Research Article

Physical Layer Secrecy Analysis of Multihop Hybrid Satellite-Terrestrial Relay Networks with Jamming

Xiaoqi Wang, Hanwei Zhang, and Zheng Hou

School of Surveying and Land Information Engineering, Henan Polytechnic University, Jiaozuo 454003, China

Correspondence should be addressed to Zheng Hou; houzheng.com@163.com

Received 12 March 2021; Revised 3 May 2021; Accepted 20 May 2021; Published 10 June 2021

Academic Editor: Yuan Ding

Copyright © 2021 Xiaoqi Wang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This paper explores the secrecy analysis of a multihop hybrid satellite-terrestrial relay network (HSTRN) with jamming, where one satellite source is aimed at communicating with destination users via multihop decode-and-forward (DF) terrestrial relays, in the existence of an eavesdropper. All the destination users are deployed randomly following a homogeneous Poisson point process (PPP) based on stochastic geometry. Each relay operates not only as a conventional DF relay to forward the received signal but also as a jammer to generate intentional interference to degrade the eavesdropper link, considering shadowed-Rician fading for legitimate link and wiretap link while Rayleigh fading for jamming link. To characterize the secrecy performance of the considered network, the accurate analytical expression for the secrecy outage probability (SOP) is derived. In order to reveal further insights on the achievable diversity order of the network, the asymptotic behavior of SOP expression at high signal-to-noise ratio (SNR) region is deduced. Moreover, the throughput of the system is discussed to characterize the secrecy performance. Finally, the theoretical results are validated through comparison with simulation results and show that (1) the secrecy performance of the considered network gets better with the decreasing of the hops and with the decreasing severity of the channel fading scenario, (2) the relay of the network operating as a jammer can provide better secrecy performance without extra network resources, and (3) small hops and high SNR can yield to high throughput of the system.

1. Introduction

With the development of wireless communication towards high-speed and broadband, there are great challenges for wireless communication to support massive and seamless connection under limited spectrum, while satellite communication has become much popular on account of its high transmission quality, wide coverage at low cost, and easy deployment [1–3], and it has various applications in navigation, military defence, disaster response, and other remote or dangerous areas. Unfortunately, between the satellite and the terrestrial terminal, masking effect caused by some obstacles and shadowing will make the line-of-sight (LOS) communication unstable even unavailable, and the performance of the satellite network will be affected seriously. Therefore, relay technology has drawn increasing attention by researchers due to its improvement in the reliability and coverage of the networks [4–9].

Satellite communication with joined relay forms a new framework of hybrid satellite-terrestrial relay networks (HSTRN) [10–13]. This framework can provide satellite services to handheld devices, which has been incorporated in the DVB-SH standard [14]. In HSTRN, the relay transmits the signal from satellite to the destination. That cooperative technique has been an important approach in relay communication for its advantage of providing diversity gain, enhancing coverage, and reducing power consumption [15]. Amplify-and-forward (AF) and decode-and-forward (DF) are two cooperative diversity protocols in common. Based on different relay protocols, more and more researchers have paid attention to improving the performance of HSTRN from different views [12, 16, 17]. An et al. [12] investigated the outage probability (OP) performance and the ergodic capacity of an AF HSTRN. Sakarellos et al. [16] examined the OP performance of a HSTRN using the maximal ratio combining (MRC) technique based on DF relaying. The authors of [17] focused their research on the performance of a multiantenna HSTRN with multiple cochannel interferes at both the terrestrial relay and destination.
However, the transmission security of HSTRN is hardly involved. Recently, the security of wireless communication has become much important to evaluate a communication system. In the beginning, the security of satellite communication mainly bases on the traditional encryption method at upper layers, but there is a great challenge for this method because of its complex algorithm and without consideration of the error transmission at the physical layer. To solve this problem, Wyner characterized fading channels to achieve physical layer security based on information-theoretic approach [18]. And yet, research on physical layer secrecy in HSTRN is limited [19–24]. In [19], the authors explored the physical layer secrecy analysis of multiuser HSTRN by deriving accurate and asymptotic expressions for secrecy outage probability (SOP) and deducing the expression for probability of nonzero secrecy capacity. Huang et al. [20] investigated the secrecy performance of HSTRN by comparing AF and DF protocols, revealing that the system secrecy performance with the DF protocol was always better than that with the AF protocol. And on this basis, Bankey and Upadhyay [21] studied the physical layer security of a downlink HSTRN with multiantenna satellite, multiple terrestrial destinations, multiple relays, and multiple eavesdroppers. Guo et al. [22] presented a joint relay selection and a user scheduling scheme based on jammer to balance the system performance and actual implementation. In order to enhance the secrecy of the system under the total power constraint of relays, Yan et al. [23] investigated cooperative jamming by the relays to maximize the secrecy rate. Likewise, Yan et al. [24] maximized the secrecy rate of HSTRN through the joint optimization of the relay beamforming vector and the covariance matrix of artificial noise. In addition, the authors of [25] proposed an unmanned aerial vehicle (UAV) to ground communication system with spatially random eavesdropper account on both ground and airspace and investigated the secrecy performance of the system.

In general, the present physical layer secrecy studies mostly have focused on the HSTRN with dual-hop relaying [19, 20] or multiple users without consideration of their distribution [19], while multihop communication has been proved to extend the coverage of a wireless network effectively as well as to combat the adverse effects of wireless fading channels without more network resources [26]. Given its indoor coverage and service availability, especially in highly shadowed regions like shopping malls, office buildings, and dense residential areas, where the users of complicated distribution do not have LOS communication with the satellite due to masking effect, the investigation is explored in this paper.

In view of the aforementioned discussion, the secrecy performance of a multihop HSTRN is investigated, where a satellite source communicates with destination users via multihop relays in the presence of an eavesdropper. The relays use the DF protocol to forward the received signal and jam the reception of the eavesdropper simultaneously, while the ground users are deployed randomly. Both of the legitimate link (including satellite link and terrestrial link) and wiretap link experience shadowed-Rician fading [27, 28], while jamming link undergoes Rayleigh fading [29]. The main works we have done can be summed up as follows:

1. A multihop HSTRN with jamming is proposed, in which all the destination users are deployed randomly following a homogeneous Poisson point process (PPP) distribution based on stochastic geometry. The probability density functions (PDFs) and the cumulative distribution functions (CDFs) of the channel gain between the relay and users are deduced.

2. The accurate analytical SOP expression of the considered network is derived.

3. The asymptotic behavior of the SOP expression at high SNR region is explored, and the throughput of the system is obtained.

4. The simulation is carried out to verify the theoretical results, which reveal that the performance of a multihop HSTRN depends on the hops, secrecy rate, jammer, and shadowing severity of the considered network.

The rest of this paper proceeds as follows. The system model and channel model are presented in Section 2. The secrecy analysis of the network is provided in Section 3, where the accurate, asymptotic SOP formulas and the throughput of the system have been derived. Numerical and simulation results are given in Section 4, and conclusions are drawn in Section 5.

Notations. In this paper, | · | denotes the absolute value of a scalar, \( E[·] \) denotes the expectation operator, \( n! \) symbolizes the factorial of \( n \), \( f_X(·) \) and \( F_X(·) \) represent the PDF and CDF, respectively, and \( \Pr (·) \) means the probability for a random variable.

2. HSTRN Description

2.1. System Model. Considering the configuration of a downlink multihop HSTRN is shown in Figure 1, where one satellite source (S) communicates with destination users (D) via \( L−1 \) DF terrestrial relays \( \{R_l\}_{l=1}^L \), in the existence of an eavesdropper (E). Each relay operates as a conventional DF relay, which can fully decode the received confidential signal and then forward it to the next legitimate node. Meanwhile, at each hop, the eavesdropper also attempts to decode the message over an eavesdropper channel. On the other hand, each relay operates as a jammer mode to generate intentional interference to degrade the eavesdropper link. And all the ground destination users are deployed randomly following a homogeneous PPP based on stochastic geometry. Here, it is assumed that each node has only one antenna. In the long distance communication between the satellite and the terrestrial terminal, masking effect caused by severe shadowing and heavy obstacles (such as clouds, hills, and mountains) will make the LOS communication unstable even unavailable, and the performance of the satellite network will be affected seriously [19, 21]. Therefore, in view of masking effect and heavy fading, we assume that the direct link between S and D as well as between S and E is unavailable [12, 30, 31]. The legitimate link \( (S \rightarrow R_l \rightarrow D) \) and wiretap link...
(R_l \rightarrow E) are assumed to undergo Shadowed-Rician fading while jamming link follows Rayleigh fading. (Here, the statistical characterization for fading channels of terrestrial link can be changed with the parameter variation of Shadowed-Rician fading distribution.) All the receivers are affected by additive white Gaussian noise (AWGN) with zero mean and variance.

Without loss of generality, the total communication is divided into l hops.

In the first hop, the satellite source transmits its signal $x_s(t)$ with $E[|x_s(t)|^2] = 1$ to the first relay $R_1$. Then, the relay forwards its received signal $\{x_l(t)\}_{l=1}^{L-1}$ with $E[|x_l(t)|^2] = 1$ to the next relay until the destination in the next hops. During the next periods, each relay performs both as a relay and a jammer, so it can fully decode the received signal and then forward the signal to the next node and use some of its available power to transmit jamming signal simultaneously. Meanwhile, the eavesdropper also attempts to decode the signal. For simplicity, we assume that the intended receiver has an a priori knowledge of the artificial jamming signal and hence is able to eliminate the effects while decoding the original signal [32]. So all the jamming signals are well known by the next relay or the destination, and the signal received at the relay or the destination at hop $l$ is given as

$$y_d = \sqrt{P_{l-1}} h_{d,l} x_{s_l}(t) + n_{d,l} \quad (1 \leq l \leq L),$$

where $P_{l-1}$ is the transmission power ($P_s$ being the transmission power at $S$) and $h_{d,l}$ represents the channel coefficient between $R_{l-1} \rightarrow R_l(D)$ ($h_{d,0}$ corresponding to $S \rightarrow R_1$), while $n_{d,l}$ is the AWGN variable at the destination.

Here, for simplicity, we assume that the eavesdropper cannot do joint decoding, which can be realized by using randomized code books at each hop to confuse the eavesdropper in practice [26, 32]. Therefore, the eavesdropper receives the signal only from $R_{l-1}$ at hop $l$, and considering the unavailability between $S$ and $E$ as well as the jamming signal, the signal received at the eavesdropper at hop $l$ can be obtained as

$$y_{ej} = \sqrt{P_{l-1}} h_{ej} x_{s_{l-1}}(t) + \sqrt{P_{j,l-1}} h_{j,l} x_{s_l}(t) + n_{d,l} \quad (2 \leq l \leq L),$$

(2)
where \( P_{j,l-1} \) is the jamming power at \( R_{l-1} \), \( h_{d,l} \) and \( h_{j,l} \) denote the, respectively, channel coefficient of wiretap and jamming link between \( R_{l-1} \rightarrow E \), and \( n_{e,l} \) is the AWGN variable at the eavesdropper.

Thus, the instantaneous received SNRs at \( R_l(D) \) and \( E \) can be expressed as

\[
\gamma_{d,l} = \frac{P_{l-1}}{\sigma^2} |h_{d,l}|^2 = \eta_d |h_{d,l}|^2, \quad (1 \leq l \leq L),
\]

\[
\gamma_{e,l} = \frac{P_{l-1}}{P_{j,l-1}} |h_{j,l}|^2 \gamma_{e,l-1} \gamma_{c,l} + 1, \quad (2 \leq l \leq L),
\]

where \( \eta_{e,l} = \eta_d |h_{d,l}|^2 \) and \( \gamma_{e,l} = \eta_d |h_{d,l}|^2 \), with \( \eta_d = P_{l-1}/\sigma^2 \) and \( \eta_e = P_{j,l-1}/\sigma^2 \).

### 2.2. Channel Model

According to most of the related works, such as [19, 28], the legitimate link and wiretap link follow the independent shadowed-Rician distribution, and the PDF of \( |h|^2 \), \( \rho = \{s, e\} \) (s, e, respectively, corresponding to the legitimate link and wiretap link), is given by

\[
f_{\rho}(\gamma) = a_\rho \sum_{k=0}^{m_\rho} \zeta(k)x^k e^{-((\beta^-_{\rho} - \delta_\rho)/\eta_\rho)x},
\]

where \( a_\rho = (2b_\rho m_\rho)(2b_\rho m_\rho + \Omega_\rho)^{-m_\rho/2}b_\rho \), \( \beta^-_\rho = \Omega_\rho/(2b_\rho m_\rho + \Omega_\rho) \), and \( \zeta(k) = (-1)^k(1 - m_\rho)\delta_\rho^k (k!)^2 \), with \( b_\rho \), \( m_\rho \), and \( \delta_\rho \) being the multipath components, the fading severity parameter, and the average power of LOS, respectively, and \( (\cdot)_n \) being the Pochhammer symbol [33].

After applying the transformation of variable, the PDF of \( \gamma_\rho \) is given by

\[
f_{\gamma_\rho}(x) = a_\rho \sum_{k=0}^{m_\rho-1} \frac{\zeta(k)}{(\eta_\rho)_k} x^{k+1} e^{-((\beta^-_{\rho} - \delta_\rho)/\eta_\rho)x},
\]

By integrating the PDF in Equation (6), the CDF of \( \gamma_\rho \) can be given as

\[
F_{\gamma_\rho}(x) = 1 - a_\rho \sum_{k=0}^{m_\rho-1} \frac{\zeta(k)}{(\eta_\rho)_k} \frac{k!}{m_\rho+1} \left( \frac{\beta^-_{\rho} - \delta_\rho}{\eta_\rho} \right)^{-(k+1)-p} x^p e^{-((\beta^-_{\rho} - \delta_\rho)/\eta_\rho)x}.
\]

For the jamming link, the channel coefficient \( |h_{j,l}| \) follows Rayleigh fading distribution (Rayleigh distributions are usually used to model multipath fading without LOS paths. For simplicity, we assumed Rayleigh fading for the jamming link. And other fading models are applicable here.) with the CDF and PDF of \( \gamma_{j,l} \) given, respectively, by

\[
F_{\gamma_{j,l}}(x) = 1 - e^{-x/\Omega_{j,l}},
\]

\[
f_{\gamma_{j,l}}(x) = \frac{1}{\Omega_{j,l}} e^{-x/\Omega_{j,l}},
\]

where \( \Omega_{j,l} \) is the average SNR of the jamming link.

### 3. Performance Analysis

In this subsection, the exact closed-form SOP expression is deduced, the asymptotic behavior of the SOP is analysed, and the throughput of the considered system is discussed.

#### 3.1. SOP Analysis

We start with the instantaneous capacity of the legitimate link and the wiretap link at hop \( l \), which is given by

\[
C_{d,l} = \frac{1}{L} \log_2 \left( 1 + \gamma_{d,l} \right), \quad (1 \leq l \leq L),
\]

\[
C_{e,l} = \frac{1}{L} \log_2 \left( 1 + \gamma_{e,l} \right), \quad (2 \leq l \leq L).
\]

The achievable secrecy capacity of the network is defined as the difference between the capacity of the legitimate link and the wiretap link. Therefore, the secrecy capacity at hop \( l \) is expressed as

\[
C_{sd} = [C_{d,l} - C_{e,l}]^+ = \left[ \frac{1}{L} \log_2 \left( \frac{1 + \gamma_{d,l}}{1 + \gamma_{e,l}} \right) \right]^+, \quad (2 \leq l \leq L),
\]

where \([x]^+ = \max(x, 0)\). To facilitate the analysis, we denote the secrecy SNR of hop \( l \) by \( \gamma_l = (1 + \gamma_{d,l})/(1 + \gamma_{e,l}) \) and Equation (11) can be expressed as

\[
C_{sd} = \left[ \frac{1}{L} \log_2 \gamma_l \right]^+, \quad (2 \leq l \leq L).
\]

For multihop DF relaying, secrecy outage of the network occurs whenever the data transmission in any hop is either unsuccessfully decoded or imperfectly secure. Given the assumption that the direct link between \( S \) and \( D \) is unavailable and considering the fact that the secrecy outage decisions are taken on each hop, the secrecy SNR of the network can be expressed as

\[
\gamma_{sys} = \min_{2 \leq l \leq L} \{ \gamma_l, \gamma_1 \},
\]

where \( \gamma_1 = \gamma_{d,1} \).

As can be seen, the form is similar to that of conventional multihop DF relay networks. However, secrecy SNR is used here instead of instantaneous SNR. It is due to the fact that the system secrecy performance is dominated by the weakest hop in view of security.

Thus, we can obtain the secrecy capacity as

\[
C_{sys} = \min_{2 \leq l \leq L} \{ C_{s,1}, C_{s,d} \}.
\]
secrecy capacity $C_{\text{sys}}$ is lower than a predefined secrecy rate $\gamma_{th}$, namely,
\[
P_{\text{sec}} = \Pr \left( C_{\text{sys}} < \gamma_{th} \right),
\]
which can be expressed as
\[
P_{\text{sec}} = \Pr \left( \gamma_{th} < \gamma \right).
\]
where $\gamma_{th} = 2^{L_{\text{th}}}$.

Assuming that all $\gamma_i$ are independent of each other and invoking Equation (13) into Equation (16), the SOP of the network can be obtained as
\[
P_{\text{sec}} = 1 - \left[1 - F_{\gamma_i}(\gamma_{th})\right] \prod_{i=2}^{L-1} \left[1 - F_{\gamma_i}(\gamma_{th})\right] \prod_{i=1}^{L} \left[1 - F_{\gamma_i}(\gamma_{th})\right].
\]
(17)

To proceed further, we require $F_{\gamma_i}(\gamma_{th})$, $P_{\gamma_i}(\gamma_{th})$, and $F_{\gamma_i}(\gamma_{th})$, respectively.

According to Equation (7), $F_{\gamma}(\gamma_{th})$ can be obtained as
\[
F_{\gamma}(\gamma_{th}) = 1 - \alpha \sum_{k=0}^{m-1} \zeta(k) \left( \frac{\beta - \delta}{\eta} \right)^{(k+1)} \eta^k e^{-(\beta - \delta, \eta)}.
\]
(18)

Then, we need to express the CDF of $\gamma_t$.

**Theorem 2.** The CDF of $\gamma_t$ can be expressed as Equation (19), where $\Phi = ((\beta - \delta) / \eta) \gamma_{th} + ((\beta - \delta) / \eta) \gamma$ and $\delta^t = \cos \left( \frac{(2i - 1)\pi}{2N} \right)$.

\[
F_{\gamma}(\gamma_{th}) = 1 - \alpha \sum_{k=0}^{m-1} \zeta(k) \left( \frac{\beta - \delta}{\eta} \right)^{(k+1)} \eta^k e^{-(\beta - \delta, \eta)}.
\]
(19)

**Proof.** See Appendix A.

In the last hop, the channel coefficient $h_{d,L}$ between the last relay $y_{L-1}$ and the destination user $D$ is denoted as
\[
h_{d,L} = \frac{h^*_{d,L}}{\sqrt{1 + d^2}},
\]
(20)

where $d$ represents the distance between the last relay $y_{L-1}$ and the user $D$, $\nu$ denotes the path loss exponent, and the coordinates of $y_{L-1}$ and the user $D$ are symbolized by $(0, 0, h)$ and $(x, y, 0)$. Hence, the distance is represented as
\[
d = \sqrt{x^2 + y^2 + h^2}.
\]
(21)

As can be seen the distance is related to the location of the last relay $y_{L-1}$ and the user $D$. Assuming that all users are modeled independently and identically distributed in the area following a homogeneous PPP [2], denoted by $A$, the PDF of $A$ is given by
\[
f_A(A) = \frac{1}{\pi R^2},
\]
(22)

where $R$ is the radius of the area.

**Theorem 3.** Based on stochastic geometry, the CDF of $h_{d,L}$ is given by
\[
F_{h_{d,L}}(x) = 1 - \frac{2}{R^2} \alpha \sum_{k=0}^{m-1} \zeta(k) \sum_{p=0}^k \frac{k!}{p!} \left( \frac{t}{1/\nu} \right)^p \left( \frac{\beta - \delta}{\eta} \right)^{-(k+1)}
\]
\[
\cdot \sum_{v=0}^\infty \left( \frac{\beta - \delta}{\eta} \right)^{-(k+1)} \left( \frac{t}{1/\nu} \right)^p \left( \frac{\beta - \delta}{\eta} \right)^{-(k+1)}
\]
\[
\cdot \left( \left( R^2 + 2h^2 \right)^{-(\nu + \nu + 2)} \right) e^{-\left( (\beta - \delta, \eta)\right) x^{\nu + p}}.
\]
(23)

**Proof.** Combining Equations (7) and (22), the CDF of $|h_{d,L}|^2$ is derived as Equation (24), where $\gamma(\cdot, \cdot)$ represents the lower incomplete Gamma function.

\[
F_{|h_{d,L}|}(x) = \int \left[ \left( F_{|h_{d,L}|}(x(1 + d^2)) \right) f_A(A) dA \right]_{h}^{\sqrt{R^2 - h^2}}
\]
\[
\cdot \left( 1 - \alpha \sum_{k=0}^{m-1} \zeta(k) \sum_{p=0}^k \frac{k!}{p!} \left( \frac{t}{1/\nu} \right)^p \left( \frac{\beta - \delta}{\eta} \right)^{-(k+1)} x^p \right)
\]
\[
\cdot \left( 1 + r^p \right) e^{-\left( (\beta - \delta, \eta)\right) x^{\nu + p}}
\]
\[
\cdot \left( \left( R^2 + 2h^2 \right)^{-(\nu + \nu + 2)} \right) e^{-\left( (\beta - \delta, \eta)\right) x^{\nu + p}}.
\]
(24)
By derivation of Equation (23), the PDF of $\gamma_{dl}$ can be obtained as

$$f_{\gamma_{dl}}(x) = \xi(k, p, t, n) e^{-(k-\delta) t/n} x^{n-1} (1 - x)^{n-1}$$

(25)

where

$$\xi(k, p, t, n) = \frac{2}{R^2} \alpha_x \sum_{k=0}^{m-1} \frac{\zeta(k)}{k!} \frac{k!}{p!} \left( \frac{p}{t} \right)^n (-1)^n (R^2 + h^2)^{(n+v+2)/2 - h^2}.$$ 

(26)

**Theorem 4.** The CDF of $\gamma_L$ can be obtained as Equation (29), where

$$\Xi_1 = -\frac{\beta_s - \delta_s}{\eta_s} \left( \frac{\delta_i + 1}{2} \right) \gamma_0^{p+1} (k_i + p + n + 1)! \left( \frac{\beta_s - \delta_s - 1}{\eta_s} + \frac{\beta_s - \delta_s}{\eta_s} \right)^{-k_i - p - 2},$$

(27)

**Proof.** See Appendix B.

**Theorem 5.** The SOP of the network can be formulated as

$$P_{sec} = 1 - \alpha_x \sum_{k=0}^{m-1} \frac{\zeta(k)}{(n+1) k!} \left( \frac{\eta_s}{\eta_s} \right) \gamma_0^p e^{-(k-\delta) \eta_s \gamma_s} \left( \frac{\beta_s - \delta_s}{\eta_s} \right)^{k-1} \gamma_0^p e^{-(k-\delta) \eta_s \gamma_s} \left( \frac{\beta_s - \delta_s}{\eta_s} \right)^{k-1}$$

$$+ \frac{\pi \alpha_s}{2N} \sum_{i=0}^{N} e^{-2\left(k_i \gamma_s \left(\frac{\beta_s - \delta_s}{\eta_s}\right)^{k_i - 1}\right)} + \frac{\pi \alpha_s}{2N} \sum_{i=0}^{N} e^{-2\left(k_i \gamma_s \left(\frac{\beta_s - \delta_s}{\eta_s}\right)^{k_i - 1}\right)}$$

$$\times \alpha_x \sum_{k=0}^{m-1} \frac{\zeta(k)}{k!} \frac{k!}{p!} \left( \frac{p}{t} \right)^n (-1)^n \left( \frac{\beta_s - \delta_s}{\eta_s} \right)^{k-1} \gamma_0^p \left( \frac{\beta_s - \delta_s}{\eta_s} \right)^{k-1} \gamma_0^p \left( \frac{\beta_s - \delta_s}{\eta_s} \right)^{k-1}$$

$$\times \left( R^2 + h^2 \right)^{(n+v+2)/2 - h^2} \left( \frac{\eta_s}{\eta_s} \right)^{k-1} \gamma_0^p \left( \frac{\beta_s - \delta_s}{\eta_s} \right)^{k-1}$$

(30)

**Proof.** Invoking Equations (18), (19), and (29) into Equation (17), Equation (30) can be obtained.

3.2. Asymptotic Behavior. To get better insights on the secrecy performance of the network, the asymptotic secrecy outage behavior at high SNR region is investigated. Here, we examine the asymptotic SOP analysis at high SNR region ($\eta_s \rightarrow \infty$).

$$\Xi_2 = (n + p) \left( \frac{\delta_i + 1}{2} \right) \gamma_0^p n (k_i + p + n)! \left( \frac{\beta_s - \delta_s}{\eta_s} \right)^{k_i - p - 1}$$

(28)

**Corollary 6.** The diversity order of the network at high SNR region can be obtained easily as

$$d = \lim_{\eta_s \rightarrow \infty} \frac{\log \left( P_{sec}^\infty \right)}{\log \eta_s} = 1.$$ 

(31)

**Proof.** As in [19], at high SNR region, assuming $\eta_s \rightarrow \infty$ and applying the Maclaurin series expansion of the exponential
function \[33\], the PDF \( f_{\gamma_p} \) can be approximated as

\[
 f_{\gamma_p}(x) = \frac{\alpha_p}{\eta_p}
\]

and by integrating Equation (32), the asymptotic behavior of \( F_{\gamma_p} \) can be given as

\[
 F_{\gamma_p}(x) = \frac{\alpha_p x}{\eta_p}.
\]

Therefore, we can derive \( F_{\gamma_0}(y_0) = (\alpha_s/\eta_s)y_0 \) and

\[
 F_{\gamma_p}(y_0) = \frac{\alpha_p\alpha_s y_0}{\eta_s} \left( 1 - e^{(\gamma_p/\eta_s)} \right) \frac{\pi}{2N} \sum_{i=0}^{N} e^{-2i(\gamma_p/\eta_s)} \sqrt{1 - \delta_i^2}
\]

\[
 \cdot \prod_{k=0}^{m-1} \frac{k!(k+1)!}{\eta_s^{k+1}} \left( \frac{\beta - \delta_i}{\eta_s} \right)^{-k_i-2}, (2 \leq l \leq L).
\]

Now, invoking \( F_{\gamma_0}(y_0) \) and Equation (34) into Equation (17), the asymptotic expression for the SOP can be derived as

\[
 P_{\text{asym}} = 1 - \left( 1 - \frac{\alpha_s}{\eta_s} \right) \left( 1 - \frac{\alpha_p}{\eta_p} \right) \left( 1 - e^{(\gamma_p/\eta_p)} \right) \pi \sum_{i=0}^{\infty} e^{-i(\gamma_p/\eta_p)} \sqrt{1 - \delta_i^2}
\]

\[
 \cdot \sum_{k=0}^{m-1} \frac{k!(k+1)!}{\eta_s^{k+1}} \left( \frac{\beta - \delta_i}{\eta_s} \right)^{-k_i-2} L^{-1}.
\]

On invoking Equation (35) into Equation (31) and doing some algebraic manipulations, the diversity order of 1 can be acquired.

Remark 7. Through the asymptotic analysis of the SOP, we can reveal that the diversity order of the multihop network at high SNR region is 1. Importantly, it remains unaffected by the hops, secrecy rate, or other channel parameters.

3.3. Throughput Analysis. In order to estimate the secrecy performance of the network further, the throughput of the overall system is explored. According to [34], the throughput is defined as

\[
 R_{\text{th}} = \frac{y_{th}}{L} \times [1 - P_{\text{sec}}(y_{th})],
\]

where the constant \( 1/L \) indicates that the communication process is divided into \( L \) hops. \( y_{th} \) represents the secrecy rate, and \( P_{\text{sec}}(y_{th}) \) can be obtained from the previous section. Thus, by substituting Equation (30) into Equation (36), the analytical throughput expression of the system is derived.

4. Numerical Results

In this section, the theoretical analysis results obtained from Section 3 are presented through comparison with Monte Carlo simulations. Monte Carlo simulations are carried out in order to verify the accuracy of the theoretical derivation. In particular, the SOP and throughput analysis are examined under various channel settings. Unless otherwise stated, channel parameters of the legitimate link are the same with those of the wiretap link and the parameter settings are used as shown in Table 1 [2, 19, 27, 35, 36].

Figure 2 shows the results of the SOP versus \( \eta_s \). Figure 3 investigates the SOP performance of the network under various channel settings. The numerical results obtained from Equations (30) and (35) \((y_{th} = 0.5, \gamma_{\rho_{\Omega,\rho}} = 1 \text{ dB})\) agree well with the Monte Carlo simulation results, which confirm the correctness of the analysis. From the figure, it can be observed that the curves of the asymptotic SOP almost overlap with the analytical ones at the moderate and high SNR region. Moreover, it is obvious that the SOP performance of the network under average shadowing scenarios is better than that under heavy shadowing scenarios and it gets worse with the increasing hops. This is because the communication distance gets increasing with the increasing hops. This figure also indicates that the achievable diversity order does not change with different hops.

Figure 3 investigates the SOP performance of the network versus hops for \( \eta_s = 20, 30, 40 \) under heavy and average shadowing scenarios. Herein, we set \( y_{th} = 0.1 \) and \( \gamma_{\rho_{\Omega,\rho}} = 1 \text{ dB} \). It is obviously found that theory results sufficiently coincide with the Monte Carlo simulation results. And as can be seen from Figure 3, the SOP performance of the network is getting worse with the increasing severity of the channel fading scenario and it gets better with the decrease of the hops \( L \).
Figure 2: SOP versus $\eta_s$ for different hops.

Figure 3: SOP versus hops for different $\eta_s$. 
Figure 4: SOP versus $\eta_s$ for different $\gamma_{th}$.

Figure 5: SOP versus $\eta_s$ for different $\gamma_{je,l}$.
Figure 6: SOP versus $\eta_s$ in different shadowing scenarios.

Figure 7: System throughput versus $\eta_s$ for different hops.
Figure 4 plots the results of the SOP versus $\eta_l$ for different secrecy rate $Y_{th}$ under heavy and average shadowing scenarios of shadowing-Rician fading. Here, it is assumed that the received signal from the satellite experiences 2 hops and $Y_{th} = 1$ dB. As is expected, the SOP performance of the network gets worse with the secrecy rate increasing.

Figure 5 shows the SOP performance comparison of the network versus $\eta_l$ for different average SNR of the jamming link $Y_{je,l}$ under heavy and average shadowing scenarios of shadowing-Rician fading. Also, the performance comparison of HSTRN without jamming is presented. Here, we suppose that the communication process experiences 2 hops and $Y_{th} = 0.1$. As shown in the figure, the SOP performance of the network with jamming is better than that without jamming obviously. And when the average SNR of the jamming link $Y_{je,l}$ gets increasing, the SOP performance of the network improves correspondingly. This can be attributed to the jammer. The stronger the jamming signal gets, the weaker the wiretap signal becomes. Hence, the jammer has a great effect on the SOP performance of the network.

Figure 6 depicts the SOP performance comparison of the network versus $\eta_l$ based on different channel settings of the legitimate link and wiretap link. Here, we still set $Y_{th} = 0.1$, $Y_{je,l} = 1$ dB, and $L = 2$. As can be seen from the figure, when the legitimate link is under heavy shadowing scenarios ($m_1 = 1$) and the wiretap link is under average shadowing ($m_1 = 5$), the SOP performance of the network is the worst. While the legitimate link is under average shadowing scenarios ($m_1 = 5$) and the wiretap link is under heavy shadowing ($m_1 = 1$), the network has the best SOP performance.

Figure 7 presents the system throughput versus $\eta_l$ ($Y_{th} = 0.1$, $Y_{je,l} = 1$ dB). As can be noted, the throughput increases with $\eta_l$ increasing and then trends to a fixed constant based on the same hop. This can be explained by the fact that SOP will approach to zero at high SNR region. Also, the throughput of system degrades with hops increasing, and it is better under average shadowing scenarios than that under heavy shadowing scenarios, which is consistent with the SOP performance seen from Figure 2.

5. Conclusions

In this work, the secrecy analysis of a multihop DF HSTRN with jamming has been investigated. Considering shadowed-Rician fading for legitimate link and wiretap link while considering Rayleigh fading for jamming link, the accurate SOP formula of the considered network has been derived. The asymptotic behavior of the SOP expression at high SNR region is explored, and the throughput of the system is discussed. Finally, simulation results are given as verification of the theoretical results and illustrate that some key system parameters have great impacts on the SOP performance of the considered network. The results reveal that the hops and the jammer play important parts in the secrecy performance of the multihop DF HSTRN with jamming. In the future, multiantenna satellite, multiantenna relay, and multiple eavesdroppers in such system could be our further research.

Appendix

A. Proof of Theorem 2

After the approximation $(1 + x)/(1 + y) \approx x/y$ and the substitution of Equation (4), $Y_l$ can be obtained as

$$Y_l \approx \frac{Y_{dl} (Y_{je,l} + 1)}{Y_{rec,l}}. \quad (A.1)$$

Therefore, $F_{Y_l}(Y_0)$ can be expressed as

$$F_{Y_l}(Y_0) = \text{Pr} \left( \frac{Y_{dl} (Y_{je,l} + 1)}{Y_{rec,l}} < Y_0 \right) = \text{Pr} \left( A < Y_0 Y_{rec,l} \right)$$

$$= \int_0^{Y_0} F_A(Y_0 Y_{rec,l}) f_{Y_{rec,l}}(Y_{rec,l}) dY_{rec,l}, \quad (A.2)$$

de where $A = Y_{dl} (Y_{je,l} + 1)$.

To proceed, we require $F_A(z)$, and it is derived as

$$F_A(z) = \text{Pr} (A < z) = \int_0^z F_{Y_{rec,l}} \left( \frac{z}{Y_{dl} - 1} \right) f_{Y_{rec,l}}(Y_{rec,l}) dY_{rec,l} \quad (A.3)$$

Invoking Equations (6) and (8) into Equation (A.3), doing some algebra processing and applying the approximation of the Gaussian-Chebyshev quadrature [37], $F_A(z)$ can be formulated as

$$F_A(z) \approx 1 - \alpha_s \sum_{p=0}^{m_1-1} \xi(k) \left( \frac{\beta_k - \delta_k}{\eta_l} \right)^{(k+1)p} \cdot 2^p e^{-((\beta_k - \delta_k)/\eta_l)z} - \frac{\pi \alpha_s}{2N} \sum_{p=0}^{m_2-1} e^{-2((\tau_{rec,l} / 2) + 1)} ((1/\tau_{rec,l})$$

$$+ \sum_{p=0}^{m_2-1} \xi(k) \left( \frac{\delta_k + 1}{2} \right)^p \left( 1 - \frac{1}{\delta_k + 1} \right), (A.4)$$

Now, substituting Equations (A.4) and (6) into Equation (A.2), Equation (19) can be obtained.

B. Proof of Theorem 4

Like Equation (A.2), $F_{Y_l}(Y_0)$ can be expressed as

$$F_{Y_l}(Y_0) = \int_0^{Y_0} F_A \left( Y_0 Y_{rec,l} \right) f_{Y_{rec,l}}(Y_{rec,l}) dY_{rec,l} \quad (B.1)$$

where $A_L = Y_{dl} (Y_{je,l} + 1)$. 

11
And $F_{A_L}(z)$ can be derived as

$$F_{A_L}(z) = \Pr (A_L < z) = \int_0^z F_{Y_d,l}(y_d,l) dy_d,l.$$  

(B.2)

Invoking Equations (25) and (8) into Equation (B.2), doing some algebra processing like Equation (A.4), $F_{A_L}(z)$ can be obtained as

$$F_{A_L}(z) = 1 - \frac{2\pi}{R^2} \sum_{k=0}^{m-1} \sum_{p=0}^k \sum_{t=0}^p \frac{\zeta(k)k!}{p!} \int_0^\infty \int_0^\infty \left( \frac{1}{\eta_i} \right)^{p+1} \left( -1 \right)^{p+1} e^{-\frac{\beta_i \psi_i}{\eta_i}} e^{-\left( \frac{2\pi}{R^2} \right)^{1/2} (t+s)/(\eta_i^{1/2})^2} \left( 1 - \delta_i - \delta_i^2 \right)^{-1/2} \Delta_i^{1/2} \right) \left( 1 - \frac{\beta_i - \delta_i}{\eta_i} \right) \left( \frac{\delta_i + 1}{2} \right)^{p+1} e^{-\frac{2\pi}{R^2} \left( \frac{\beta_i - \delta_i}{\eta_i} \right) \left( \frac{\delta_i + 1}{2} \right)^2 z^{p+1}} \right)$$  

(B.3)

Then, substituting Equations (B.3) and (6) into Equation (B.1), doing some algebra processing, Equation (29) can be obtained.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (41474021 and 41931075), Key scientific and technological project of Henan provincial (212102310436), Fundamental Research Funds for the Universities of Henan Provincial (NSFRF210329), and doctoral fund of Henan Polytechnic University (B2021-18).

References

[1] A. Vanelli-Coralli, G. Corazza, G. Karagiannidis, T. Mathiopoulos, and S. Scalise, "Satellite communications: research trends and open issues," in 2007 International Workshop on Satellite and Space Communications, pp. 71–75, Salzburg, Austria, 2007.

[2] X. Li, Q. Wang, H. Peng et al., "A unified framework for HS-UAV NOMA networks: performance analysis and location optimization," IEEE Access, vol. 8, pp. 13329–13340, 2020.

[3] K. Guo, D. Guo, Y. Huang, X. Wang, and B. Zhang, "Performance analysis of a dual-hop satellite relay network with hardware impairments," in 2016 25th Wireless and Optical Communication Conference (WOCC), pp. 1–5, Chengdu, China, 2016.

[4] S. W. Peters and R. W. Heath, “The future of wireless multi-hop relaying with IEEE 802.16j,” IEEE Communications Magazine, vol. 47, no. 1, pp. 104–111, 2009.

[5] X. Li, J. Li, Y. Liu, Z. Ding, and A. Nallanathan, "Residual transceiver hardware impairments on cooperative NOMA networks," IEEE Transactions on Wireless Communications, vol. 19, no. 1, pp. 680–695, 2020.

[6] X. Li, J. Li, and L. Li, “Performance analysis of impaired SWIPT NOMA relaying networks over imperfect Weibull channels,” IEEE Systems Journal, vol. 14, no. 1, pp. 669–672, 2020.

[7] X. Li, M. Zhao, M. Zeng et al., "Hardware impaired ambient backscatter NOMA systems: reliability and security," IEEE Transactions on Communications, vol. 69, no. 4, pp. 2723–2736, 2021.

[8] X. Li, "Secrecy analysis of ambient backscatter NOMA systems under I/Q imbalance," IEEE Transactions on Vehicular Technology, vol. 69, no. 10, pp. 12286–12290, 2020.

[9] X. Li, Q. Wang, Y. Liu, T. A. Tsiftsis, Z. Ding, and A. Nallanathan, "UAV-aided multi-way NOMA networks with residual hardware impairments," IEEE Wireless Communications Letters, vol. 9, no. 9, pp. 1538–1542, 2020.

[10] B. Evans, M. Werner, E. Lutz et al., “Integration of satellite and terrestrial systems in future multimedia communications,” IEEE Wireless Communication, vol. 12, no. 5, pp. 72–80, 2005.

[11] S. Kim, H. W. Kim, K. Kang, and D. S. Ahn, "Performance enhancement in future mobile satellite broadcasting services," IEEE Communications Magazine, vol. 46, no. 7, pp. 118–124, 2008.

[12] K. An, M. Lin, and T. Liang, "On the performance of multiuser hybrid satellite-terrestrial relay networks with opportunistic scheduling," IEEE Communications Magazine, vol. 19, no. 10, pp. 1722–1725, 2015.

[13] Y. Bu, M. Lin, K. An, J. Ouyang, and C. Yuan, "Performance analysis of hybrid satellite-terrestrial cooperative systems with fixed gain relaying," Wireless Personal Communications, vol. 89, no. 2, pp. 427–445, 2016.

[14] Digital video broadcasting (DVB); system specifications for satellite services to handheld services (SH) below 3 GHz, European Telecommunications Standards Institute (ETSi), 2008, ETSI EN 102 585 V1.1.2.

[15] X. Li, M. Liu, J. Deng, J. Li, and Q. Yu, "Power beacon assisted wireless power cooperative relaying using NOMA with hardware impairments and imperfect CSI," International Journal of Electronics and Communications, vol. 108, pp. 275–286, 2019.

[16] V. K. Sakarellos, C. Kourogiorias, and A. D. Panagopoulos, "Cooperative hybrid land mobile satellite-terrestrial broadcasting systems: outage probability evaluation and accurate simulation," Wireless Personal Communications, vol. 79, no. 2, pp. 1471–1481, 2014.

[17] K. An, M. Lin, T. Liang et al., "Performance analysis of multi-antenna hybrid satellite-terrestrial relay networks in the presence of interference," IEEE Transactions on Communications, vol. 63, no. 11, pp. 4390–4404, 2015.
[18] A. D. Wyner, ”The wire-tap channel,” *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[19] V. Bankey and P. K. Upadhyay, ”Physical layer secrecy performance analysis of multi-user hybrid satellite-terrestrial relay networks,” *CSI Transactions on ICT*, vol. 6, no. 2, pp. 187–193, 2018.

[20] Q. Huang, M. Lin, K. An, J. Ouyang, and W. P. Zhu, ”Secrecy performance of hybrid satellite-terrestrial relay networks in the presence of multiple eavesdroppers,” *IET Communications*, vol. 12, no. 1, pp. 26–34, 2018.

[21] V. Bankey and P. K. Upadhyay, ”Physical layer security of multiuser multirelay hybrid satellite-terrestrial relay networks,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2488–2501, 2019.

[22] K. Guo, K. An, B. Zhang, Y. Huang, and D. Guo, ”Physical layer security for hybrid satellite terrestrial relay networks with joint relay selection and user scheduling,” *IEEE Access*, vol. 6, pp. 55815–55827, 2018.

[23] S. Yan, X. Wang, Z. Li, B. Li, and Z. Fei, ”Cooperative jamming for physical layer security in hybrid satellite terrestrial relay networks,” *China Communications*, vol. 16, no. 12, pp. 154–164, 2019.

[24] Y. Yan, B. Zhang, D. Guo, S. Li, H. Niu, and X. Wang, ”Joint beamforming and jamming design for secure cooperative hybrid satellite-terrestrial relay network,” in 2016 25th *Wireless and Optical Communication Conference (WOCC)*, pp. 71–75, Chengdu, China, 2016.

[25] J. Ye, C. Zhang, G. Pan, Y. Chen, and Z. Ding, ”Secrecy analysis for spatially random UAV systems,” in 2018 *IEEE Globecom Workshops (GC Wkshps)*, pp. 1–6, Abu Dhabi, United Arab Emirates, 2018.

[26] X. He and A. Yener, ”End-to-end secure multi-hop communication with untrusted relays,” *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 1–11, 2013.

[27] V. Bankey, P. K. Upadhyay, D. B. da Costa, P. S. Bithas, A. G. Kanatas, and U. S. Dias, ”Performance analysis of multi-antenna multiuser hybrid satellite-terrestrial relay systems for mobile services delivery,” *IEEE Access*, vol. 6, pp. 24729–24745, 2018.

[28] A. Abdi, W. C. Lau, M. S. Alouini, and M. Kaveh, ”A new simple model for land mobile satellite channels: first- and second-order statistics,” *IEEE Transactions on Wireless Communications*, vol. 2, no. 3, pp. 519–528, 2003.

[29] M. Lin, Y. Jiang, J. Ouyang, and K. An, ”The performance of a hybrid satellite-terrestrial cooperative networks with interferences,” *Acta Electronica Sinica*, vol. 46, no. 1, pp. 8–14, 2018.

[30] A. Pandey and S. Yadav, ”Physical layer security in cooperative AF relaying networks with direct links over mixed Rayleigh and double-Rayleigh fading channels,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 10615–10630, 2018.

[31] L. Fan, N. Yang, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, ”Exploiting direct links for physical layer security in multiuser multirelay networks,” *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 3856–3867, 2016.

[32] E. R. Alotaibi and K. A. Hamdi, ”Secure relaying in multihop communication systems,” *IEEE Wireless Communications Letters*, vol. 20, no. 6, pp. 1120–1123, 2016.

[33] I. S. Gradshteyn and I. M. Ryzhik, *Tables of Integrals, Series and Products*, Academic Press, New York, NY, USA, 6th edition, 2000.