs) at the m receiver and e-th eavesdropper are given as [29]

$$\begin{aligned} \gamma_{m,n} &= \frac{P_n \left|h_{m,n}\right|^2}{\sigma^2 H_{m,n}}, \\ \gamma_{e,n} &= \frac{P_n \left|h_{e,n}\right|^2}{\sigma^2 H_{e,n}}. \end{aligned} \tag{5}$$

2.5. Relay selection scheme

In this paper, two relay selection schemes are considered, outlined as follows:

Channel-gain based method. The first relay selection scheme relies on the instantaneous channel gain among all available relays at each hop. Mathematically, the selected relay at the k-th hop, denoted by m^*, is chosen according to the following formula:

$$m^* \; : \; \max_{m \in \{1,\ldots,K_M\}} \left\{\left|h_{m,n}\right|^2\right\}. \tag{6}$$

Random-based method. The second relay selection scheme involves randomly selecting a relay from among all available relays.

2.6. Performance metrics

Outage probability. In this work, our focus is on the reliability aspect of the considered cluster-based multi-hop wireless networks. Specifically, we aim to study the OP, which quantifies the occurrence of outage events among all total transmissions. It is important to note that if any hop fails to decode the information, it is considered an outage for the entire transmission of that information. Mathematically, the OP at the destination is formulated as follows [30]:

$$\mathrm{OP} = \Pr\left\{ \min_{k\in\{1,\ldots,K+1\}} \left\{\gamma_{m^*,n}\right\} \le \gamma_{th} \right\}, \tag{7}$$

Here, $\gamma_{th} = 2^{(K+1)C_{th}} - 1$ represents the received signal-to-noise ratio threshold, which is a function of the quality-of-service (QoS) threshold, denoted as C_{th} [bit/s/Hz]. The factor $K+1$ in γ_{th} arises from the fact that the information from the source requires $K+1$ time slots to reach the destination. In the context of conventional wireless networks, K would be equal to 1.

3. Performance Analysis

In this section, we aim to derive the OP in closed-form expression. However, before delving into the OP analysis, we address the power allocation at the transmitter of each hop. Specifically, we propose a transmit power allocation scheme for the transmitters of each hop to ensure the security of the considered networks. The transmit power of all transmitters is given by the following lemma.

Lemma 1. Let P_n denote the transmit power of transmitter n at the k-th hop, computed as follows [31]:

$$\begin{aligned} P_n =& \min\left\{\max\left\{P_{com,n}, 0\right\}, P_{\max}\right\}, \forall n, k \\ P_{com,n} =& \frac{\sigma^2 H_{e,n} C_{th}}{\Omega}\left(\log\left(1-(1-\varphi)^{\frac{1}{E}}\right)\right)^{-1}, \end{aligned} \tag{8}$$

where φ is the intercept probability (IP) threshold, and $\min\{.\}$ and $\log\{.\}$ denote the minimum and logarithm functions, respectively.

Proof. The proof is available at the Appendix A. □

3.1. OP with channel-gain based approach

The OP under the channel-gain based approach is given by following equations [32]

$$\begin{aligned} \mathrm{OP}(\gamma_{th}) =& 1-(1-\mathrm{OP}_D(\gamma_{th}))\prod_{k=1}^{K}(1-\mathrm{OP}_k(\gamma_{th})) \\ \mathrm{OP}_k(\gamma_{th}) =& \sum_{l=0}^{\mathcal{O}} \Lambda_l(\gamma_{th})\, l! \left(\frac{1-\rho}{(K-1)\rho+1}\right)^{l+1} \\ \Lambda_l(\gamma_{th}) =& \sum_{o=1}^{l} \frac{oK-l+o}{l\tau_0(\gamma_{th})}\left(\frac{\rho}{1-\rho}\right)^{o} \frac{\Lambda_{l-o}(\gamma_{th})}{(o!)^2} \\ & \times \gamma\left(o+1, \frac{\gamma_{th}}{\overline{\gamma}(1-\rho)}\right), l \ge 1 \\ \Lambda_0(\gamma_{th}) =& (\tau_0(\gamma_{th}))^K \\ \tau_0(\gamma_{th}) =& 1-\exp\left(-\frac{\gamma_{th}}{\overline{\gamma}(1-\rho)}\right). \\ \mathrm{OP}_D(\gamma_{th}) =& 1-\exp\left(-\frac{\gamma_{th}}{\overline{\gamma}}\right) \end{aligned} \tag{9}$$

where $\gamma(.,.)$ is the lower incomplete Gamma function. $\overline{\gamma} = \frac{P_n}{\sigma^2 H_{m,n}}$ is the average signal-to-noise-ratio (ASNR) of the k-th hop.

Proof. The proof is available at Appendix B □

3.2. OP with random selection approach

The OP under the random selection scheme is computed as follows [33]:

$$\begin{aligned} \mathrm{OP}(\gamma_{th}) =& 1-\prod_{k=1}^{K+1}(1-\mathrm{OP}_k(\gamma_{th})) \\ \mathrm{OP}_k(\gamma_{th}) =& 1-\exp\left(-\frac{\gamma_{th}}{\overline{\gamma}}\right) \end{aligned} \tag{10}$$

Proof. The proof is available at Appendix C. □

Remark 2. Upon a direct examination of (10), it is apparent that the correlated fading has no impact on the random selection scheme. This is evident from the absence of the correlation coefficient ρ in the framework. Additionally, the equation reveals that the degree of freedom obtained from multiple relays at each hop is nullified in this scheme. Nevertheless, the positive contribution of multi-hop transmissions to the outage probability remains evident.

4. Numerical results

This section presents computer-based simulation results obtained through Monte-Carlo simulations to validate the accuracy of the derived mathematical framework. The numerical results are also utilized to reveal the impact of various key parameters on the performance of the outage probability. Without loss of generality, the following parameters are used throughout this section: $\rho = 0.9$, $C_{th} = 0.5$ bits/s/Hz, $K = 3$, $K_M = 3, 5, 4$, $E = 4$, $\mathcal{O} = 20$, $\delta = 3.5$, $f_c = 2.1$ GHz, BW = 500 KHz, NF = 6 dB, $P_{\max} = 40$ dBm, $P_{\min} = -10$ dBm, IP = 0.1. The source node and destination are located at coordinates [0,0] and [1000,0] m, respectively, while the eavesdroppers are positioned at [500,500]. All clusters are equally spaced along a straight line between the source and the destination.

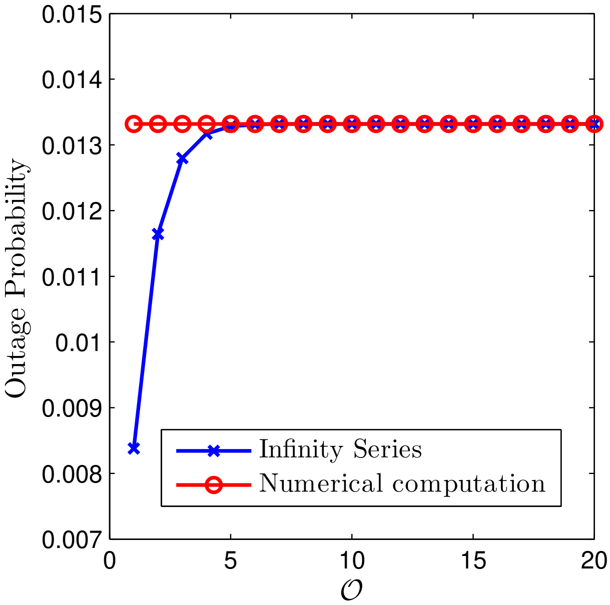

Figure 2. OP vs. O.

Figure 2 examines the accuracy and convergence of the infinite series in (9). The plot demonstrates that the infinite series in (9) converges rapidly to the numerical computations. Notably, only 10 terms are needed for the series to closely match the curve obtained through numerical methods.

Fig. 3 illustrates the relative error between the derived framework from (9) and numerical computation, maintaining consistency with the setup presented in Fig. 2. It is observed that the relative error decreases exponentially with $\mathcal{O}$. For instance, when $\mathcal{O} = 20$, the relative error is less than 10^{-10}, which is deemed sufficient for all contemporary applications and services. Consequently, $\mathcal{O} = 20$ is utilized throughout this section unless stated otherwise.

In Fig. 4, the transmit power of the source is plotted against the intercept probability. It is evident that increasing the IP scales up the transmit power of the source node. This observation indicates that a higher transmit power corresponds to a higher susceptibility to wiretapping, emphasizing the trade-off between system security and power consumption. Similar trends can be expected for other transmitters, though they are not explicitly presented in this figure. Additionally, the plot illustrates that a larger path-loss exponent results in

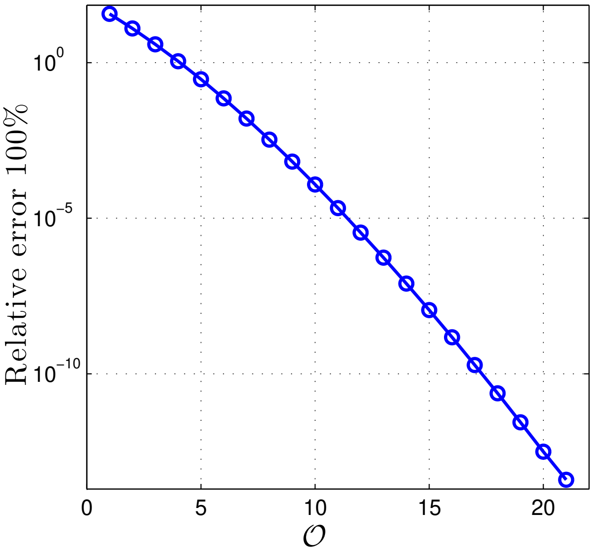

Figure 3. Relative error vs. $\mathcal{O}$ which is computed by $\frac{|X-\widetilde{X}|}{X} \times 100\%$ where X is attained by employing numerical computation and $\widetilde{X}$ is from (9).

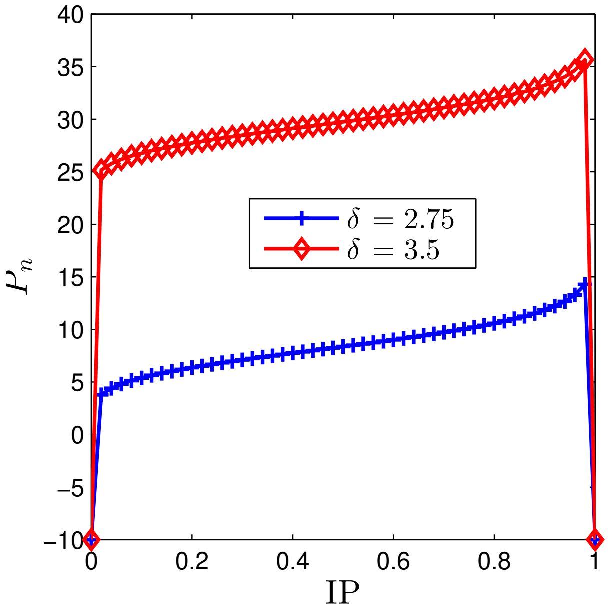

Figure 4. P_S vs. IP. The curves are plotted by (8).

higher transmit power. This phenomenon is intuitive, as a larger path-loss exponent implies quicker signal degradation, necessitating higher transmit power to compensate for the increased loss.

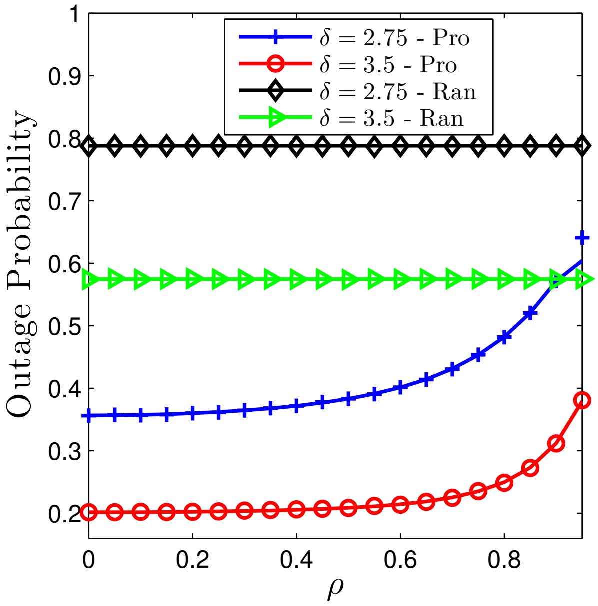

Figure 5. OP vs. ρ with several values of δ. Solid lines are plotted by (9), (10). Markers are from Monte Carlo simulations.

Fig. 5 illustrates the impact of the correlation coefficient ρ on the performance of the outage probability. Firstly, it is noted that the derived mathematical framework for both channel-gain-based and random selection schemes aligns well with Monte Carlo simulations. Secondly, the plot reveals that the outage probability increases with the correlation coefficient. This implies the absence of diversity gain as all antennas experience the same fading level. Additionally, higher path-loss exponents result in lower outage probabilities. It is noteworthy that the outage probability under the random selection scheme is independent of ρ, as indicated in (10). Fig. 5 further confirms the superiority of the proposed channel-gain-based scheme compared to the random selection scheme, regardless of the value of δ. Particularly, when $\rho = 0$ (indicating full diversity gain), the proposed scheme outperforms the random selection scheme, especially for $\delta = 3.5$ where the difference is more pronounced.

Figure 6 depicts the performance of the outage probability concerning the maximal transmit power $P_{\max}$. The plot clearly shows that increasing $P_{\max}$ is advantageous for the system, as the OP consistently decreases. However, it is important to note the existence of an OP floor due to the intercept probability constraint. This floor signifies that the system's performance improvement reaches a limit dictated by the IP constraint, and further increases in $P_{\max}$ do not lead to additional reductions in the OP.

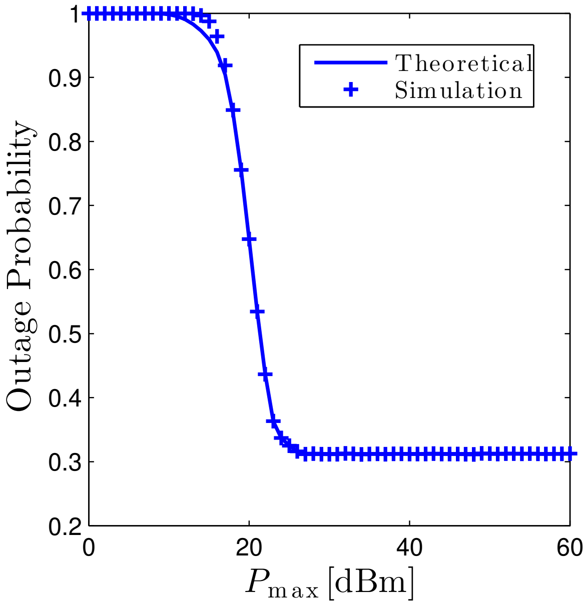

Figure 6. OP vs. $P_{\max}$.

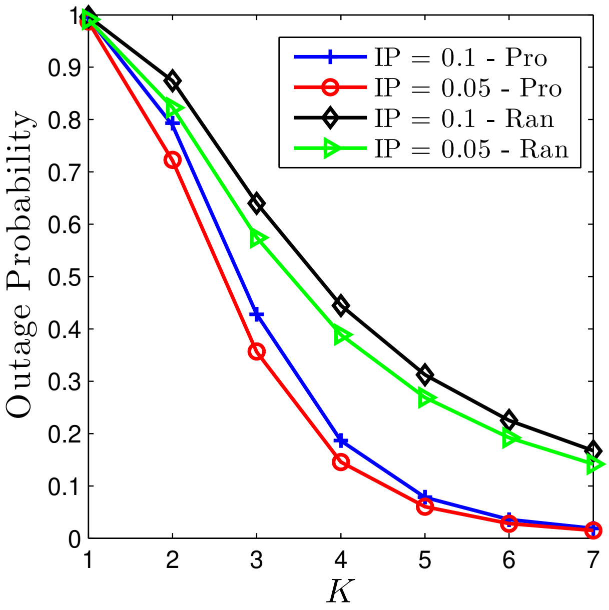

Figure 7. OP vs. K with several values of IP. Solid lines are plotted by (9), (10). Markers are from Monte Carlo simulations.

Fig. 7 provides insights into the influence of the number of clusters on the performance of the OP. Once again, there is a clear match between the derived mathematical framework and Monte Carlo simulations. Additionally, as mentioned earlier, increasing the number of hops is beneficial for the system, regardless of the adopted relay selection scheme. This observation is obvious, as an increase in the number of hops implies a reduction in transmission distance, thereby facilitating system performance. Moreover, from this figure, it is evident that higher IP result in higher outage probabilities. Lastly, the gap between the random scheme and the channel-based scheme initially increases and then decreases. This behavior can be explained by the fact that as the number of hops increases, the diversity gain diminishes since all transmissions are likely to succeed.

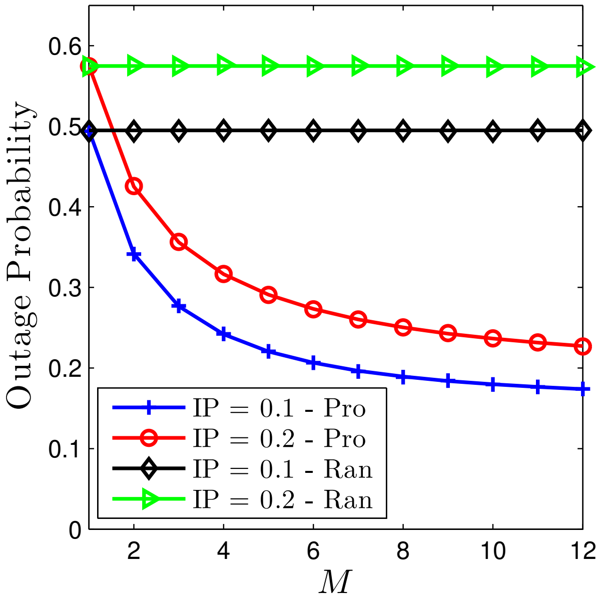

Figure 8. OP vs. M with different values of IP. Solid lines are plotted by (9), (10). Markers are from Monte Carlo simulations.

Fig. 8 investigates the impact of the number of relays per cluster. It is assumed that all clusters have the same number of relays, denoted as M. The curves plotted by the random scheme are constant with respect to M, as this scheme always selects a relay randomly, resulting in no cluster gain. In contrast, the channel-based scheme fully benefits from cluster gain, as improving M monotonically enhances the OP performance. However, the rate of improvement is nonlinear. Specifically, the OP initially experiences a sharp decline, followed by a more gradual decrease.

Figure 9 illustrates the relationship between the OP and the IP. The plot shows that increasing IP results in a reduction of the OP, and vice versa. This relationship underscores the trade-off between intercept probability and system reliability.

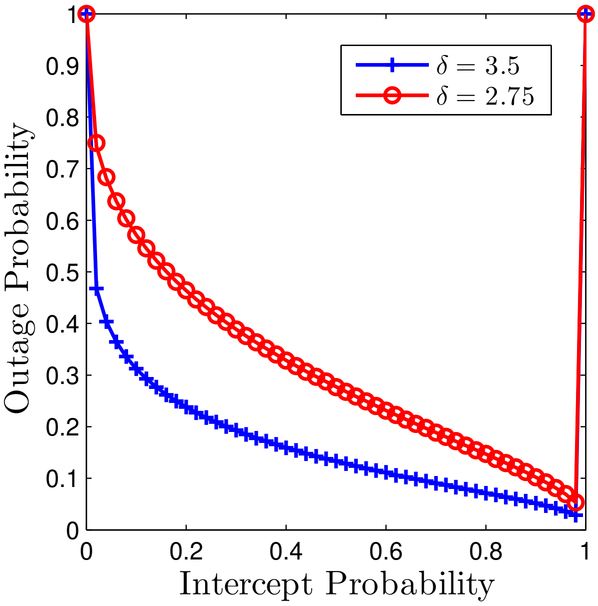

Figure 9. OP vs. IP with several values of δ. Solid lines are plotted by (9), (10). Markers are from Monte Carlo simulations.

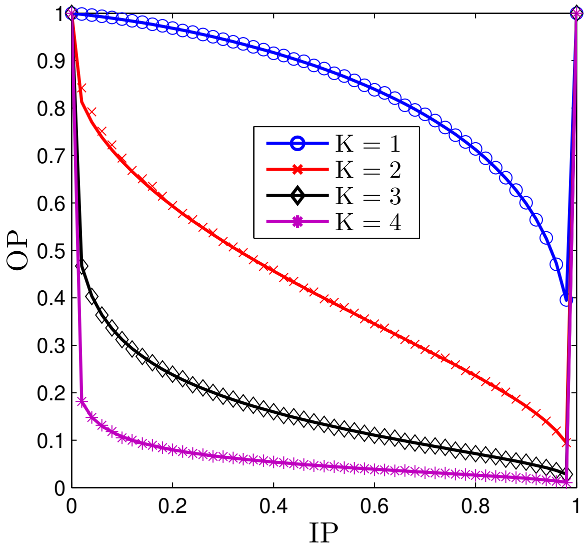

Figure 10. OP vs. IP with different values of K and $K_M = [3, 5, 4, 6]$. Solid lines are plotted by (9), (10). Markers are from Monte Carlo simulations.

Fig. 10 also investigates the security and reliability trade-off of the considered networks via OP vs. IP analysis. It is observed that increasing IP results in an improvement in OP, effectively reducing it. Conversely, enhancing IP comes at the cost of sacrificing OP, with OP approaching 1. However, this trade-off can be effectively mitigated by increasing the number of immediate hops, i.e., K. For instance, under the same IP constraint (i.e., IP $= 0.2$), if $K = 1$, the OP is approximately 0.96, whereas with $K = 4$, the OP is less than 0.08, a twelve-fold improvement. Additionally, escalating the number of immediate hops helps overcome the negative impact of equally correlated fading.

5. Conclusion

The present manuscript investigated the performance of multi-hop cluster-based wireless networks with equally correlated Rayleigh fading. Specifically, we studied the OP under two relay selection schemes: channel-gain based and random approaches. The exact framework for the channel-gain based scheme was derived, and closed-form expressions for the random scheme were provided. Additionally, we proposed a novel power allocation at each transmitter to strictly satisfy a given intercept probability. The results demonstrated the consistent superiority of the channel-based scheme over the random-based scheme. There are several potential avenues for extending this work. One possibility is to explore the use of passive devices, such as reconfigurable intelligent surfaces, in place of relays. Another avenue is to incorporate unmanned aerial vehicles to provide flexible support for transmissions from source to destination. Finally, the application of Fountain codes could be explored to enhance the spectral efficiency of the considered networks.

References

[1] Tran, Q.N., Vo, N.S., Nguyen, Q.A., Bui, M.P., Phan, T.M., Lam, V.V. and Masaracchia, A. (2021) D2d multi-hop multi-path communications in b5g networks: A survey on models, techniques, and applications. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems* **7**(25): 167839. doi:10.4108/eai.7-1-2021.167839, URL http://dx.doi.org/10.4108/eai.7-1-2021.167839.

[2] Tu, L.T., Phan, V.D., Nguyen, T.N., Tran, P.T., Duy, T.T., Nguyen, Q.S., Nguyen, N.T. *et al.* (2023) Performance analysis of multihop full-duplex NOMA systems with imperfect interference cancellation and near-field path-loss. *Sensors* **23**(1): 524. doi:10.3390/s23010524, URL https://doi.org/10.3390/s23010524.

[3] Duy, T.T. and Kong, H.Y. (2015) Secrecy performance analysis of multihop transmission protocols in cluster networks. *Wireless Personal Communications* **82**(4): 2505–2518. doi:10.1007/s11277-015-2361-y, URL http://dx.doi.org/10.1007/s11277-015-2361-y.

[4] Anh, N.T., Minh, N.C., Duy, T.T., Hanh, T. and Hai, H.D. (2021) Reliability-security analysis for harvest-to-jam based multi-hop cluster mimo networks using cooperative jamming methods under impact of hardware impairments. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems* **8**(28). doi:10.4108/eai.17-9-2021.170963.

[5] Phu, T.T., Dang, T.H., Tran, T.D. and Voznak, M. (2017) Security-reliability analysis of noma-based multi-hop relay networks in presence of an active eavesdropper with imperfect eavesdropping csi. *Advances in Electrical and Electronic Engineering* **15**(4). doi:10.15598/aeee.v15i4.2386, URL http://dx.doi.org/10.15598/aeee.v15i4.2386.

[6] Huan, N.T., Duy, T.T., Tu, L.T., Sang, N.Q., Ta, Q.H. and Tuan, P.V. (2022) Incremental cooperation based multi-hop relaying scheme with fountain codes, wirelessly energy harvesting and partial relay selection. In *2022 International Conference on Advanced Technologies for Communications (ATC)*: 338–343. doi:10.1109/ATC55345.2022.9943044.

[7] Thi Nguyen, T.T. and Do, D.T. (2021) Exploiting full-duplex and fixed power allocation approaches for dual-hop transmission in downlink noma. *Advances in Electrical and Electronic Engineering* **19**(3). doi:10.15598/aeee.v19i3.4116, URL http://dx.doi.org/10.15598/aeee.v19i3.4116.

[8] Vo, D.T., Van Chien, T., Nguyen, T.N., Tran, D.H., Voznak, M., Kim, B.S. and Tu, L.T. (2023) Swipt-enabled cooperative wireless iot networks with friendly jammer and eavesdropper: Outage and intercept probability analysis. *IEEE Access* **11**: 86165–86177. doi:10.1109/ACCESS.2023.3303369.

[9] Tran, Q.N., Vo, N.S., Bui, M.P., Phan, T.M., Nguyen, Q.A. and Duong, T.Q. (2022) Spectrum sharing and power allocation optimised multihop multipath d2d video delivery in beyond 5g networks. *IEEE Transactions on Cognitive Communications and Networking* **8**(2): 919–930. doi:10.1109/TCCN.2021.3133838.

[10] Nguyen, Q., Nguyen, V., Trung Duy, T., Nguyen, L. and Tu, L.T. (2023) On the security and reliability trade-off of the satellite terrestrial networks with fountain codes and friendly jamming. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems* **10**: e3. doi:10.4108/eetinis.v10i4.4192.

[11] Mahey, R. and Malhotra, J. (2015) Upper capacity bounds of mimo wireless systems through fading channels. *Advances in Electrical and Electronic Engineering* **13**. doi:10.15598/aeee.v13i5.1407.

[12] Quyen, N.X., Nguyen, N.P. and Vo, N.S. (2015) An oversampling-correlation receiver for enhancing performance of chaotic ds-cdma systems over flat fading channels. In *2015 International Conference on Communications, Management and Telecommunications (ComManTel)*: 157–161. doi:10.1109/ComManTel.2015.7394279.

[13] Nguyen, Toan-Van and Vu, Thai-Hoc and Huynh-The, Thien and da Costa, Daniel Benevides (2024) Secrecy performance of short-packet communications in multihop iot networks with imperfect csi. *IEEE Wireless Communications Letters* : 1–1doi:10.1109/LWC.2024.3361379.

[14] Lu, Jianzhong and He, Dongxuan and Wang, Zhaocheng (2022) Secure routing in multihop adhoc networks with srr-based reinforcement learning. *IEEE Wireless Communications Letters* **11**(2): 362–366. doi:10.1109/LWC.2021.3128582.

[15] Trung Duy, Tran and Duong, Trung and Tu, Lam-Thanh and Bao, Vo Nguyen (2015) Secrecy performance analysis with relay selection methods under impact of co-channel interference. *IET Communications* **9**: . doi:10.1049/iet-com.2014.1128.

[16] Miao, Jiansong and Li, Hairui and Zheng, Ziyuan and Wang, Chu (2021) Secrecy energy efficiency maximization for uav swarm assisted multi-hop relay system: Joint trajectory design and power control. *IEEE Access* **9**: 37784–37799. doi:10.1109/ACCESS.2021.3062895.

[17] Letafati, Mehdi and Kuhestani, Ali and Behroozi, Hamid (2020) Three-hop untrusted relay networks with hardware imperfections and channel estimation errors for internet of things. *IEEE Transactions on Information Forensics and Security* **15**: 2856–2868. doi:10.1109/TIFS.2020.2978627.

[18] Wang, Hui-Ming and Zhang, Yan and Zhang, Xu and Li, Zhetao (2020) Secrecy and covert communications against uav surveillance via multi-hop networks. *IEEE Transactions on Communications* **68**(1): 389–401. doi:10.1109/TCOMM.2019.2950940.

[19] Ty, Vo Ta and Duy, Tran Trung and Tu, Lam-Thanh and Nguyen, Tien-Tung and Trinh, D. and Hanh, Tan (2023) Security-reliability tradeoff of multi-hop secure communication networks using fountain codes and ris-aided cooperative communication. In *2023 International Conference on Advanced Technologies for Communications (ATC)*: 499–504. doi:10.1109/ATC58710.2023.10318517.

[20] Tran, Duc-Dung and Vo, Nguyen-Son and Vo, Tan-Loc and Ha, Dac-Binh (2015) Physical layer secrecy performance of multi-hop decode-and-forward relay networks with multiple eavesdroppers. In *2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops*: 430–435. doi:10.1109/WAINA.2015.33.

[21] Nam-Phong Nguyen and Tu, Lam-Thanh and Trung Q. Duong and A. Nallanathan (2017) Secure communications in cognitive underlay networks over nakagami-m channel. *Physical Communication* **25**: 610–618. doi:https://doi.org/10.1016/j.phycom.2016.05.003.

[22] Ha Duy Hung and Tran Trung Duy and Miroslav Voznak (2020) Secrecy outage performance of multi-hop leach networks using power beacon aided cooperative jamming with jammer selection methods. *AEU - International Journal of Electronics and Communications* **124**: 153357. doi:https://doi.org/10.1016/j.aeue.2020.153357, URL `https://www.sciencedirect.com/science/article/pii/S1434841120301898`.

[23] Dang The Hung and Tran Trung Duy and Do Quoc Trinh (2019) Security-reliability analysis of multi-hop leach protocol with fountain codes and cooperative jamming. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems* **6**(18). doi:10.4108/eai.28-3-2019.157120.

[24] Tin, Phu Tran and Minh Nam, Pham and Trung Duy, Tran and Tran, Phuong T. and Voznak, Miroslav (2019) Secrecy performance of tas/sc-based multihop harvest-to-transmit cognitive wsns under joint constraint of interference and hardware imperfection. *Sensors* **19**(5). doi:10.3390/s19051160, URL `https://www.mdpi.com/1424-8220/19/5/1160`.

[25] Tran, Minh and Tu, Lam-Thanh and Minh, Bui Vu and Nguyen, Quang-Sang and Rejfek, Lubos and Lee, Byung Moo (2024) Security and reliability analysis of the power splitting-based relaying in wireless sensors network. *Sensors* **24**(4). doi:10.3390/s24041300, URL `https://www.mdpi.com/1424-8220/24/4/1300`.

[26] Tu, L.T., Bao, V.N.Q., Ngoc, P.T.D. and Duy, T.T. (2016) On the performance of cognitive underlay SIMO networks over equally correlated rayleigh fading channels. *REV Journal on Electronics and Communications* **5**(1-2). doi:10.21553/rev-jec.96, URL `https://doi.org/10.21553/rev-jec.96`.

[27] Duong, T.Q., Alexandropoulos, G.C., Zepernick, H.J. and Tsiftsis, T.A. (2011) Orthogonal space–time block codes with csi-assisted amplify-and-forward relaying in correlated nakagami-m fading channels. *IEEE Transactions on Vehicular Technology* **60**(3): 882–889. doi:10.1109/TVT.2011.2104379.

[28] Di Renzo, M., Zappone, A., Tu, L.T. and Debbah, M. (2019) Spectral-energy efficiency pareto front in cellular networks: A stochastic geometry framework. *IEEE Wireless Communications Letters* **8**(2): 424–427. doi:10.1109/LWC.2018.2874642.

[29] Abedini, M. and Al-Anbagi, I. (2024) Enhanced active eavesdroppers detection system for multihop wsns in tactical iot applications. *IEEE Internet of Things Journal* **11**(4): 6748–6760. doi:10.1109/JIOT.2023.3313048.

[30] Nguyen, Tan N. and Tu, Lam-Thanh and Fazio, Peppino and Van Chien, Trinh and V. Le, Cuong and Binh, Huynh Thi Thanh and Voznak, Miroslav (2024) On the dilemma of reliability or security in unmanned aerial vehicle communications assisted by energy harvesting relaying. *IEEE Journal on Selected Areas in Communications* **42**(1): 52–67. doi:10.1109/JSAC.2023.3322756.

[31] Tu, L.T., Nguyen, T.N., Duy, T.T., Tran, P.T., Voznak, M. and Aravanis, A.I. (2022) Broadcasting in cognitive radio networks: A fountain codes approach. *IEEE Transactions on Vehicular Technology* **71**(10): 11289–11294. doi:10.1109/TVT.2022.3188969.

[32] Rostami Ghadi, F., López-Martínez, F.J., Zhu, W.P. and Gorce, J.M. (2022) The impact of side information on physical layer security under correlated fading channels. *IEEE Transactions on Information Forensics and Security* **17**: 3626–3636. doi:10.1109/TIFS.2022.3212198.

[33] Ghadi, F.R. and Hodtani, G.A. (2021) Copula-based analysis of physical layer security performances over correlated rayleigh fading channels. *IEEE Transactions on Information Forensics and Security* **16**: 431–440. doi:10.1109/TIFS.2020.3014553.

[34] Le, K. (2015) Comments on “distribution functions of selection combiner output in equally correlated rayleigh, rician, and nakagami-m fading channels”. *Communications, IEEE Transactions on* **63**: 5283–5287. doi:10.1109/TCOMM.2015.2495211.

Biographies

Appendix A. Proof of Lemma 1

We begin the proof with the definition of the IP at the eavesdropper as follows:

$$\begin{aligned}\mathrm{IP} &= \Pr\left(C_E = \frac{P_n \max\left\{\left|h_{e,n}\right|^2\right\}}{\sigma^2 H_{e,n}} \geq \gamma_{th}\right)\\ &= \Pr\left(C_E = \max\left\{\left|h_{e,n}\right|^2\right\} \geq \frac{\sigma^2\gamma_{th}}{P_n}\right)\\ &= 1 - \prod_{i=1}^{E}\left(1 - \exp\left(-\frac{\sigma^2\gamma_{th}}{P_n\Omega}\right)\right)\\ &= 1 - \left(1 - \exp\left(-\frac{\sigma^2\gamma_{th}}{P_n\Omega}\right)\right)^E \end{aligned} \qquad \text{(A.1)}$$

Having obtained the IP at the best eavesdropper, we derive the transmit power of the transmitter as follows:

$$\begin{aligned}&\mathrm{IP} \leq \varphi \Rightarrow 1 - \left(1 - \exp\left(-\frac{\sigma^2\gamma_{th}}{P_n\Omega}\right)\right)^E \leq \varphi\\ &\Rightarrow (1-\varphi)^{\frac{1}{E}} \leq 1 - \exp\left(-\frac{\sigma^2\gamma_{th}}{P_n\Omega}\right)\\ &\Rightarrow -\log\left(1-(1-\varphi)^{\frac{1}{E}}\right) \leq \frac{\sigma^2\gamma_{th}}{P_n\Omega}\\ &\Rightarrow P_{com,n} \leq \frac{\sigma^2\gamma_{th}}{\Omega}\left(\log\left(1-(1-\varphi)^{\frac{1}{E}}\right)\right)^{-1} \end{aligned} \qquad \text{(A.2)}$$

Next, we apply the hardware constraint of the transmitter we obtain (8).

Appendix B. Proof of (9)

Let us begin the proof with the definition of the OP as follows:

$$\mathrm{OP}\left(\gamma_{th}\right) = 1 - \left(1 - \mathrm{OP}_D\left(\gamma_{th}\right)\right)\prod_{k=1}^{K}\left(1 - \mathrm{OP}_k\left(\gamma_{th}\right)\right) \qquad \text{(B.3)}$$

where (B.3) is obtained owing to the property of the multi-hop wireless networks that the OP events appear if at least one hop fails to decode the information. It signifies that the end-to-end (e2e) SNR is constrained by the worst link. The derivation of the k-th link is derived as follows:

$$\begin{aligned}\mathrm{OP}_k\left(\gamma_{th}\right) &= \Pr\left\{\gamma_{m,n} = \frac{P_n \max\left\{\left|h_{m,n}\right|^2\right\}}{\sigma^2 H_{m,n}} \leq \gamma_{th}\right\}\\ &= \int_0^\infty F_{X_{\max}|U}\left(\frac{\sigma^2 H_{m,n}\gamma_{th}}{P_n}\right) f_U(u)\,du\\ &= \int_{u=0}^\infty \left(1 - Q\left(\sqrt{\frac{2\rho u}{(1-\rho)}}, \sqrt{\frac{2}{(1-\rho)}\frac{\sigma^2 H_{m,n}\gamma_{th}}{P_n}}\right)\right)^{K_M}\\ &\quad \times \exp(-u)\,du. \end{aligned} \qquad \text{(B.4)}$$

Here $Q(.)$ is the Marcum Q-function Eq. (B.4) can be attained with the help of [34] and is given below

$$\begin{aligned}\mathrm{OP}_k\left(\gamma_{th}\right) &= \sum_{l=0}^{\mathcal{O}} \Lambda_l\left(\gamma_{th}\right) l!\left(\frac{1-\rho}{(K-1)\rho+1}\right)^{l+1}\\ \Lambda_l\left(\gamma_{th}\right) &= \sum_{o=1}^{l} \frac{oK - l + o}{l\tau_0\left(\gamma_{th}\right)}\left(\frac{\rho}{1-\rho}\right)^o \frac{\Lambda_{l-o}\left(\gamma_{th}\right)}{(o!)^2}\\ &\quad \times \gamma\left(o+1, \frac{\gamma_{th}}{\overline{\gamma}(1-\rho)}\right), l \geq 1\\ \Lambda_0\left(\gamma_{th}\right) &= \left(\tau_0\left(\gamma_{th}\right)\right)^K\\ \tau_0\left(\gamma_{th}\right) &= 1 - \exp\left(-\frac{\gamma_{th}}{\overline{\gamma}(1-\rho)}\right). \end{aligned} \qquad \text{(B.5)}$$

Here $\overline{\gamma} = \frac{P_n}{\sigma^2 H_{m,n}}$. Finally, the $\mathrm{OP}_D\left(\gamma_{th}\right)$ is calculated as follows:

$$\mathrm{OP}_D\left(\gamma_{th}\right) = 1 - \exp\left(-\frac{\gamma_{th}}{\overline{\gamma}}\right) \qquad \text{(B.6)}$$

Eq. (B.6) is obtained by employing the cumulative distribution function (CDF) of the exponential distribution since the last hop only has a destination without relays and we close the proof here.

C. Proof of (10)

Let us begin the proof by rewriting the definition as follows

$$
\begin{aligned}
\mathrm{OP}_k\left(\gamma_{th}\right) =& \Pr\left\{\gamma_{m,n} = \frac{P_n\left|h_{m,n}\right|^2}{\sigma^2 H_{m,n}} \le \gamma_{th}\right\} \\
=& \int\limits_0^\infty F_{X|U}\left(\frac{\sigma^2 H_{m,n}\gamma_{th}}{P_n}\right) f_U\left(u\right) du \\
=& \int\limits_{u=0}^\infty \left(1 - Q\left(\sqrt{\frac{2\rho u}{(1-\rho)}}, \sqrt{\frac{2}{(1-\rho)\gamma}\frac{\sigma^2 H_{m,n}\gamma_{th}}{P_n}}\right)\right) \\
& \times \exp\left(-u\right) du \\
=& 1 - \int\limits_{u=0}^\infty Q\left(\sqrt{\frac{2\rho u}{(1-\rho)}}, \sqrt{\frac{2\gamma_{th}}{(1-\rho)\overline{\gamma}}}\right) \exp\left(-u\right) du \\
=& 1 - \left[\exp\left(-\frac{\gamma_{th}}{\overline{\gamma}}\right) + \exp\left(-\frac{\gamma_{th}}{(1-\rho)\overline{\gamma}}\right)\right. \\
& \left. - \exp\left(-\frac{\gamma_{th}}{\overline{\gamma}}\frac{1}{(1-\rho)}\right)\right] \\
=& 1 - \exp\left(-\frac{\gamma_{th}}{\overline{\gamma}}\right).
\end{aligned}
\tag{7}
$$

Having obtained $\mathrm{OP}_k\left(\gamma_{th}\right)$, we are going to derive $\mathrm{OP}_D\left(\gamma_{th}\right)$. It can be easily attained by borrowing the results in (B.6) and we terminate the proof here.