Relay Selection for Improving Physical-Layer Security in Hybrid Satellite-Terrestrial Relay Networks

Weifeng Cao, Yulong Zou, Senior Member, IEEE, Zhen Yang, and Jia Zhu

Abstract—In this paper, a hybrid satellite-terrestrial relay network (HSTRN) interconnecting a satellite and multiple terrestrial nodes is considered, where communication is achieved by the satellite transmitting information to a destination through multiple relays at the appearance of an eavesdropper attempting to intercept the transmissions from both the satellite and relays. We present the single-relay selection and multi-relay selection as well as round-robin scheduling schemes to investigate the physical-layer security of this considered HSTRN by adopting the decode-and-forward (DF) relay strategy. Specifically, in single-relay selection scheme, a relay is chosen as the “best” relay who has the maximum instantaneous capacity of relay-destination channel out of the decoding relay set, which is composed of all the relays capable to decode the received signals from satellite successfully. By contrast, in multi-relay selection scheme, all relays of the decoding relay set are invoked simultaneously to aid the satellite communicating with the destination. Moreover, suppose that only the main channels’ state information is known while the wiretap channels’ is unavailable due to the passive eavesdropper, we analyze the secrecy performance in accordance with secrecy outage probability (SOP) of the HSTRN by driving out the closed-form expressions for the single-relay selection and baseline round-robin scheduling schemes, as well as by computer simulations for multi-relay selection scheme. Numerical results show that the two relay selection schemes generally outperform the round-robin scheduling baseline scheme in the light of improving the secrecy performance of HSTRN even when the legitimate links are inferior to the wiretap links.

Index Terms—Hybrid satellite-terrestrial relay network, physical-layer security, secrecy outage probability, relay selection

I. INTRODUCTION

AND mobile satellite (LMS) communication is a promising and ideal transmission solution for broadcasting, navigation and rescue, owing to its high data rate transmission and large area of coverage [1]-[4]. As security threats such as eavesdropping, hijacking and data corruption emerge due to the inherent property of wireless transmission, demanding requirements are further imposed on satellite communication. To address such challenges, recent advances in wireless network security have been further explored in the context of satellite-terrestrial network [5]-[6].

Traditionally, classic cryptographic techniques are utilized widely for defending transmission confidentiality, which rely on secret keys [7], [8]. While these techniques are capable of providing a certain level of transmission security, they do impose severe limitations, for example an extra computational overhead and additional system complexity. Furthermore, if an eavesdropper has extraordinary computing power, it may decrypt the cryptogram by exhaustive key search, which makes the classic cryptographic techniques flawed, thus increasing the security risk.

Alternatively, physical-layer security, which makes good use of the physical properties of wireless channels to assure the data confidentiality, is emerging as a research breakthrough of wireless network security in the last decade. Among the existing literature on physical-layer security, most of them are focusing on the terrestrial wireless networks. Whereas only limited attention has been dedicated to satellite communication security [9]-[18]. An overview of security issues in hybrid satellite networks was provided in [10], where various security attacks and their countermeasures are discussed. In [11], the authors secure transmission in hybrid satellite networks is explored in [11] on the network layer in conjunction with the transport layer. Better yet, the existing literature of [12]-[18] investigated the physical-layer security of satellite communications based on an information-theoretic understanding. More specifically, [12] aimed at maximizing the secrecy rate of satellite-terrestrial network through beamforming, whereas in [13], the secrecy performance was evaluated in a satellite system where a land mobile satellite delivers messages to a terrestrial user at the appearance of an eavesdropper at a high signal-to-noise ratio. [14] employed multiple beams to increase the spectrum reuse and system coverage, as well as designed an optimal transmit beam former which can ensure each user secure transmission with the minimum total transmit power. The authors of [15] explored network coding to realize confidential communications of satellite networks. Du et al. [16] achieved the maximum secrecy rate by employing a cooperative beamforming scheme for millimeter wave com-
communications between the satellite and terrestrial networks. Furthermore, [17] dealt with the secure transmission issues of a cognitive satellite terrestrial communication system and [18] evaluated the secrecy performance in a single relay satellite terrestrial system with multiple eavesdroppers in the light of ergodic secrecy rate.

Cooperative communication techniques [19], which rely on the terrestrial relay nodes forwarding their received information delivered by the satellite to terrestrial users in a hybrid satellite-terrestrial satellite network, are utilized for extending the network coverage and improving the transmission performance. In particular, a popular satellite communication system named as hybrid satellite-terrestrial relay network (HSTRN) was proposed in [20], refraining from the masking effect of satellite communication. Consequently, a number of techniques have been exploited to better the performance of HSTRN in terms of developing different relay protocols as well as various network architectures. In [21], Manav R. Bhatnagar et al. measured the error performance of an amplify-and-forward (AF) satellite-terrestrial relay system involved an information exchange between a satellite and a single user via a relay, considering satellite channels are described as Shadowed-Rician distribution and the channels on ground are modeled as Nakagami-m fading. In [22] and [23], the authors calculated outage probabilities of a HSTRN employing DF and AF protocols, respectively, and improved the system performance by adopting best relay selection scheme. In [24], the performance of an AF HSTRN was evaluated with the existence of interference. Furthermore, an extended network architecture composed of multi-user and multi-relay with a multi-antenna satellite was considered in [25], and the outage probability as a metric of system performance was analyzed and improved by employing the best user-relay pair selection scheme.

As discussed in [26], relaying techniques not only improve the system performance, but also show great possibility of achieving confidential communication against eavesdropping attack. However, compared with conventional terrestrial wireless networks, it is much more challenging and complicated to measure the secrecy performance of Shadowed-Rician channel. Motivated by the above discussion, we explore the physical layer properties to deal with the secure transmission of a DF HSTRN at the appearance of an eavesdropper utilizing two relay selection schemes. Our main focus is on calculating the SOP to describe the secrecy performance of a cooperative satellite-terrestrial network. The following summarizes the main contributions of this paper.

- Considering that the eavesdropper is able to intercept from both the satellite network and the terrestrial network, we develop a new framework of physical layer security in a HSTRN, where one satellite delivers signals to one terrestrial destination through multiple terrestrial relays at the appearance of one terrestrial eavesdropper. This framework is different from the system models of [14]-[18], [25], [27].
- Assuming a passive eavesdropping scenario that the CSI of wiretap links is unknown, we employ two relay selection schemes referred as both single-relay and multi-relay selection to enhance the physical-layer security of HSTRN, which is different from the work [23], [25] and [27]. Specifically, instantaneous information of eavesdropping links is supposed to be unavailable, since a passive eavesdropper is considered.
- We derive closed-form expressions under Shadowed-Rician fading of the SOP in a HSTRN for the single-relay selection and round-robin scheduling scheme. Meanwhile, the secrecy performance of multi-relay selection scheme is analyzed by computer simulations. It is much more challenging and complicated to derive the SOP in Shadowed-Rician channels than in terrestrial Rayleigh environments [28], [29]. To our best knowledge, it is the first time to develop the secrecy outage probability analysis of the relay selection schemes in a HSTRN.

The remainder of this paper is organized as follows. First, we describe the characters of a HSTRN in section II, in the context of the conventional round-robin scheduling and single-relay as well as multi-relay selection schemes. In section III, we analyze their secrecy outage probability with DF strategies. Next, computer simulation results of these schemes are discussed in section IV, and the conclusions are drawn in section V.

II. RELAY SELECTION AIDED SECURE TRANSMISSION IN HYBRID SATELLITE-TERRESTRIAL NETWORKS

A. System Model

As depicted in Fig. 1, a source node satellite $S$, multiple terrestrial relay nodes denoted by $R_i$ ($i = 1, 2, \cdots, N$), and a terrestrial node destination $D$ with the existence of an eavesdropper $E$ are considered to be involved in a DF HSTRN, where $N$ relay nodes are introduced for assisting the transmission from $S$ to $D$. Meanwhile, a terrestrial eavesdropper attempts to intercept the legitimate transmissions from both the satellite and the relays. As a result of masking effect, following [23], [24], [30], [31], suppose that the direct connection to link satellite and destination is blocked, which is a common assumption widely adopted in HSTRN literature. It is assumed that the satellite is mon-beam, and each node has a single antenna. Additionally, all the links in the network are considered to be independent and flat fading. Now, we describe the statistical characters of channels as follows.

The satellite links are characterized by the Shadowed-Rician fading model, which is a popular LMS fading channel model derived in [32]. Moreover, it has nice mathematical properties and less computational burden than other satellite models. Under Shadowed-Rician fading model, let $|h_{sj}|^2 (j \in \{r_n, e\})$ be the power channel gain from satellite to other nodes, the probability distribution function (PDF) of $|h_{sj}|^2$ can be described as

$$f_{|h_{sj}|^2}(x) = \alpha_j e^{-\beta_j x} F_1(m_j; 1; \delta_j x),$$

where

$$\alpha_j = \frac{1}{2\beta_j} \left( \frac{2\beta_j m_j}{2\beta_j m_j + 1} \right)^{m_j}, \quad \beta_j = \frac{1}{2\beta_j}, \quad \delta_j = \frac{\Omega_j}{2\beta_j (2\beta_j m_j + 1)},$$

with $\Omega_j$ and $2\beta_j$ denoting the average power of the LOS and multipath component, respectively, and $m_j$
the Nakagami parameter. Moreover, \( F_1(a; b; z) \) represents the confluent hypergeometric function \([33, \text{eq } (9.210.1)]\).

According to Eq. (1), given \( \gamma_{sj} = |h_{sj}|^2 \gamma_j \) with \( \gamma_j \) being the signal-to-noise ratio (SNR),

\[
f_{\gamma_{sj}}(x) = \frac{1}{\gamma_j} \times f_{|h_{sj}|^2}(x) = \alpha_j \frac{x^{-\frac{\alpha_j}{\gamma_j}}}{\gamma_j} F_1(m_j; 1; \frac{\delta_j x}{\gamma_j} )
\]  

is the PDF of \( \gamma_{sj} \). Employing \([33, \text{eq } (3.351.1)]\) and \([33, \text{eq } (8.350.1)]\), yields

\[
F_{\gamma_{sj}}(x) = \alpha_j \sum_{k=0}^{\infty} \frac{\Gamma(m_j + k)}{\Gamma(m_j) \Gamma(1 + k)!} \frac{\delta_j^k}{\gamma_j^k} \left( k + 1, \frac{\delta_j x}{\gamma_j} \right),
\]

which is the cumulative distribution function (CDF) of \( \gamma_{sj} \), and \( \Gamma(\cdot, \cdot) \) represents the lower incomplete Gamma function \([33, \text{eq } (8.350.1)]\).

The terrestrial links between relay to destination and eavesdropper both follow Rayleigh fading, and the power channel gain \( |h_{rt}|^2 \) \((i \in \{1, 2, \ldots, N\}, t \in \{d, e\})\) undergoes an exponential distribution with a mean of \( \sigma_{rt}^2 \), thus

\[
f_{|h_{rt}|^2}(x) = \frac{1}{\sigma_{rt}^2} e^{-\frac{x}{\sigma_{rt}^2}}, \quad x \geq 0
\]

is the PDF of \( |h_{rt}|^2 \). For convenience, we name the channels spanning from the transmission nodes (i.e. the satellite \( S \) and relay \( R_i \)) to receive nodes (i.e. the destination \( D \) and eavesdropper \( E \)) as \( S-R_i, S-E, R_i-D \) and \( R_i-E \) channel, respectively. Correspondingly, the fading coefficient of each channel can be denoted by \( h_{sr}, h_{se}, h_{rt,d}, h_{rt,e} \). Moreover, the additive white Gaussian noise (AWGN) with zero mean and variance \( N_0 \) at each receiver is denoted by \( n_p \) \((p \in \{r, d, e\})\).

According to Fig. 1, the process of a satellite sending signals to a destination through multiple DF relays involves two phases. First, the signal \( x_s \) is delivered by the satellite source at a power of \( P_s \) and a rate of \( R_s \) to the set of \( N \) terrestrial relays. In this case, the signal received at relay \( R_i \) can be given by

\[
y_{ri} = \sqrt{P_sh_{sr}}x_s + n_r.
\]

Correspondingly, the capacity of \( S-R_i \) channel can be written as

\[
C_{si} = \frac{1}{2} \log_2 \left( 1 + |h_{sr}|^2 \gamma_0 \right),
\]

where \( \gamma_0 = P_s/N_0 \). In the next phase, if a relay \( R_i \) is capable of decoding the signal \( x_s \) successfully and to be selected to forward a version of \( x_s \) with a power denoted by \( P_r \), the signal arrived at destination can be written as

\[
y_{id} = \sqrt{P_r h_{ri,d}}x_s + n_d.
\]

Hence,

\[
C_{id} = \frac{1}{2} \log_2 \left( 1 + |h_{ri,d}|^2 \gamma_1 \right)
\]

is the capacity of \( R_i-D \) channel, and \( \gamma_i = P_r/N_0 \). Meanwhile, the eavesdropper is capable of tapping the transmission of each phase, as a result, the signals arrived at the eavesdropper are given by

\[
y_{ie}^1 = \sqrt{P_sh_{se}}x_s + n_e,
\]

\[
y_{ie}^2 = \sqrt{P_r h_{re}}x_s + n_e.
\]

Accordingly, under the assumption of the selection combining (SC), the maximum achievable rate at the eavesdropper received from the satellite and the relays is viewed as the transmission capacity of the wiretap channel, which can be written as

\[
C_{ie} = \frac{1}{2} \log_2 \left( 1 + \max(|h_{se}|^2 \gamma_0, |h_{re}|^2 \gamma_1) \right).
\]

As is discussed in \([34]\), an achievable rate is said to be the secrecy rate if the source is able to send the messages to intended destination confidentially, and we define the capacity difference between the main and wiretap channels

\[
C_s = (C_{id} - C_{ie})^+
\]

as the secrecy capacity, being the maximum secrecy rate. In (12), \( C_{id} \) and \( C_{ie} \) are given by (8) and (11), respectively, and \((a)^+ \) denotes that in case of \( a < 0 \), let \( a = 0 \).

B. Round-Robin Scheduling

Consider conventional round-robin scheduling to be a benchmark scheme, where each relay takes turn to assistant the transmission from the satellite to the destination. To be specific, a relay \( R_i \) first attempts to decode the information which is sent by the satellite, then forwards the signal if the former decoding is successful, otherwise it remains silent.

In accordance with Shannon’s coding theorem, let \( \phi = 1 \) be the case that a relay is capable to decode the received message, when the capacity \( C_{si} \) is greater than the transmission rate \( R_s \). However, in case of the capacity \( C_{si} \) falling below \( R_s \), the relay will fail in decoding the received message, which is referred to as \( \phi = 0 \). Therefore, we can describe this event can as

\[
\begin{align*}
\text{if } C_{si} < R_s, & \quad \text{then } \phi = 0, \\
\text{if } C_{si} > R_s, & \quad \text{then } \phi = 1,
\end{align*}
\]
where \( R_s \) denotes the rate when the satellite transmits the source signal to relays, and \( C_{si} \) is given by (6). Once a relay who is selected in turns to participate in the transmission decodes its received signal successfully, it will forward its received information. Consequently, the eavesdropper has a chance to intercept the relay’s transmission. Otherwise, the outage occurs under the circumstance of a relay failing decoding.

C. Single-Relay Selection

In this work, considering a HSTRN of Fig. 1, we assume that the destination is beyond the coverage of satellite, thus \( N \) relay nodes employing DF are exploited for assisting the source transmission. As aforementioned, there are two transmission phases. Firstly, \( N \) relays receive and attempt to decode the signal sent by the satellite. Let \( D \) be a set, which is comprised of the relay who can decode the received signals successfully. In terms of \( N \) relays, there exists \( 2^N \) decoding conditions. Hence, we formulate the sample space of \( D \) as

\[
\Omega = \{ \emptyset, D_1, D_2, \ldots, D_n, \ldots, D_{2^N-1} \},
\]

where \( \emptyset \) represents a null set which means no relay can decode the received signals successfully, and \( D_n \) is the \( n \)-th subset.

In the light of Shannon’s coding theorem, if the capacity of \( S-R_i \) channel exceeds \( R_s \), the relay node is in a position of decoding signals. Thus, we can define that

\[
\begin{align*}
& \text{if } C_{si} > R_s, \quad i \in \{1, 2, \ldots, N\}, \quad \text{then } D = \emptyset \\
& \text{if } C_{sj} < R_s, \quad j \in \bar{D}_n, \quad \text{then } D = D_n
\end{align*}
\]

(14)

where \( C_{si} \) is given by (6) and \( \bar{D}_n \) is the complementary set of \( D_n \).

During the second phase, only one relay is selected to be the “best” relay from the set \( D_n \) to help the satellite transmission while other relays keep silent. In practice, due to the passive eavesdropper, the CSI of the wiretap link is challenging to obtain. That is to say, the fading coefficients of the wiretap link i.e. \( h_{se} \) and \( h_{re} \) are not available at the satellite, relays and destination. As a consequence, we consider only the main links’ CSI is available in performing the selection while the instantaneous channel information of the eavesdropper links is not involved. In this case, let the relay be “best” relay who has the maximum instantaneous capacity of the channel spanning from the relay \( R_i \) to destination \( D \), thus the selection criterion for best relay can be expressed as

\[
\text{Best relay } = \arg \max_{i \in D_n} C_{id} = \arg \max_{i \in \bar{D}_n} |h_{r,d}|^2.
\]

(16)

Under this condition, let ‘b’ denote the “best” relay, therefore, the capacity of the channel between selected relay and destination is

\[
C_{bd} = \frac{1}{2} \log_2 \left( 1 + \max_{i \in D_n} |h_{r,d}|^2 \gamma_1 \right).
\]

(17)

Meanwhile, upon (11), the transmission capacity of eavesdropper channel is easily given by

\[
C_{be} = \frac{1}{2} \log_2 \left( 1 + \max(|h_{se}|^2 \gamma_0, |h_{be}|^2 \gamma_1) \right).
\]

(18)

Thus, from (12), we have

\[
C_{\text{single}} = |C_{bd} - C_{be}|^2
\]

(19)

as the secrecy capacity of best relaying transmission, where \( C_{bd} \) and \( C_{be} \) are given in (17) and (18), respectively.

D. Multi-Relay Selection

Another important type of relay selection scheme is multi-relay selection scheme, where multiple relays are invoked for simultaneously helping the satellite to communicate with the destination. As mentioned before, \( D \) denotes the successful decoding set. If \( D \) is empty, which means no relay can decode the received signals. If \( D = D_n \), in multi-relay selection scheme, a weighted version of a re-encoded signal is transmitted by all the relay nodes within \( D_n \) simultaneously. On the contrary, in single-relay selection scheme, just the optimal relay is chosen among \( D_n \) according to the selection criterion to forward the source signal. To make the best of multiple relays, the weight of all the relays within \( D_n \) is assumed to be stacked in a vector denoted by \( w = [w_1, w_2, \ldots, w_{|D_n|}]^T \). Suppose the set \( D_n \) has a cardinality of \( |D_n| \). Furthermore, for comparison purpose, it is fair to constrain the sum of all the relays’ power within \( D_n \) to be \( P_r \).

Suppose all the relays within \( D_n \) send the weighted signal simultaneously, stacked in vector \( w \), the signal arrived at destination is

\[
y_d^{\text{multi}} = \sqrt{P_r} w^T H_d x_s + n_d.
\]

(20)

Meanwhile, the signal intercepted by eavesdropper from the multiple relays and satellite can be respectively written as

\[
y_e^{\text{satellite}} = \sqrt{P_s} h_{se} x_s + n_e
\]

(21)

and

\[
y_e^{\text{relays}} = \sqrt{P_r} w^T H_e x_s + n_e,
\]

(22)

where \( H_d = [h_{r_1,d}, h_{r_2,d}, \ldots, h_{r_{|D_n|},d}]^T \) and \( H_e = [h_{r_1,e}, h_{r_2,e}, \ldots, h_{r_{|D_n|},e}]^T \). Furthermore, the received SNR at destination is given by

\[
SNR_d^{\text{multi}} = |w^T H_d |^2 \gamma_1.
\]

(23)

Similarly, upon (21) and (22), and utilizing selection combining at eavesdropper, we get the received SNR at eavesdropper as

\[
SNR_e^{\text{multi}} = \max \left( |w^T H_e |^2 \gamma_1, |h_{se}|^2 \gamma_0 \right).
\]

(24)

It is challenging to know the passive eavesdroppers’ CSIs in practice, therefore, without taking \( SNR_e^{\text{multi}} \) into account, we are motivated to maximize the \( SNR_d^{\text{multi}}, \) subjected to a normalization constraint, i.e.,

\[
\max_{w} SNR_d^{\text{multi}} = \max_{w} |w^T H_d |^2, \quad \text{s.t. } \|w\| = 1
\]

(25)

According to the Cauchy-Schwarz inequality that

\[
|\langle w, H_d \rangle|^2 \leq \langle w, w \rangle \langle H_d, H_d \rangle
\]

(26)

and \( |\langle w, H_d \rangle| = |w^T H_d | = |w^*|^T H_d \), there exists \( c \in \mathbb{F} \), such that \( w^* = c \cdot H_d \), the inequality can hold as an equality.
Here $F$ is the field of real or complex numbers. Using $\|w\| = 1$, its optimal solution is obtained as
\[
\mathbf{w}_{\text{opt}} = \frac{\mathbf{H}_d^H}{\|\mathbf{H}_d\|},
\]
which manifests merely the main link’s CSI $\mathbf{H}_d$ is required in the optimal vector design with no need for the eavesdropper’s CSI $\mathbf{H}_e$. Substituting (27) into (23), the capacity achieved at the destination can be expressed as
\[
C_{d}^\text{multi} = \frac{1}{2} \log_2 \left( 1 + \sum_{i \in D_n} |h_{r,d}|^2 \gamma_1 \right).
\]
Similarly, employing (24) and (27), we get
\[
C_{e}^\text{multi} = \frac{1}{2} \log_2 \left( 1 + \max \left( \frac{\mathbf{H}_d^H \mathbf{H}_e}{\|\mathbf{H}_d\|^2} \gamma_1, |h_{s,e}|^2 \gamma_0 \right) \right),
\]
where $\mathbf{H}_d^H$ represents the Hermitian transpose of $\mathbf{H}_d$. As defined earlier, we obtain the secrecy capacity of the multiple relaying transmission as
\[
C_{s}^\text{multi} = \left[ C_{d}^\text{multi} - C_{e}^\text{multi} \right]^+,
\]
where $C_{d}^\text{multi}$ and $C_{e}^\text{multi}$ are given in (28) and (29), respectively.

### III. Performance Analysis

As is known, a common criterion to characterize the secrecy performance is SOP. Therefore, we measure the SOPs for the round-robin scheduling, single-relay selection and multi-relay selection schemes in a DF HSTRN communication system, where the secrecy performance of round-robin scheduling is evaluated for comparison purpose.

#### A. Round-Robin Scheduling

As a baseline, we first calculate the SOP of conventional Round-Robin Scheduling. As we all know than a secrecy event happens under the condition that the secrecy capacity is below a preset rate. Hence, the secrecy probability of the communication between a satellite to a destination through a selected relay $R_i$ is given by
\[
P_{sout}^{R_i} = \Pr(\phi = 0) + \Pr(\phi = 1, C_s < R_s),
\]
where $C_s$ is given by (12). Using (6) and (13), we have
\[
\Pr(\phi = 0) = \Pr(C_{si} < R_s) = \Pr(\gamma_{si} < \gamma_{th}) = F_{\gamma_{si}}(\gamma_{th})
\]
and
\[
\Pr(\phi = 1) = \Pr(C_{si} > R_s) = \Pr(\gamma_{si} > \gamma_{th}) = 1 - F_{\gamma_{si}}(\gamma_{th}),
\]
where $\gamma_{si} = |h_{si}|^2 \gamma_0$. $\gamma_{th} = 2^R_s - 1$. Thus, (31) can be written by
\[
P_{sout}^{R_i} = F_{\gamma_{si}}(\gamma_{th}) + (1 - F_{\gamma_{si}}(\gamma_{th})) \Pr(C_s < R_s).
\]
As aforementioned, considering that the satellite to relay $R_i$ channel undergoes the Shadowed-Rician fading, whose parameters are $(\Omega_0, m_0, \delta_0)$, and according to (3), we have
\[
F_{\gamma_{si}}(\gamma_{th}) = \alpha_0 \sum_{k=0}^{\infty} \frac{\delta_0^k}{\Gamma(m_0+1+2k)\beta_0^k} \gamma_{th} \left( k + 1, \frac{\delta_0 \gamma_{th}}{\beta_0} \right),
\]
where $\alpha_0 = \frac{1}{2\beta_0} \left( \frac{2\delta_0 m_0}{2\delta_0 m_0 + \Omega_0} \right)^{m_0}$, $\beta_0 = \frac{1}{2\delta_0}$, and $\delta_0 = \frac{\Omega_0}{2\delta_0 (2\delta_0 m_0 + \Omega_0)}$.

According to (8) and (11), we get
\[
\Pr(C_s < R_s) = \Pr(C_{id} - C_{ie} < R_s) = \Pr \left( \max (|h_{sc}|^2 \gamma_0, |h_{r,e}|^2 \gamma_1) > \frac{|h_{r,d}|^2 \gamma_1 - \theta}{2^R_s} \right),
\]
where $\theta = 2^R_s - 1$. After some algebraic manipulations as Appendix A, the item $\Pr(C_s < R_s)$ is calculated as (37), where $G_{p,m}^{n,q} [\cdot, \cdot]$ represents the Meijer-G function with single variable [33].

Lastly, replacing the term $F_{\gamma_{si}}(\gamma_{th})$ and $\Pr(C_s < R_s)$ in (34) with (35) and (37) gets a closed-form solution of $P_{sout}^{RR}$.

For the reason that $N$ relays have the same chance to forward the satellite information, we can achieve the total SOP for the conventional round-robin scheduling as
\[
P_{sout}^{RR} = \frac{1}{N} \sum_{i=1}^{N} P_{sout}^{R_i}.
\]

#### B. Single-Relay Selection

In this subsection, an exact closed-form expression of SOP is derived for the proposed single-relay selection scheme in the considered DF HSTRN. Upon the secrecy outage definition and the total probability principle, we can describe the SOP for single-relay selection scheme in a HSTRN as
\[
P_{sout}^{single} = \Pr(D = \emptyset, C_s^{single} < R_s) + \sum_{n=1}^{2^N-1} \Pr(D = D_n, C_s^{single} < R_s),
\]
where $C_s^{single}$ is given by (19). It is obvious that in case of $D = \emptyset$, there is no relay succeed in decoding the source transmission. This will result in the destination failing to receive the source signal, which lead to $C_s^{single} = 0$. Consequently, (39) can be rewritten as
\[
P_{sout}^{single} = \Pr(D = \emptyset) + \sum_{n=1}^{2^N-1} \Pr(D = D_n, C_s^{single} < R_s).
\]

Substituting (19) into (40) yields
\[
P_{sout}^{single} = \Pr(D = \emptyset) + \sum_{n=1}^{2^N-1} \Pr(D = D_n) \Pr(C_{sd} - C_{be} < R_s).
\]

According to (15), we have
\[
\Pr(D = \emptyset) = \Pr(C_{si} < R_s) = \prod_{i=1}^{N} \Pr(\gamma_{si} < \gamma_{th})
\]
\[
= \prod_{i=1}^{N} F_{\gamma_{si}}(\gamma_{th})
\]
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2877709, IEEE Access

Depending on the best relay selection criterion in (16) and the total probability principle, the term \( F_{\gamma,\gamma} (\gamma_{th}) \) is given by (35). Therefore,

\[
F_{\text{sout}}^{\text{single}} = \prod_{i=1}^{N} F_{\gamma,\gamma} (\gamma_{th}) + \sum_{n=1}^{2^{N}-1} \left( \prod_{i \in D_n} (1 - F_{\gamma,\gamma} (\gamma_{th})) \right) \times \prod_{j \in D_n} F_{\gamma,\gamma} (\gamma_{th}) \Pr(C_{bd} - C_{be} < R_s) \tag{44}
\]

is the SOP of single-relay selection scheme. We note that there is a probability for each relay node to be chosen as the “best” one, out of a decoding collection of relays \( D_n \). Depending on the best relay selection criterion in (16) and the total probability principle, the term \( \Pr(C_{bd} - C_{be} < R_s) \) can be rewritten as

\[
\Pr(C_{bd} - C_{be} < R_s) = \sum_{i \in D_n} \Pr(C_{id} - C_{ie} < R_s, b = i) = \sum_{i \in D_n} \Pr(C_{id} - C_{ie} < R_s, |h_{r,d}|^2 > \max_{j \in D_n - \{i\}} |h_{r,d}|^2) \tag{45}
\]

where \( \theta = 2^{2R_s} - 1 \). Moreover, note that \( |h_{r,d}|^2 \) and \( |h_{r,e}|^2 \) obey the exponentially distribution with respective means \( \sigma_r^2 \) and \( \sigma_e^2 \), after some algebraic manipulations as Appendix B, we get (46) shown at the top of next page. Here,

\[
A = \alpha_1 \frac{e^{-\sigma_r^2 \gamma_{th}}}{\sigma_r^2 \gamma_{th}} \sum_{k=0}^{\infty} \frac{(m+k) \Gamma(m+1) \Gamma(1+k) \delta_{r,k} \delta_{e,k}^1}{\Gamma(m+k+k\delta_{r,k})} = \frac{1}{\sigma_r^2 \gamma_{th}} + \sum_{r,j \in U_m} \frac{e^{-\sigma_r^2 \gamma_{th}}}{\sigma_r^2 \gamma_{th}} \tag{46}
\]

Similarly to (40), the SOP is given by

\[
P_{\text{sout}}^{\text{multi}} = \Pr(D = \emptyset) + \sum_{n=1}^{2^{N}-1} \Pr(D = D_n) \Pr(C_{\text{bd}}^{\text{multi}} - C_{\text{be}}^{\text{multi}} < R_s). \tag{47}
\]

Substituting (30) into (47) yields

\[
P_{\text{sout}}^{\text{multi}} = \Pr(D = \emptyset) + \sum_{n=1}^{2^{N}-1} \Pr(D = D_n) \Pr(C_{\text{bd}}^{\text{multi}} - C_{\text{be}}^{\text{multi}} < R_s). \tag{48}
\]

Since the term \( \Pr(D = \emptyset) \) and \( \Pr(D = D_n) \) are expressed as (42) and (43), upon (28) and (29), we rewrite \( P_{\text{sout}}^{\text{multi}} \) as (49), where \( F_{\gamma,\gamma} (\gamma_{th}) \) is shown as (35).

Since the PDF of \( \frac{|H_{r,d} \cdot H_{r,e}|^2}{|H_{r}|^2} \) is unknown, it places fundamental difficulties to achieve a closed-form SOP expression for multi-relay selection scheme. However, it is fairly simple to numerically curve the character of SOP by computer simulations.

IV. NUMERICAL RESULTS AND DISCUSSIONS

This section shows the numerical simulation results of SOP with respect to round-robin scheduling, single-relay selection and multi-relay selection schemes, corresponding to (38), (44) and (49). Here, we assume the terrestrial links obey the Rayleigh distribution while the satellite-terrestrial channels are subject to the Shadowed-Rician model, where the average shadowing (AS) [32] is considered in our numerical results, with parameters (\( b, m, \Omega \)) being (0.126, 10.1, 0.835) unless otherwise noted. For notational convenience, let \( \lambda \) denote the ratio of \( \sigma_r^2 \) to \( \sigma_e^2 \), i.e., \( \lambda = \sigma_r^2 / \sigma_e^2 \) named main-to-eavesdropper ratio (MER). In addition, the performance curves are given by carrying out \( 10^7 \) channel realization, adopting \( R_s = 0.5 \text{ bit/s/Hz} \) as the data rate.

Fig. 2 depicts the SOP comparison among the three relay selection schemes presented above as a function of MER for different values of relay number \( N \) (\( N=2, 3 \) and 5) in a DF HSTRN. Obviously, the derived results are aligned with the simulation results, which validate the correctness of the aforementioned derivation. As shown in Fig. 2, even in low MER region, the performance of relay selection schemes exceeds round-robin scheduling in the light of their SOPs, confirming the advantages of relay selection scenario. Moreover, it can be easily found in Fig. 2 that the SOPs of the three aforementioned schemes reduce when the MER increases. Additionally, with all the values of \( N=2, 3 \) and 5 in Fig. 2, the multi-relay selection outperforms single-relay selection scheme dramatically, nevertheless, at the expense of a higher implementation complexity. Also it needs to be pointed out that once the strict synchronization is not perfect, a performance degradation will occur in multi-relay selection.
results. In high SNR region of Fig. 3, it can be seen that relay selection schemes agree excellently to the simulation theory curves related to the round-robin scheduling and single-relay selection schemes for different number of relays \( N \). As expected, the secrecy outage performance significantly increases, the physical-layer security performance of the two schemes in HSTRN environments. Simulation results showed that the secrecy floor can be reduced by employing more relays. Concretely, for single-relay selection scheme, once the value of relay number gets large, the chance of choosing a better relay accelerates, along with the more correctness of receiving the symbols from the source. Meanwhile, for multi-relay selection scheme, the larger the number of relays is, the more relays may decode the source signal successfully, accordingly more relays are employed simultaneously in the transmission, achieving a better performance.

Fig. 4 shows the secrecy performance of the three schemes for different shadowing conditions with \( N=3 \). Here, assuming the satellite-eavesdropper link always obey the AS shadowing, whereas the satellite-relay links experience all the three kinds of shadowing including the AS, the frequent heavy shadowing (FHS) \((b,m,\Omega) = (0.063, 0.0739, 8.97 \times 10^{-4})\) and infrequent light shadowing (ILS) \((b,m,\Omega) = (0.158, 19.4, 1.29)\) [32]. As expected, the secrecy outage performance significantly improves with a better channel condition. Moreover, as is seen in high SNR region, the SOPs of three schemes converge to their secrecy outage floor respectively for different shadowing conditions, implying the better channel quality could not improve the secrecy outage floor.

V. CONCLUSION

We studied the secrecy outage performance of a DF HSTRN, where a satellite connects to a terrestrial destination through multiple relays at the appearance of an eavesdropper. We improve the physical-layer security of HSTRN by utilizing the single-relay selection and multi-relay selection schemes which both only need the CSIs of the legitimate channels without knowing the wiretap channel’s CSI. The SOP of round-robin scheduling scheme was also evaluated for comparison purpose. Moreover, we derived closed-form SOP expressions for the round-robin scheduling and single-relay schemes in HSTRN environments. Simulation results showed that the security performance of the presented two relay selection schemes generally outperform round-robin scheduling scheme. Additionally, along with the value of relay number increasing, the physical-layer security performance of the two relay selection schemes improves remarkably, illustrating their advantages of the secure transmission enhancement for the HSTRN.
Suppose that the satellite to eavesdropper channel experiences the Shadowed-Rician fading with parameters \((\Omega_1, m_1, b_1)\), according to (3), we get

\[
F_{\gamma_{se}}(x) = \alpha_1 \sum_{k=0}^{\infty} \frac{\Gamma(m_1+k)}{\Gamma(m_1)\Gamma(1+k)!} \frac{\delta_1^k}{\beta_1^k} \gamma \left(k + 1, \frac{\beta_{se} \cdot t}{\gamma_0 \cdot 2R_s} \right).
\]

Here, \(\alpha_1 = \frac{1}{2|b_1|} \left(\frac{2b_1m_1}{2b_1m_1+1}\right)^{m_1/2} \), \(\beta_1 = \frac{1}{2|b_1|}\), and \(\delta_1 = \frac{2|b_1|}{(2b_1m_1+1)}\).

Hence, (A.3) can be rewritten as

\[
\Pr(C_s < R_s) = 1 - (A - \int_{0}^{\infty} \gamma \left(k + 1, \frac{\beta_{se} \cdot t}{\gamma_0 \cdot 2R_s} \right) \times \left[ e^{-\frac{x}{\sigma_{r,d}^2} \gamma_1} - e^{-\frac{x}{\sigma_{r,d}^2} \gamma_1} e^{-\frac{x^2}{2\sigma_{r,e}^2 \gamma_1}} \right] dx),
\]

where \(A = \alpha_1 \frac{1}{\sigma_{r,d}^2} e^{-\frac{\theta}{\sigma_{r,d}^2} \gamma_1} \sum_{k=0}^{\infty} \frac{\Gamma(m_1+k)}{\Gamma(m_1)\Gamma(1+k)!} \frac{\delta_1^k}{\beta_1^k} \gamma \left(k + 1, \frac{\beta_{se} \cdot t}{\gamma_0 \cdot 2R_s} \right).

For convenience, we express the incomplete gamma function \(\gamma(\cdot, \cdot)\) as Meijer-G function by employing [35, eq. (8.4.16.1)], thus

\[
\gamma \left(k + 1, \frac{\beta_{se} \cdot t}{\gamma_0 \cdot 2R_s} \right) = G_{1,2}^{1,1} \left[ \frac{\beta_{se}}{\gamma_0 \cdot 2R_s} \middle| \begin{array}{c} 1,0,1 \end{array} \right].
\]

Then according to [35, eq.(12.7.813.1)], we perform the integration, yielding (37).

### APPENDIX B

### DERIVATION OF (46)

Considering that \(|h_{r,d}|^2, |h_{r,e}|^2\) and \(|h_{r,e}|^2\) are independent and denoting \(|h_{r,d}|^2\gamma_1 = X, \max(|h_{se}|^2\gamma_0, |h_{r,e}|^2\gamma_1) = Y\) and \(|h_{r,d}|^2\gamma_1 = Z_j\), thus we can rewrite (45) as

\[
\Pr(C_{bd} - C_{be} < R) = \sum_{i \in D_n} \Pr \left(Y > \frac{X - \theta}{2R_s}, X > \max_{j \in D_n-(i)} Z_j \right).
\]

Let \(t = x - \theta\), yielding

\[
\Pr(C_s < R_s) = 1 - \int_{0}^{\infty} F_{\gamma_{se}} \left( \frac{\theta}{\sigma_{r,e}^2} \right) F_{\gamma_{se}} \left( \frac{\theta}{\sigma_{r,d}^2} \right) e^{-\frac{t}{\sigma_{r,d}^2} \gamma_1} dt.
\]

Note that \(|h_{r,d}|^2, |h_{r,e}|^2\) and \(|h_{r,e}|^2\) are exponentially random variables with parameters \(\sigma_{r,d}^2, \sigma_{r,e}^2\) and \(\sigma_{r,e}^2\), and \(|h_{se}|^2\) obeys the Shadowed-Rician distribution with the PDF of (1). Assuming \(\Pr(C_{bd} - C_{be} < R) = P1 - P2\), we obtain (B.2) at the top of next page.
\[
\Pr(C_{bd} - C_{bc} < R) = \sum_{i \in D_n} \int_0^\infty \frac{1}{\sigma^2 r_i d^\gamma_1} e^{-\frac{\sigma r_i d^{\gamma_1}}{\sigma^2}} \prod_{j=1 \atop j \neq i}^{D_n} \left( 1 - e^{-\frac{r_j d^{\gamma_1}}{\sigma^2}} \right) dx
\]

\[
- \sum_{i \in D_n} \int_0^\infty F_{\gamma_{nx}} \left( x - \theta \right) F_{\gamma_{nx}} \left( \frac{x - \theta}{2 R_x} \right) \frac{1}{\sigma^2 r_i d^\gamma_1} e^{-\frac{\sigma r_i d^{\gamma_1}}{\sigma^2}} \prod_{j=1 \atop j \neq i}^{D_n} \left( 1 - e^{-\frac{r_j d^{\gamma_1}}{\sigma^2}} \right) dx
\]

\[
P_2 = \sum_{i \in D_n} \sum_{m=0}^{2^{D_n} - 1} A \cdot (1)^{|U_m|} \int_0^\infty \frac{1}{\gamma_0} \left( k + 1, \frac{\beta_{sc} \cdot t}{\gamma_0} \cdot \frac{2}{2 R_x} \right) e^{-\left( \frac{\gamma_0 + \sum_{j=1 \atop j \neq m}^{D_n} \frac{\beta_{sc} \cdot t}{\gamma_0} \cdot \frac{2}{2 R_x}}{\sigma^2 r_i d^{\gamma_1}} \right) dt
\]

Using the binomial theorem, term \[
\prod_{j=1 \atop j \neq i}^{D_n} \left( 1 - e^{-\frac{r_j d^{\gamma_1}}{\sigma^2}} \right)
\] can be expanded as

\[
\prod_{j=1 \atop j \neq i}^{D_n} \left( 1 - e^{-\frac{r_j d^{\gamma_1}}{\sigma^2}} \right) = \sum_{m=0}^{2^{D_n} - 1} (-1)^{|U_m|} e^{- \sum_{j \in U_m} \frac{r_j d^{\gamma_1}}{\sigma^2}}
\]

where \(U_m\) is the m-th subset of \(U - \{U_i\}\), and \(-\cdot\) is the set difference. Thus performing the integration, we have

\[
P_1 = \sum_{i \in D_n} \sum_{m=0}^{2^{D_n} - 1} (-1)^{|U_m|} \left( 1 - \frac{1}{\sigma^2 r_i d^{\gamma_1}} \right) \sum_{j \in U_m} \frac{1}{\sigma^2 r_j d^{\gamma_1}}
\]

Then substituting (A.3) and (B.3) into (B.2), and let \(t = x - \theta\), similarly to Appendix A, we get \(P_2\) as (B.5), where

\[
A = \frac{1}{\sigma^2 r_i d^{\gamma_1}} e^{-\frac{\sigma r_i d^{\gamma_1}}{\sigma^2}} \sum_{k=0}^\infty \frac{\Gamma(m+k)}{\Gamma(m)\Gamma(1+k)\Gamma(k)!} \delta^k e^{-\frac{r_j d^{\gamma_1}}{\sigma^2}}
\]

Considering Meijer-G function, we employ [35, eq. (8.4.16.1)] into (B.5), then according to [35, eq. (12.7.813.1)] to perform the integration, we can arrive at (46).

REFERENCES


[20] B. Evans, M. Werner, E. Lutz, and et al., “Integration of satellite and...


