Wireless Networks (2021) 27:795–807
https://doi.org/10.1007/s11276-020-02487-w

Can a multi-hop link relying on untrusted amplify-and-forward relays render security?

Milad Tatar Mamaghani[1] · Ali Kuhestani[2,3] · Hamid Behroozi[2]

Accepted: 23 October 2020 / Published online: 6 November 2020

Abstract
Cooperative relaying is utilized as an efficient method for data communication in wireless sensor networks and the Internet of Things. However, sometimes due to the necessity of multi-hop relaying in such communication networks, it is challenging to guarantee the secrecy of cooperative transmissions when the relays may themselves be eavesdroppers, i.e., we may face with the untrusted relaying scenario where the relays are both necessary helpers and potential adversary. To obviate this issue, a new cooperative jamming scheme is proposed in this paper, in which the data can be confidentially communicated from the source to the destination through multiple untrusted relays. In our proposed secure transmission scheme, all the legitimate nodes contribute to providing secure communication by intelligently injecting artificial noises to the network in different communication phases. For the sake of analysis, we consider a multi-hop untrusted relaying network with two successive intermediate nodes, i.e, a three-hop communications network. Given this system model, a new closed-form expression is presented in the high signal-to-noise ratio (SNR) regime for the Ergodic secrecy rate (ESR). Furthermore, we evaluate the high-SNR slope and power offset of the ESR to gain an insightful comparison of the proposed secure transmission scheme and the state-of-arts. Our numerical results highlight that the proposed secure transmission scheme provides better secrecy rate performance compared with the two-hop untrusted relaying as well as the direct transmission schemes.

Keywords Physical layer security · Untrusted AF relaying · Multi-hop communication · Cooperative jamming

1 Introduction

The open broadcast nature of wireless media, though makes communications ubiquitously accessible as the world has witnessed in the past decades, leads the security requirement to be a paramount challenge of such communications systems [1]. Indeed, the flow of a large amount of data over wireless links that potentially may be sensitive in nature is more vulnerable than other transmission links to various security breaches such as location privacy [2] and eavesdropping attacks. Security in wireless communication networks is conventionally implemented above the physical layer using key-based cryptography methods [3]. However that these computationally-based security methods have worked well in conventional systems, they may not be applicable to the emerging fifth generation and beyond (B5G) wireless networks for the Internet of Things (IoT) which includes a broad range of applications such as unmanned aerial vehicle (UAV) networks, vehicular and

✉ Ali Kuhestani
kuhestani@sharif.edu

Milad Tatar Mamaghani
milad.tatarmamaghani@monash.edu

Hamid Behroozi
behroozi@sharif.edu

[1] Electrical and Computer Systems Engineering Department, Faculty of Engineering, Monash University, Melbourne, Australia

[2] Electrical Engineering Department, Sharif University of Technology, Tehran 11365-11155, Iran

[3] Communications and Electronics Department, Faculty of Electrical and Computer Engineering, Qom University of Technology, Qom 3716146611, Iran

ad-hoc networks (VANET), Internet of Vehicles (IoV), massive machine communication (MMC), and so forth [4]. As a matter of fact, these types of time-varying network topologies require complicated key management and sharing which is difficult to implement in distributed networks. Additionally, the computation and processing abilities of the nodes may be naturally limited and the complicated encryption calculations may not be supported [5].

To complement these complex schemes, wireless transmitters can also be validated at the physical layer by exploiting the dynamic characteristics of the associated communication links [6]. To accomplish this idea, physical layer security (PLS) has been emerged as a promising paradigm and an unbreakable security approach from the information-theoretic perspective, and provisioned for safeguarding 5G wireless communications networks against eavesdropping attacks without incurring additional security overhead [6, 7]. The fundamental notion of PLS is to intelligently exploit the characteristics of wireless channels and their impairments, eg., noise, fading, diversity, etc, and possibly the information source [8]. Indeed, the main design goal of PLS is to establish a performance gap between the link of the legitimate receiver, also known as *Main link* and that of the eavesdropper, or the so called *Wiretap link*, by using some well-designed secure transmission techniques (see, eg., [9] and references therein).

In the context of PLS, cooperative jamming, which involves the transmission of some artificial noise signals to degrade the quality of received signal-to-noise ratio (SNR) at the potential eavesdropper while maintaining that at the intended destination, has been contemplated a powerful security technique [3]. Further, cooperative jamming transmissions can be applied by any legitimate node of the network such as source [10], wherein some artificial noise is transmitted alongside the information signal, some dedicated authorized nodes [11, 12], wherein extra helper entities are employed for the jamming transmission, or even intended receivers, which is named as *destination-assisted jamming* technique [13–15]. Based on this technique, the decoding of the jammed signal by the authenticated user (destination) at some appropriate rate is possible, owing to the fact that the destination is able to receive quite a clean signal after self-interference cancellation, whereas the eavesdropper is kept unable to distinguish information-bearing signal from jamming transmitted by the destination.

Recently, the relay-assisted communications wherein low-cost intermediate nodes may be exploited to assist the source-to-destination transmission, has attracted the attention of many researchers. Indeed, relaying technology can assist in providing reliable communication between the long-distance users, and improve the spectral efficiency and coverage. Additionally, it has been viewed as a pervasive technology for the wireless sensor networks (WSN) and 5G IoT networks on the grounds that it can be adopted over a wide domain of applications such as smart homes, health-care services, device-to-device (D2D), IoV, and UAV communications [7, 13, 16–18]. For example, the authors in [13] explored the end-to-end communications between long-distance users via UAV-assisted relaying. The authors in [18] have considered a multi-hop scenario for a wireless sensor network and then applied a Genetic algorithm based optimization to enhance the energy expenditures, scalability, and lifetime of the WSN. Further, [19] presented a novel interference mitigation algorithm with low complexity to improve the throughput and the outage performances for Heterogeneous Networks (Het-Nets). The problem of designing the optimum beamforming vector for multiuser multiple-input and multiple-output (MU-MIMO) wireless communication system to minimize interference has also been investigated in [20] where the authors analyzed the Ergodic sum-rate capacity with Rician fading channels. However, it should be mentioned that the aforementioned research works have considered the end-to-end communications via trusted intermediate nodes, while the security issues of intermediate nodes have not been taken into account.

Nonetheless, several practical scenarios mentioned above may include *untrusted relay* nodes, i.e., the intermediate nodes which lack perfect security clearance, from which the source-destination pair wishes to keep the confidential information to be exchanged secret in spite of enlisting their help for the purpose of reliable communications [7, 21]. Hence, in these networks, it is important to protect the confidentiality of information from the untrustworthy relay, while simultaneously exploiting its relaying capability to improve the data transmission rate. In the area of untrusted relaying, an obvious yet thought-provoking question might initially arise is whether or not a chain of untrusted relays can be beneficial for the secure transmission of source-destination pair?

1.1 Related works

In the past decade, several works have considered the interesting scenario of untrusted relaying [22–30]. Thanks to the destination-based jamming strategy [22], it is shown that a positive secrecy rate can still be attained in untrusted relay networks. The authors in [26] proposed a joint relay selection and power allocation scheme for an untrusted relaying scenario in the presence of either non-colluding passive eavesdroppers or colluding ones. We note that non-colluding eavesdroppers independently try to obtain the confidential information without cooperating with each other. However, colluding eavesdroppers can potentially pose more harmful attacks by cooperatively attempting in decoding the confidential messages which are common in large-scale distributed networks [31]. Further, Mamaghani et al. by performing secrecy performance analyses, thoroughly investigated a two-way secure untrusted amplify-and-forward (AF) relaying in the presence of an extra jammer [15, 24, 25]. In their system model, the energy-limited intermediate nodes are powered via simultaneous wireless information and power transfer (SWIPT) technique to establish a self-reliant secure relaying network.

Notably, most of the recent works [23–26] have focused on the simple scenario of two-hop untrusted relaying. In some communication networks such as ad-hoc and IoT, it is of great interest to develop a communication network with more than two hops to provide the source-to-destination communication [28–30]. Note that the consecutive relays may be necessary helpers to deliver the information signal to the destination. This is particularly valid when the communications channels experience a heavy shadowing where the communication environment gets harsh, or when the distance between terminals is large, or even when the nodes suffer from limited power resources. Amongst the real-world communication systems that developing multiple relays might be crucial for message transmission are WSN, 5G IoT communications, and UAV-based relaying. For the latter application as an example, the wireless communication links may be easily blocked due to mountains and terrains in rural areas, or high-rise buildings in a metropolitan urban, which usually demands employing multiple UAV-relays to resolve the blockage or long-distance issues [27].

Having said that, extending the analysis from two-hop to multi-hop untrusted relaying networks is non-trivial because using more hops means that more nodes get involved in the transmission as well as more chances for eavesdropping. In addition, the number of hops becomes a design parameter that affects the end-to-end delay and throughput. Interestingly, He et al. in [30] demonstrated that a non-negative secrecy rate can be achieved for such a network by properly exploiting friendly jamming transmission from the appropriate nodes including both untrusted relays and destination. The main research question of that paper was whether an achievable non-vanishing perfect secrecy rate is attainable regardless of how many unauthenticated intermediate nodes are required for establishing source-destination communication? They showed that by employing an intelligent combination of some coding schemes, this goal could be achieved. It is worth pointing out that the untrusted relays considered in [30] adopt compute-and-forward (CF) protocol for data transmission. However, in 5G IoT wireless networks which devices are low-power with limited computational capability, the designers aim at implementing architectures with low computational complexity, eg., [32]. With that in mind, taking into account the CF relaying protocol, as investigated in [30], might become costly owing to the fact that each intermediate node needs to reliably retrieve the message from the received signal and then retransmit what decoded to the next subsequent node. Therefore, this relaying scheme may not be suitable for the computationally-limited intermediate nodes to be employed for end-to-end transmission protocol. As such, to the best of the authors' knowledge, the problem of low-complex untrusted relaying with more than two hops has not yet been extensively addressed.

1.2 Our contribution

In this paper, considering the need for multiple relays for reliable communications, differing from [23–26], and motivated by the solid work [30], we take into account secure transmission in a multi-hop AF untrusted relaying network. In the considered system model, a chain of intermediate nodes with low computational capabilities is necessary to facilitate end-to-end communications but a potential eavesdropper resides at each of them posing an eavesdropping attack. Note that in AF relaying, the intermediate nodes simply forward what they have received without attempting in decoding the information signal. Therefore, compared to CF relaying [30], AF relaying enjoys more simplex structure.

The main contributions of this research work are threefold summarized as:

1. We propose a new artificial noise injection based secure transmission protocol in a multi-hop *amplify-and-forward* untrusted relaying network to keep the communication confidential from the internal eavesdroppers for any number of hops.
2. We derive a novel closed-form expression for the ESR of three-hop untrusted relaying as a special case of multi-hop communications with two successive untrusted relays, at the high-SNR regime. Furthermore, we characterize the high-SNR slope corresponding to the maximum multiplexing gain of the network, and the high-SNR power offset metric to obtain an insightful comparison of the proposed secure transmission scheme and the other benchmarks.
3. We validate the theoretical analysis by comparing them with Monte–Carlo simulations, and demonstrate the significant secrecy performance improvement of the proposed cooperative jamming based multi-hop relaying over the conventional competitive benchmarks. We further study the impacts of some key system parameters such as nodes distance, environmental path-loss,

and transmission power on the overall system performance.

The rest of this paper is organized as follows. System model is given in Sect. 2, followed by detailing the proposed multi-hop transmission scheme with two relays and then deriving SNR representation at all the nodes in Sect. 3. Section 4 is dedicated for the secrecy performance analysis of the proposed secure protocol where we derive new closed-form expressions for the ESR, as well as analyze the asymptotic SNR metrics including the high-SNR slope and the high-SNR power offset. Next, numerical results and discussions are provided in Sect. 5 to illustrate the performance of the secure transmission scheme and obtain some key design insight into the proposed system model. Finally, conclusions are drawn in Sect. 6.

2 System model

We propose a secure communications system via multi-hop untrusted relaying, as illustrated in Fig. 1, where the source node, denoted by ($\mathcal{S}$), sends the information signal to the destination ($\mathcal{D}$) with the help of multiple consecutive relays, denoted by $\mathcal{R}_i$ where $i = 1, 2, \ldots N$. We assume all the involving nodes are equipped with a single antenna operating in half-duplex mode, i.e., sending and receiving can not be done concurrently. In the so-called line network, it is also assumed that each node $\mathcal{R}_i$ can communicate with its two neighbors $\mathcal{R}_{i-1}$ and $\mathcal{R}_{i+1}$ on the grounds that the channel quality between non-consecutive nodes is too weak to establish communications. Further, the AF relaying architecture is assumed operating at the relays where the relay simply forwards what they have received and so is very inexpensive to implement. Besides that, the intermediate nodes are assumed to be untrustworthy and hence, they would overhear the transmitted information signal while relaying. Moreover, we assume that the relays are non-colluding, as for the line network taken into account it is less likely that non-consecutive intermediate illegitimate nodes could share their information and collude with each other due to the channel conditions of these nodes. To be specific, it is assumed that the untrusted relays, at which the eavesdroppers residing, adopt selection combining (SC) processing technique to extract the information solely based on their own findings similar to [23, 26]. Additionally, the channel between any two consecutive nodes is assumed to follow channel reciprocity obeying complex Gaussian distribution.[1]

Now, we turn our focus to the proposed secure transmission protocol and provide a detailed explanation with analysis for the considered system model when the number of relays is two, i.e., three-hop untrusted relaying, and then discuss the system performance for the higher number of relays, from engineering perspectives.

3 Transmission protocol

The proposed multi-hop secure untrusted relaying with two relays, i.e., $\mathcal{R}_1$ and $\mathcal{R}_2$, can be detailed as follows. Considering a time division multiple access (TDMA) scheme, wherein the communication link is divided into separate time slots while sharing the same frequency band, one frame of transmission from $\mathcal{S}$ to $\mathcal{D}$ takes place in three phases, lasting $\frac{T}{3}$ seconds each, as shown in Fig. 2. At the outset, during the first phase of communication, $\mathcal{S}$ transmits the information signal to $\mathcal{R}_1$ using superposition coding, and simultaneously, $\mathcal{R}_2$ jams the first untrusted relay ($\mathcal{R}_1$) by transmitting an artificial noise. During the next phase, $\mathcal{R}_1$ forwards a scaled version of the received signal towards $\mathcal{R}_2$. Concurrently, $\mathcal{D}$ jams $\mathcal{R}_2$ via transmitting a jamming signal to guarantee secrecy. Finally, in the third phase, $\mathcal{R}_2$ amplifies and broadcasts the received signal which can be further received by $\mathcal{D}$ and $\mathcal{R}_1$. After self-interface cancellation at $\mathcal{D}$, the information signal can be extracted at $\mathcal{D}$. Notably, during the last time slot, since $\mathcal{R}_1$ can overhear the broadcasted signal by $\mathcal{R}_2$, the node $\mathcal{S}$ is forced to emit jamming to enhance the confidentiality of communication. As such, $\mathcal{R}_1$ may fail to successfully eavesdrop during the last phase, as well. Note that depending on the level of security required, $\mathcal{S}$ might be idle in the last phase, and therefore, an appropriate power allocation scheme plays an important role in the proposed cooperative jamming based untrusted relaying.

Now, let assume that the complex Gaussian channel gains from $\mathcal{S}$ to $\mathcal{R}_1$ $\mathcal{R}_1$ to $\mathcal{R}_2$, and $\mathcal{R}_2$ to $\mathcal{D}$ are denoted by $g \sim \mathcal{CN}(0, m_g)$, $h \sim \mathcal{CN}(0, m_h)$ and $f \sim \mathcal{CN}(0, m_f)$, respectively. We here consider block fading channel model such that the channel coefficients vary independently from one frame to another frame, but do not change within one frame. To make the analysis tractable, we consider the equal transmit power P by the nodes, i.e., $P_s = P_{r_1} = P_{r_2} = P_d = P$. We also define $\gamma_g \overset{\Delta}{=} \rho|g|^2$, $\gamma_h \overset{\Delta}{=} \rho|h|^2$, and $\gamma_f \overset{\Delta}{=} \rho|f|^2$, where $\rho = \frac{P}{N_0}$ describes the transmit SNR per each node. Remarkably γ_g, γ_h and γ_f follow exponential distributions with means $\bar{\gamma_g} = \rho m_g$, $\bar{\gamma_h} = \rho m_h$, and $\bar{\gamma_f} = \rho m_f$, respectively. Without loss of generality, the power of additive white Gaussian noise (AWGN) at each receiver is considered to be N_0. We also suppose that the

[1] Note that this is a valid assumption for terrestrial networks, however, our work can be readily extended to consider other channel modeling based on the applications of interest, such as UAV-ground based channels as considered in [13].

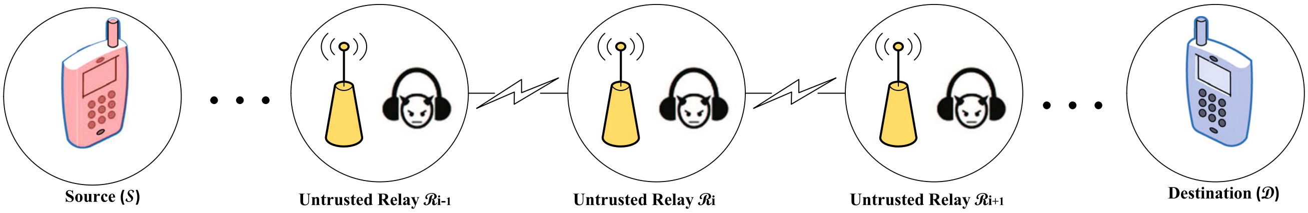

Source ($\mathcal{S}$)
Untrusted Relay $\mathcal{R}_{i-1}$
Untrusted Relay $\mathcal{R}_i$
Untrusted Relay $\mathcal{R}_{i+1}$
Destination ($\mathcal{D}$)

Fig. 1 System model of secure multi-hop untrusted relaying

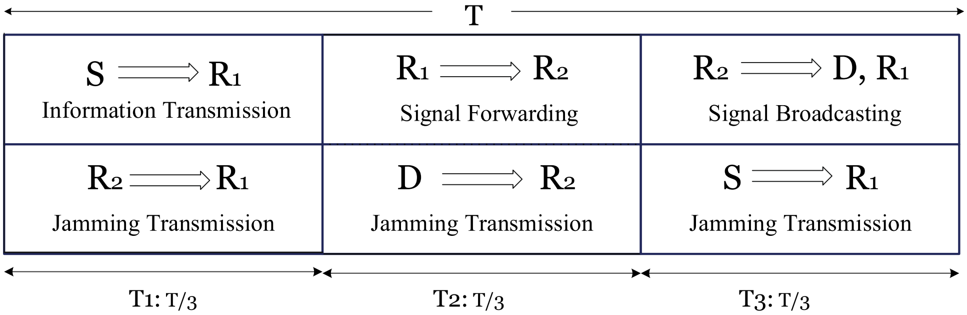


Fig. 2 Secure transmission protocol of three-hop untrusted relaying

nodes are aware from the necessary channel state information (CSI), by which the relays as well as the destination can thoroughly cancel the self-interference term from the received signal. Note that this assumption leads to the maximum probability of eavesdropping at the relays, and in some sense, can be considered as the worst case scenario.

Based on the above descriptions and after some mass manipulations, the exact signal-to-interference-plus-noise-ratios (SINRs) at $\mathcal{R}_1$ in the first phase, at $\mathcal{R}_2$ in the second phase, at $\mathcal{R}_1$ and $\mathcal{D}$ in the third phase, are respectively, obtained as

$$\gamma_{R_1}^{(1)} = \frac{\gamma_g}{\gamma_h + 1}, \tag{1}$$

$$\gamma_{R_2}^{(2)} = \frac{\gamma_g \gamma_h}{\gamma_g} \gamma_f + \gamma_h \gamma_f + 2\gamma_h + \gamma_g + \gamma_f + 1, \tag{2}$$

$$\gamma_{R_1}^{(3)} = \frac{\gamma_g {\gamma_h}^2}{\gamma_h^2} + \gamma_h(\gamma_g + 1)^2 + (\gamma_g + \gamma_h + 1)^2(\gamma_f + 1), \tag{3}$$

$$\gamma_{D}^{(3)} = \frac{\gamma_g \gamma_h \gamma_f}{3} \gamma_h \gamma_f + 2\gamma_f \gamma_g + \gamma_g \gamma_h + 2\gamma_f + 2\gamma_h + \gamma_g + 1, \tag{4}$$

where superscripts represent the phase of transmission. Under the high-SNR regime with $\gamma_k \gg 1$ for $k \in \{g, h, f\}$, the above exact SINRs derived can be respectively, simplified as

$$\gamma_{R_1}^{(1)} \approx \frac{\gamma_g}{\gamma_h}, \gamma^{(2)})_{R_2} \approx \frac{\gamma_g \gamma_h}{\gamma_f(\gamma_g + \gamma_h)}, \gamma_{R_1}^{(3)} \approx \frac{\gamma_g {\gamma_h}^2}{(\gamma_g + \gamma_h)^2 \gamma_f + 2\gamma_h {\gamma_g}^2}, \tag{5}$$

$$\gamma_{D}^{(3)} \approx \frac{\gamma_g \gamma_h \gamma_f}{3} \gamma_h \gamma_f + 2\gamma_f \gamma_g + \gamma_g \gamma_h. \tag{6}$$

Remark 1 The SINR expressions in (5) reveal that the amount of information leakage is saturated when the transmit SNR goes to infinity. However, the received SINR at the legitimate receiver is a monotonically increasing function of the transmit SNR. As a result, the achievable ESR is increased as the transmit SNR grows which is fundamentally different from the direct transmission scheme [14].

Remark 2 As can be understood, in the proposed scheme, when a node transmits the information signal in the line of destination, the node which is near to the receiving untrusted relay is forced to propagate artificial noise to confuse the eavesdropping node. As a consequence, this proposed scheme can be routinely extended to multi-hop untrusted relaying in which more than two untrusted relays cooperate to forward a confidential message to the destination. Specifically, when $\mathcal{R}_{i-1}$ forwards the received signal to $\mathcal{R}_i$, $\mathcal{R}_{i+1}$ jams the eavesdropper $\mathcal{R}_i$, and likewise, when re-transmitting the amplified version of the received signal by $\mathcal{R}_{i+1}$ to the next node, the nearest node to the transmitting relay, i.e., $\mathcal{R}_i$ may pose an eavesdropping attack, therefore, the relay $\mathcal{R}_{i-1}$ is scheduled to send artificial jamming signals to make the wiretap link of $\mathcal{R}_i$ degraded. Setting $\mathcal{R}_0$ and $\mathcal{R}_{N+1}$ to be $\mathcal{S}$ and $\mathcal{D}$, respectively, the above explanation, can be readily extended for the multi-hop untrusted relaying. However, this extension gets too involved to analyze, and more importantly, may not be efficient for a large number of hops. Since the latency of the network grows by increasing the number of intermediate nodes [21]. This is not acceptable in real-time communication scenarios. Furthermore, in IoT networks with low-cost and low-power equipment, the need for large overhead for the training process is challenging, especially when the environment is dynamic and thus, the coherence time of the wireless channel is short. As a result, in this work the three-hop untrusted scenario is considered for the purpose of analysis, though, may not be the optimal choice in terms of the number of relays. However, as we shall see later, the proposed multi-hop untrusted relaying with two relays improves the system performance.

Remark 3 It is worth pointing out that in the considered line network in which the end-to-end message delivery is conducted via multiple untrusted relays, we need to have careful scheduling and synchronization of transmissions based on the proposed TDMA-based protocol. Hence, all the network nodes are assumed to perform their transmissions in the equally-allocated time slots. Practically speaking, the communication channel, which could be considered as a sub-carrier of orthogonal frequency-division multiplexing (OFDM) system, is divided into separate time slots, and then, the communication process is accomplished through the mentioned multiple-phase protocol. Note that in this work, we have not considered scheduling and synchronization errors, each of which is worthy of deep investigation.

4 Secrecy performance analysis

Note that the Ergodic secrecy rate (ESR), as a widely used secrecy criteria in the literature, characterizes the rate below which any average secure transmission rate can be obtained. In this section, we proceed to derive a new closed-form expression for the ESR of three-hop untrusted relaying.

Based on the definition, the instantaneous secrecy rate is achieved by subtracting the eavesdropping channel capacity from the legitimate channel capacity [3]. Since the untrusted relays are non-colluding and they adopt SC technique, the instantaneous secrecy rate, R_s, for a three-hop relaying can be evaluated by

$$R_s = \frac{1}{3}\left[I_D^{(3)} - \max\{I_{R_1}^{(1)}, I_{R_2}^{(2)}, I_{R_1}^{(3)}\}\right]^+, \tag{7}$$

where $I_K = \log_2(1+\gamma_K)$ with $K \in \{\mathcal{R}_1, \mathcal{R}_2, \mathcal{D}\}$ and $[x]^+ = \max(x, 0)$. Notably, the pre-log factor $\frac{1}{3}$ is due to the fact that one round of transmission is done in three hops.

Remark 4 It is worth noting that $\gamma_{R_2}^{(2)} \gg \gamma_{R_1}^{(3)}$, which can be readily concluded by invoking $\gamma_{R_2}^{(2)}$ and $\gamma_{R_1}^{(3)}$ expressions given in (5). Therefore, the maximum information leakage of three-hop untrusted relaying can be simplified as

$$\gamma_E \triangleq \max\left\{\gamma_{R_1}^{(1)}, \gamma_{R_2}^{(2)}\right\}, \tag{8}$$

The exact ESR expression of the proposed three-hop untrusted relaying can be obtained by forming a multiple integral expression as

$$\bar{R_s} = \mathbb{E}\{R_s\} = \int_0^\infty \int_0^\infty \int_0^\infty R_s(p,q,r) f_{\gamma_g}(p) f_{\gamma_h}(q) f_{\gamma_f}(r) \mathrm{d}p\mathrm{d}q\mathrm{d}r, \tag{9}$$

where in $R_s(p,q,r)$ is given in (7), and the probability density functions (PDFs) $f_{\gamma_t}(s) = \frac{1}{\bar{\gamma}_t}\exp\left(-\frac{s}{\bar{\gamma}_t}\right)$ with $s \geq 0$ for $t \in$ {g, h, f}. Although, the integral expression given above can be calculated numerically, in order to obtain deep insight into the impact of parameters in secrecy rate, we are interested in obtaining a new compact expression for the ESR. To that aim, we first derive closed-form expressions for the Ergodic legitimate rate $\bar{R_L}$ and the Ergodic eavesdropping rate $\bar{R_E}$ in the following lemmas, and thereafter, we will be ready to present a tight lower-bound expression for the ESR performance in Proposition 1.

Lemma 1 The lower-bound closed-form expression for the Ergodic rate of the legitimate channel, without pre-log factor, is given by

$$\begin{aligned}\bar{R_L} &= \mathbb{E}\left\{\log_2(1+\gamma_D)\right\} \\ &\geq \log_2\left(1+\exp\left[-3\Phi + \ln\left(\frac{\bar{\gamma}_g\bar{\gamma}_h\bar{\gamma}_f}{3\bar{\gamma}_h\bar{\gamma}_f + 2\bar{\gamma}_f\bar{\gamma}_g + \bar{\gamma}_g\bar{\gamma}_h}\right)\right]\right) \\ &\triangleq \bar{R}_L^{LB},\end{aligned} \tag{10}$$

where $\Phi \approx 0.577215$ is the Euler constant.

Proof The proof can be done straightforwardly by considering the facts that: (1) the Jensen's inequality can apply on the convex function $\ln(1+\exp(x))$ with respect to x and, (2) for the exponential random variable (RV) X with the mean of m_X, we have $\mathbb{E}\{\ln(X)\} = -\Phi + \ln(m_x)$ [33, Eq. (4.331.1)]. □

Before proceeding further to derive an analytical expression for $\bar{R_E}$, we present the following fruitful Lemma.

Lemma 2 *Let X and Y be exponential RVs with means m_x and m_y, respectively. Then the new RVs $Z = \frac{X}{Y}$ and $W = \frac{XY}{X+Y}$ have the following cumulative distribution functions (CDFs), respectively, as*

$$F_Z(z) = \frac{m_y z}{m_y z + m_x}, \tag{11}$$

$$F_W(w) = 1 - \frac{2\omega}{\sqrt{m_x m_y}} \exp\left(-\frac{\omega}{m_x} - \frac{\omega}{m_y}\right) \mathrm{K}_1\left(\frac{2\omega}{\sqrt{m_x m_y}}\right), \tag{12}$$

where $\mathrm{K}_v(\cdot)$ is the modified Bessel function of the second kind and v-th order.

Proof See "Appendix A". □

Lemma 3 *The closed-form expression for the Ergodic rate of the eavesdropping channel, without pre-log factor, is formulated as*

$$\begin{aligned} \bar{R_E} &= \mathbb{E}\left\{ \log_2(1+\gamma_E) \right\} \\ &= \frac{1}{\ln 2}\mathbb{E}\left\{ \ln\left(1 + \mathbb{1}_{\left\{\gamma_{R_1}^{(1)} \geq \gamma_{R_2}^{(2)}\right\}} \gamma_{R_1}^{(1)} + \mathbb{1}_{\left\{\gamma_{R_2}^{(2)} > \gamma_{R_1}^{(1)}\right\}} \gamma_{R_2}^{(2)} \right) \right\} \\ &= \frac{1}{\ln 2}\mathbb{E}\left\{ \mathbb{1}_{\left\{\gamma_{R_1}^{(1)} \geq \gamma_{R_2}^{(2)}\right\}} \ln\left(1+\gamma_{R_1}^{(1)}\right) + \mathbb{1}_{\left\{\gamma_{R_2}^{(2)} > \gamma_{R_1}^{(1)}\right\}} \ln\left(1+\gamma_{R_2}^{(2)}\right) \right\} \\ &= \frac{1}{\ln 2}\left(\mathcal{P}T_1 + (1-\mathcal{P})T_2\right), \end{aligned} \tag{13}$$

where

$$\mathbb{1}_{\{X\}} = \begin{cases} 1 & \text{if } \mathrm{X} = \mathit{True} \\ 0 & \text{o.w.,} \end{cases}$$

represents the indicator function which is one iff its condition is satisfied, and the last equation follows from total probability theorem or simply considering the expectation of indicator function which can be further calculated analytically as

$$\begin{aligned} \mathcal{P} &= \mathbb{E}\left\{ \mathbb{1}_{\left\{\gamma_{R_1}^{(1)} \geq \gamma_{R_2}^{(2)}\right\}} \right\} \\ &= \Pr\left\{ \gamma_{R_1}^{(1)} \geq \gamma_{R_2}^{(2)} \right\} \\ &= \frac{\sqrt{\bar{\gamma}_f \bar{\gamma}_g}^{3/2}}{\bar{\gamma}_g - \bar{\gamma}_h \sqrt{\bar{\gamma}_f}\sqrt{\bar{\gamma}_g} + 2\,\bar{\gamma}_g\,\bar{\gamma}_h} \\ &\times \sum_{n=1}^{M}\sum_{i=1}^{n} \Lambda(1,n,i) i! \left(\frac{2\bar{\gamma}_g\,\bar{\gamma}_h}{\bar{\gamma}_g - \bar{\gamma}_h \sqrt{\bar{\gamma}_f\,\bar{\gamma}_g} + 2\,\bar{\gamma}_g\,\bar{\gamma}_h} \right)^i, \end{aligned} \tag{14}$$

where the parameter M holds an arbitrary positive integer value controlling the approximation accuracy. Also,

$$\Lambda(v,n,i) = \frac{(-1)^i \sqrt{\pi}\Gamma(2v)\Gamma(n-v+\frac{1}{2})\mathrm{L}(n,i)}{2^{v-i}\Gamma(\frac{1}{2}-v)\Gamma(n+v+\frac{1}{2})n!},$$

where $\mathrm{L}(i,n) = \binom{n-1}{i-1}\frac{n!}{i!}$ for $n, i > 0$ represents the Lah numbers [34], $\Gamma(x)$ is the Gamma function [33, Eq. (8.31)]. Furthermore,

$$T_1 = \frac{\bar{\gamma}_g \ln(\frac{\bar{\gamma}_g}{\bar{\gamma}_h})}{\bar{\gamma}_g - \bar{\gamma}_h}, \tag{15}$$

$$T_2 = \ln\left(1 + \frac{\bar{\gamma}_g\bar{\gamma}_h\left(\bar{\gamma}_g^2 - \bar{\gamma}_h^2 - 2\bar{\gamma}_g\bar{\gamma}_h \ln\frac{\bar{\gamma}_g}{\bar{\gamma}_h}\right)}{\bar{\gamma}_f(\bar{\gamma}_g - \bar{\gamma}_h)^3}\right), \tag{16}$$

Proof See "Appendix B". □

Proposition 1 *The tight closed-form lower-bound expression for the ESR performance of the proposed three-hop untrusted relaying is given by*

$$\bar{R_s^{LB}} = \frac{1}{3}\left[\bar{R_L^{LB}} - \bar{R_E}\right]^+. \tag{17}$$

4.1 Asymptotic ergodic secrecy rate analysis

Now , we are going to obtain the asymptotic expression for the ESR performance, denoted by R_s^∞, when the transmit SNR of each node, ρ, goes to infinity by deriving the high-SNR slope S_∞ in bits/s/Hz and the high-SNR power offset L_∞ in 3dB unit. These parameters are defined, respectively, as [26]

$$\begin{aligned} S_\infty &= \lim_{\rho\to\infty} \frac{\bar{R_s}}{\log_2 \rho} \\ \text{and} L_\infty &= \lim_{\rho\to\infty} (\log_2 \rho - \frac{\bar{R_s}}{S_\infty}), \end{aligned} \tag{18}$$

$$R_s^\infty = S_\infty(\log_2 \rho - L_\infty), \tag{19}$$

Following the same steps as in [24], the high-SNR slope and power offset of the three-hop untrusted relaying are obtained as

$$S_\infty = \frac{1}{3}, \tag{20}$$

and

$$\begin{aligned} L_\infty &= \frac{3\Phi}{\ln 2} + \log_2\left(\frac{3}{m_g} + \frac{2}{m_h} + \frac{1}{m_f}\right) \\ &+ \mathcal{P}_1\mathcal{A} + (1-\mathcal{P}_1)\mathcal{B}, \end{aligned} \tag{21}$$

where

$$\mathcal{A} = \frac{m_g(\log_2(m_g) - \log_2(m_h))}{m_g - m_h}, \tag{22}$$

$$\mathcal{B} = \log_2\left[1 + \frac{m_g m_h(m_g + m_h - 2m_h\mathcal{A})}{m_f(m_g - m_h)^2}\right], \tag{23}$$

Proof The analytical expressions of S_∞ and L_∞ can be readily obtained by plugging (1), while considering

Remark 1, into the definition of high-SNR slope and power offset given by (18) and using the approximation $\log(1+x) \approx \log(x)$ when $x \gg 1$. Besides, $\mathcal{P}_1$ is defined in "Appendix A". Hence, we skipped the details for the sake of brevity.

Expression (20) highlights that the channel powers have no impact on the ESR slope which is equal to the maximum multiplexing gain of the network. Furthermore, different from the high-SNR slope, we find that the high-SNR power offset in (21) is related to the all channel powers. As such, by properly positioning the relays between the source and destination, the high-SNR power offset can be reduced. Notably, a decrease in the power offset corresponds to an increase in the ESR performance.

5 Numerical results and discussions

In this section, we prepare some simulations to reveal the accuracy of the presented closed-form expressions. Additionally, we compare the secrecy performance of the proposed multi-hop relaying scheme with two competitive counterparts: (1) the two-hop communication scheme where only one relay is selected for data transmission and the other relay is considered as pure eavesdropper, and (2) the direct transmission where the confidential information is directly forwarded to the destination without getting assistance from the two relays. In this case, both the relays are considered as pure eavesdroppers. Unless otherwise stated, the following simulation parameters are adopted. We assume that the nodes $\mathcal{S}$, $\mathcal{D}$, $\mathcal{R}_1$, and $\mathcal{R}_2$ are placed on one-dimensional space at positions -3, $+3$, -1 and $+1$, respectively. Additionally, the large-scale path-loss factor is chosen η= 2.7. Besides, for Mont-Carlo simulations we averaged over 10^5 channel realizations.

Figure 3 is plotted to depict the ESR performance versus the transmit SNR ρ (in dB). As can be seen in this figure, our proposed lower-bound expression for the ESR in Proposition 1 agrees well with the exact ESR. Furthermore, our asymptotic ESR performance given by (19) well-approximates the exact ESR in the high-SNR regime. As observed from Fig. 3, the ESR curve corresponding to the case when considering only the first term of the equivalent series, denoted by Theory with $M=1$ is so close to the exact ESR curve, especially in high-SNR regime. This reaffirms the accuracy and tightness of analytical expressions we obtained.

To reveal the advantage of the proposed three-hop untrusted relaying scheme, we compare the ESR performance of our new scheme with two well-known transmission schemes, i.e., two-hop untrusted relaying and direct transmission. Note that under two-hop relaying scheme, we face with two cases. In Case I, the relay $\mathcal{R}_1$ is employed for data re-transmission and the relay $\mathcal{R}_2$ is considered as a pure eavesdropper, as illustrated in Fig. 4a. Whereas, in Case II, the converse scenario is considered, i.e., the relay $\mathcal{R}_2$ is the helper node and $\mathcal{R}_1$ is considered as an idle eavesdropper, as illustrated in Fig. 4b. Additionally, two network topologies are considered. In Topology 1, we have the same network structure as considered in Fig. 3, and for Topology 2, we have the scaled version of Topology 1 with the factor of 3, i.e., the nodes $\mathcal{S}$, $\mathcal{D}$, $\mathcal{R}_1$ and $\mathcal{R}_2$ are located at -9, $+9$, -3 and $+3$, respectively.

As it can be observed in Fig. 5, the secrecy performance of the proposed three-hope relaying scheme always outperforms the mentioned two benchmarks for the transmit SNRs fewer than approximately 36 dB (i.e., $\rho <$ 36 dB). This result highlights the priority of our scheme compared with the state-of-the-arts in untrusted relaying networks. One can easily predict that the proposed scheme under Topology 2 outperforms the two-hop relaying schemes for $\rho >$ 36 dB. Interestingly, under Topology 1 and for $\rho >$ 36 dB, the two-hop relaying scheme with Case I would provide a better ESR compared with our scheme. The reason is that when the communication nodes are close together with much power budget, naturally, the two-hop relaying would be sufficient for data transmission and hence, it is not necessary to implement multi-hop relaying scheme. Additionally, as proved in [26], the high-SNR slope for two-hop relaying is $S_\infty = \frac{1}{2}$ which is more than the high-SNR slope of tree-hop relaying scheme, $S_\infty = \frac{1}{3}$, as we derived in (20). It is worth noting that in IoT and

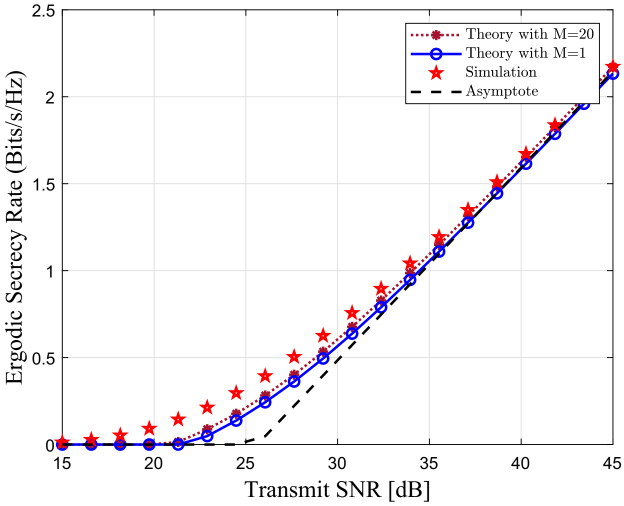
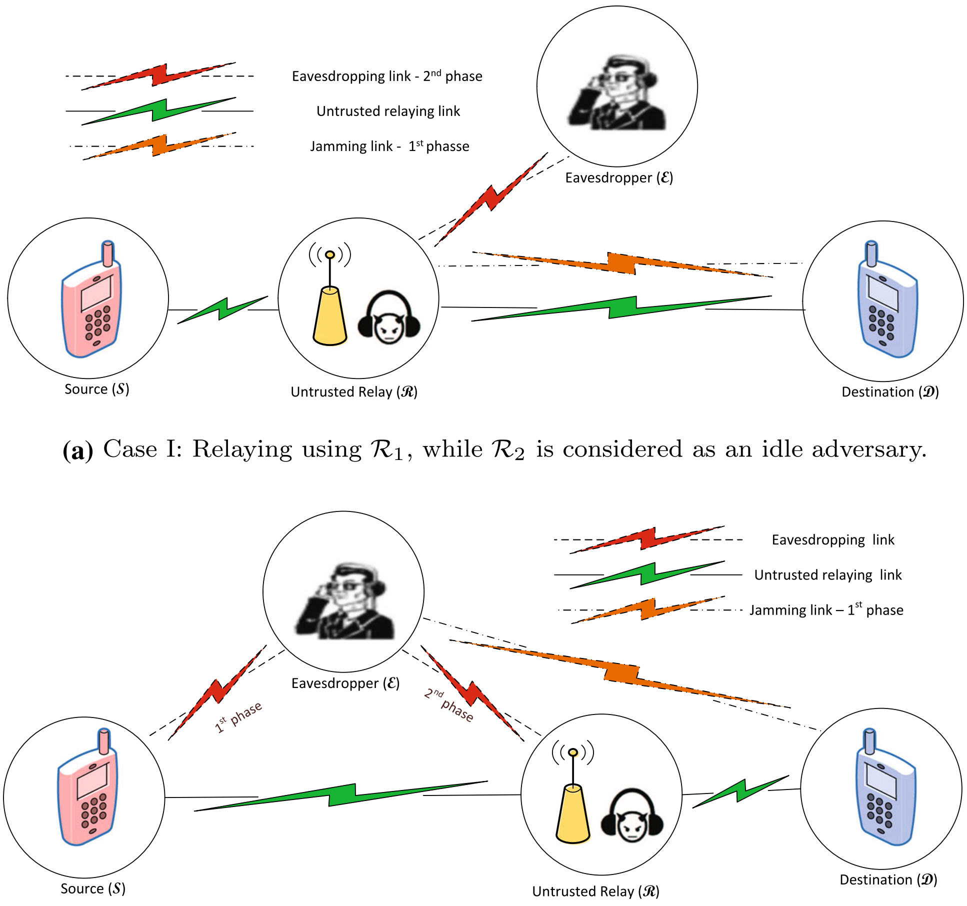


Fig. 3 Validation of theoretical results for the ESR performance

Fig. 4 Considered two-hop untrustworthy relaying as benchmarks



(a) Case I: Relaying using $\mathcal{R}_1$, while $\mathcal{R}_2$ is considered as an idle adversary.

(b) Case II: Relaying using $\mathcal{R}_2$, while $\mathcal{R}_1$ is considered as an idle adversary.

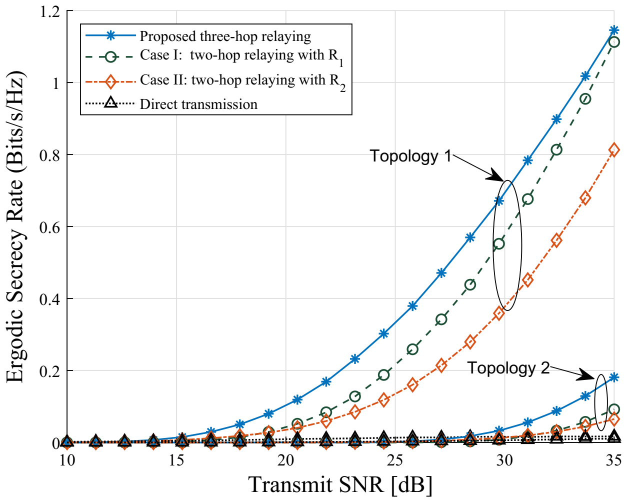


Fig. 5 ESR versus transmit SNR for different transmission schemes and topologies

WSNs, the devices are power-limited and thus, they cannot consume much power for data transmission/forwarding. As a result, the proposed secure three-hop relaying scheme in this paper is applicable for IoT networks where low or medium transmit SNRs can be supported by the devices. Finally, this figure depicts that the direct transmission scheme presents a near to zero, but non-zero, secrecy rate. As discussed in [26], even when the destination is very far from the source while the eavesdroppers locate between them, a positive secrecy rate is achievable.

Figure 6 exhibits the ESR performances of the proposed multi-hop untrusted relaying and the known schemes against the path-loss exponent. Obviously, the ESR gets decreased for higher order of path-loss values which demonstrates severe fading or blockage results in lower ESR. Nonetheless, the proposed scheme with two relays provides a significantly pronounced ESR performance for practical values of η. For example, the ESR of the proposed

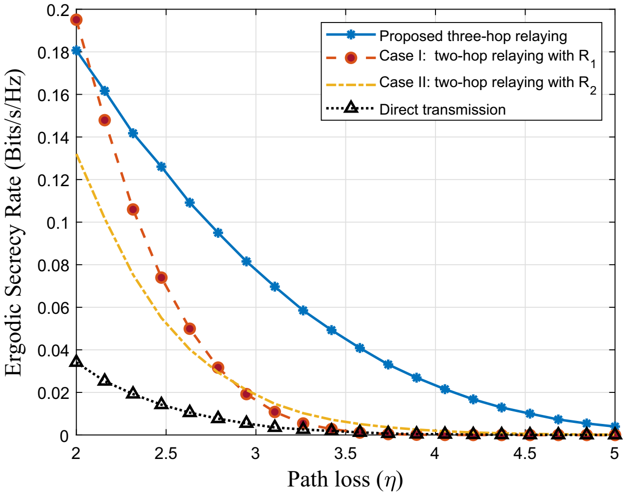


Fig. 6 ESR versus path-loss exponent for different transmission schemes. SNR is set to $\rho = 20$dB

scheme has threefold improvement compared to that of the two-hop relaying for the path-loss of 3. This again boosts the effectiveness of our proposed secure scheme in real-world applications such as WSN and low-altitude UAV-based relaying networks [13] wherein fading or blockage are undeniable.

6 Conclusions

In this contribution, we designed a new secure transmission scheme over a multi-hop untrusted relaying network. To this end, we first studied a three-hop communication network with two successive untrusted relays. Given this system model, a novel closed-form expression was derived in the high-SNR regime for the ESR performance. We next evaluated the high-SNR slope and power offset of the ESR. Our numerical results presented that the proposed secure transmission scheme improves the secrecy performance compared with the competitive benchmarks, i.e., the two-hop relaying and the conventional direct transmission schemes. As future work, we could consider the impacts of imperfect CSI and hardware impairments on the secrecy performance of the considered multi-hop untrusted relaying as well as resource allocation problem for such a network.

A Proof of Lemma 2

The CDF of $Z = \frac{X}{Y}$ has been derived in [14]. To obtain the CDF of $W = \frac{XY}{X+Y}$, we start from the definition of CDF as

$$\begin{aligned} F_W(\omega) &= \Pr\left\{\frac{XY}{X+Y} < \omega\right\} \\ &= \Pr\left\{XY - \omega(X+Y) < 0\right\} \\ &= \Pr\left\{X < \frac{\omega Y}{Y-\omega} | Y-\omega \geq 0\right\} \Pr\{Y-\omega \geq 0\} \\ &\quad + \Pr\left\{X \geq \frac{\omega Y}{Y-\omega} | Y-\omega < 0\right\} \Pr\{Y-\omega < 0\} \\ &= \int_{\omega}^{\infty} F_X\left(\frac{\omega y}{y-\omega}\right) f_Y(y)\mathrm{d}y + \int_0^{\omega} f_Y(y)\mathrm{d}y \\ &= \int_{\omega}^{\infty} \left[1 - \exp\left(-\frac{\omega y}{m_x(y-\omega)}\right)\right] f_Y(y)\mathrm{d}y + \int_0^{\omega} f_Y(y)\mathrm{d}y \\ &= 1 - \frac{1}{m_y}\int_{\omega}^{\infty} \exp\left(-\frac{\omega y}{m_x(y-\omega)} - \frac{y}{m_y}\right)\mathrm{d}y \\ &= 1 - \frac{1}{m_y}\exp\left(-\frac{\omega}{m_x} - \frac{\omega}{m_y}\right)\int_0^{\infty} \\ &\quad \exp\left(-\frac{\omega^2}{m_x y} - \frac{y}{m_y}\right)\mathrm{d}y \\ &\overset{(a)}{=} 1 - \frac{2\omega}{\sqrt{m_x m_y}}\exp\left(-\frac{\omega}{m_x} - \frac{\omega}{m_y}\right)\mathrm{K}_1\left(\frac{2\omega}{\sqrt{m_x m_y}}\right), \end{aligned} \tag{24}$$

Finally, after calculating the integral term using [33, Eq. (3.324.1)], one can obtain the expression given in (11). □

B Proof of Lemma 3

In the following, we proceed to prove Lemma 3 wherein the different exact/approximate expressions for $\mathcal{P}$, $\mathcal{T}_1$, and $\mathcal{T}_2$ are given.

A. Calculating $\mathcal{P}$ Plugging (5) into $\mathcal{P} = \Pr\{\gamma_{R_1}^{(1)} > \gamma_{R_2}^{(2)}\}$, and then defining $X = \gamma_f$, $Y = \gamma_h$ and $Z = \gamma_g$, we get

$$\begin{aligned}\mathcal{P} &= \Pr\left\{\gamma_f > \frac{\gamma_h^2}{\gamma_g+\gamma_h}\right\} = 1 - \Pr\left\{X < \frac{Y^2}{Y+Z}\right\}\\ &= 1 - \mathbb{E}_Y\left\{\mathbb{E}_Z\left\{F_X\left(\frac{y^2}{y+z}\right)\right\}\right\}\\ &= \frac{1}{m_y m_z}\int_0^\infty\int_0^\infty\\ &\quad \exp\left(-\frac{y^2}{(y+z)m_x} - \frac{y}{m_y} - \frac{z}{m_z}\right)\mathrm{d}z\mathrm{d}y\\ &\overset{(a)}{=} \frac{1}{m_y m_z}\int_0^\infty\int_0^\infty\\ &\quad \exp\left(-\frac{v^2}{u m_x} - \frac{v}{m_y} - \frac{u-v}{m_z}\right)\mathrm{d}u\mathrm{d}v\\ &\overset{(b)}{=} \sqrt{\frac{4}{m_x m_y m_z}}\int_0^\infty\\ &\quad \exp\left(-v\frac{m_y - m_z}{m_y m_z}\right) v K_1\left(\sqrt{\frac{2}{m_x m_z}v}\right)\mathrm{d}v\\ &\overset{(c)}{\approx} \frac{\sqrt{m_x}{m_z}^{3/2}}{m_z - m_y\sqrt{m_x}\sqrt{m_z}} + 2\, m_z\, m_y\\ &\quad \sum_{n=1}^{M}\sum_{i=1}^{n}\Lambda(1,n,i)i!\left(\frac{2m_z\, m_y}{m_z - m_y\sqrt{m_x\, m_z} + 2\, m_z\, m_y}\right)^i,\\ &\overset{(d)}{\approx} \frac{4\sqrt{m_x}{m_z}^{5/2}m_y}{3\left(m_z - m_y\sqrt{m_x}\sqrt{m_z} + 2\, m_z\, m_y\right)^2} \overset{\Delta}{=} \mathcal{P}_1,\end{aligned} \tag{25}$$

where (a) follows from defining the auxiliary variables $u = y + z$ and $v = y$, (b) follows from using [33, Eq. (3.324.1)] and [33, Eq. (3.351.3)], (c) follows from substituting the equivalent series of modified Bessel function of the second kind and first order as presented in [34], which is a well-tight approximation with finite series, as observed later in numerical results. For $v > 0$ and positive integer M which controls the accuracy of infinite series, we have [34]

$$K_v(\beta x) \approx \exp(-\beta x)\sum_{n=0}^{M}\sum_{i=0}^{n}\Lambda(v,n,i)(\beta x)^{i-v},$$

Finally, (d) presents the first term of the infinite series given for $M = 1$ to have a closed-form approximation. We will show in the simulation results how this simple closed-form expression works well.

B. Calculating T_1 Using Lemma 2, we can derive a closed-form expression for T_1, after assuming $X = \frac{\gamma_g}{\gamma_h}$, as

$$\begin{aligned} T_1 &= \mathbb{E}\left\{\ln(1+\frac{\gamma_g}{\gamma_h})\right\}\\ &= \int_0^\infty \ln(1+x)f_X(x)\mathrm{d}x\\ &\overset{(a)}{=} \end{aligned} \tag{26}$$

where (a) follows from integration by parts law. Then, computing the last integral, considering $F_X(x)$ given in Lemma 2, leads to the closed-form expression for T_1 given in (27).

C. Calculating T_2 The part T_2 can be mathematically calculated as

$$T_2 = \mathbb{E}\left\{\ln\left(1 + \frac{\gamma_g\gamma_h}{\gamma_f(\gamma_g+\gamma_h)}\right)\right\} \overset{(a)}{\approx} \ln\left(1 + \frac{\mathbb{E}\left\{\frac{\gamma_g\gamma_h}{\gamma_g+\gamma_h}\right\}}{\mathbb{E}\{\gamma_f\}}\right), \tag{27}$$

where (a) follows after using the approximation $\mathbb{E}\left\{\log(1+\frac{X}{Y})\right\} \approx \log\left(1+\frac{\mathbb{E}\{X\}}{\mathbb{E}\{Y\}}\right)$ given in [35]. Thus, after further calculation, using Lemma 2, one can obtain T_2 in (27). □

References

1. Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, *104*(9), 1727–1765.
2. Memon, I., Ali, Q., Zubedi, A., & Mangi, F. A. (2017). DPMM: dynamic pseudonym-based multiple mix-zones generation for mobile traveler. *Multimedia Tools and Applications*, *76*(22), 24359–24388.
3. Mukherjee, A., Fakoorian, S. A. A., Huang, J., & Swindlehurst, A. L. (2014). Principles of physical-layer security in multiuser wireless networks: A survey. *IEEE Communication on Surveys and Tutorials*, *16*(3), 3062–3080.
4. Wang, N., Wang, P., Alipour-Fanid, A., Jiao, L., & Zeng, K. (2019). Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities. *IEEE Internet of Things Journal*, *6*(5), 8169–8181.
5. Yener, A., & Ulukus, S. (2015). Wireless physical-layer security: Lessons learned from information theory. *Proceedings of the IEEE*, *103*(10), 1814–1825.
6. Yang, N., Wang, L., Geraci, G., Elkashlan, M., Yuan, J., & Renzo, M. D. (2015). Safeguarding 5G wireless communication networks using physical layer security. *IEEE Communications Magazine*, *53*(4), 20–27.
7. Wang, N., Wang, P., Alipour-Fanid, A., Jiao, L., & Zeng, K. (2019). Physical layer security of 5G wireless networks for IoT: Challenges and opportunities. *IEEE Internet of Things Journal*, *6*(5), 8169–8181.
8. Hamamreh, J. M., Furqan, H. M., & Arslan, H. (2018). Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. *IEEE Communications Surveys and Tutorials*, *21*(2), 1773–1828.

9. Sun, L., & Du, Q. (2018). A review of physical layer security techniques for internet of things: Challenges and solutions. *Entropy*, *20*(10), 730.
10. Yang, N., Yan, S., Yuan, J., Malaney, R., Subramanian, R., & Land, I. (2015). Artificial noise: Transmission optimization in multi-input single-output wiretap channels. *IEEE Transactions on Communications*, *63*(5), 1771–1783.
11. Wang, L., Cai, Y., Zou, Y., Yang, W., & Hanzo, L. (2015). Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays. *IEEE Transactions on Vehicular Technology*, *65*(8), 6259–6274.
12. Tatar Mamaghani, M., & Hong, Y. (2020). Improving PHY-security of UAV-enabled transmission with wireless energy harvesting: Robust trajectory design and communications resource allocation. *IEEE Transactions on Vehicular Technology*, *69*(8), 8586–8600.
13. Tatar Mamaghani, M., & Hong, Y. (2019). On the performance of low-altitude UAV-enabled secure AF relaying with cooperative jamming and SWIPT. *IEEE Access*, *7*, 153060–153073.
14. Kuhestani, A., Mohammadi, A., & Yeoh, P. L. (2018). Security-reliability trade-off in cyber-physical cooperative systems with non-ideal untrusted relaying. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore*, (pp. 552–557).
15. Tatar Mamaghani, M., Mohammadi, A., Yeoh, P. L., & Kuhestani, A. (2017). Secure two-way communication via a wireless powered untrusted relay and friendly jammer. Paper presented at the GLOBECOM 2017 IEEE Global Communications Conference.
16. Shakhatreh, H., et al. (2019). Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges. *IEEE Access*, *7*, 48572–48634.
17. Chen, Y., Zhao, N., Ding, Z., & Alouini, M. (2018). Multiple UAVs as relays: Multi-hop single link versus multiple dual-hop links. *IEEE Transactions on Wireless Communications*, *17*(9), 6348–6359.
18. Abro, A., et al., (2019). Minimizing Energy Expenditures using Genetic Algorithm for Scalability and Longlivety of Multi hop Sensor Networks. In *2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC)* (pp. 183–187).
19. Hasan, M. K., Ismail, A. F., Islam, S., Hashim, W., Ahmed, M. M., & Memon, I. (2019). A novel HGBBDSA-CTI approach for subcarrier allocation in heterogeneous network. *Telecommunication Systems*, *70*(2), 245–262.
20. Abdo, A. M. A., Zhao, X., Zhang, R., Zhou, Z., Zhang, J., Zhang, Y., et al. (2018). MU-MIMO downlink capacity analysis and optimum code weight vector design for 5G big data massive antenna millimeter wave communication. *Wireless Communications and Mobile Computing*,. https://doi.org/10.1155/2018/7138232.
21. Sung, Y., Lee, S., & Lee, M. (2018). A multi-hop clustering mechanism for scalable IoT networks. *Sensors*,. https://doi.org/10.3390/s18040961.
22. He, X., & Yener, A. (2008). Two-hop secure communication using an untrusted relay: A case for cooperative jamming. In *Proceedings of IEEE Globecom*, (pp. 1–5). New Orleans, LA .
23. Sun, L., Ren, P., Du, Q., Wang, Y., & Gao, Z. (2014). Security-aware relaying scheme for cooperative networks with untrusted relay nodes. *IEEE Communications Letters*, *19*(3), 463–466.
24. Tatar Mamaghani, M., Kuhestani, A., & Wong, K.-K. (2018). Secure two-way transmission via wireless-powered untrusted relay and external jammer. *IEEE Transactions on Vehicular Technology*, *67*(9), 8451–8465.
25. Tatar Mamaghani, M., & Abbas, R. (2019). Security and reliability performance analysis for two-way wireless energy harvesting based untrusted relaying with cooperative jamming. *IET Communications*, *13*(4), 449–459.
26. Kuhestani, A., Mohammadi, A., & Mohammadi, M. (2018). Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers. *IEEE Transactions on Information Forensics and Security*, *13*(2), 341–355.
27. Zhang, G., Yan, H., Zeng, Y., Cui, M., & Liu, Y. (2018). Trajectory optimization and power allocation for multi-hop UAV relaying communications. *IEEE Access*, *6*, 48566–48576.
28. Wang, H., Zhang, Y., Ng, D. W. K., & Lee, M. H. (2018). Secure routing with power optimization for ad-hoc networks. *IEEE Transactions on Communications*, *66*(10), 4666–4679.
29. Yao, J., Zhou, X., Liu, Y., & Feng, S. (2018). Secure transmission in linear multi-hop relaying networks. *IEEE Transactions on Wireless Communications*, *17*(2), 822–834.
30. He, X., & Yener, A. (2013). End-to-end secure multi-hop communication with untrusted relays. *IEEE Transactions on Wireless Communications*, *12*(1), 1–11.
31. Mirmohseni, M., & Papadimitratos, P. (2014). Colluding eavesdroppers in large cooperative wireless networks. In *2014 IEEE Iran Workshop on Communication and Information Theory (IWCIT)*, (pp. 1-6).
32. Zhao, X., Abdo, A. M. A., Xu, C., Geng, S., Zhang, J., & Memon, I. (2017). Dimension reduction of channel correlation matrix using CUR-decomposition technique for 3D massive antenna system. *IEEE Access*, *6*, 3031–3039.
33. Gradshteyn, I. S., & Ryzhik, I. M. (2007). *Table of integrals, series, and products* (7th ed.). New York: Academic.
34. Molu, M. M., Xiao, P., Khalily, M., Zhang, L., & Tafazolli, R. (2017). A novel equivalent definition of modified Bessel functions for performance analysis of multi-hop wireless communication systems. *IEEE Access*, *5*, 7594–7605.
35. Bjornson, E., Matthaiou, M., & Debbah, M. (2013). A new look at dual-hop relaying: Performance limits with hardware impairments. *IEEE Transactions on Communications*, *61*(11), 4512–4525.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Milad Tatar Mamaghani was born in Tabriz, Iran, on May 12, 1994. He received the B.Sc. degree in electrical-communications engineering (major) and control engineering (minor) from the Amirkabir University of Technology, Tehran, Iran. He is currently working towards the Ph.D. degree with the Department of Electrical and Computer Systems Engineering, Monash University, Melbourne, VIC, Australia. He has served as a Reviewer of many and various prestigious IEEE transactions journals and conferences. His research interests mainly focus on B5G wireless communications and networking, physical-layer security, and UAV communications.

Ali Kuhestani (Student Member, IEEE) received the Ph.D. degree in electrical engineering from the Amirkabir University of Technology, Tehran, Iran, in 2017. From 2018 to 2020, he was a Post-Doctoral Researcher with the Department of Electrical Engineering, Sharif University of Technology, Tehran. He is currently an Assistant Professor with the Faculty of Electrical and Computer Engineering, Qom University of Technology (QUT), and an Adjunct Professor with the Electrical Engineering Department, Amirkabir University of Technology (Tehran Polytechnic), Tehran. He has authored or co-authored more than 30 journals in prestigious publication avenues (e.g., the IEEE and IET) and more than 10 articles in major conference proceedings. His research interests include physical layer security of wireless communications, the Internet of Things, millimeter-wave communication, massive MIMO systems, and space-time coding. He was a recipient of Iran's National Elites Foundation Award for outstanding students in 2017. He was a Reviewer of the IEEE TRANSACTIONS/JOURNALS and conferences.

Hamid Behroozi (Member, IEEE) received the B.Sc. degree in electrical engineering from the University of Tehran, Tehran, Iran, in 2000, the M.Sc. degree in electrical engineering from the Sharif University of Technology, Tehran, in 2003, and the Ph.D. degree in electrical engineering from Concordia University, Montreal, QC, Canada, in 2007. From 2007 to 2010, he was a Post-Doctoral Fellow with the Department of Mathematics and Statistics, Queen's University, Kingston, ON, Canada. He is currently an Associate Professor with the Department of Electrical Engineering, Sharif University of Technology. His research interests include information theory, joint source-channel coding, artificial intelligence in signal processing and data science, and cooperative communications. He was a recipient of several academic awards, including the Ontario Postdoctoral Fellowship awarded by the Ontario Ministry of Research and Innovation (MRI), the Quebec Doctoral Research Scholarship awarded by the Government of Quebec (FQRNT), the Hydro Quebec Graduate Award, and the Concordia University Graduate Fellowship.