Physical Layer Security for Multiuser Satellite Communication Systems with Threshold-based Scheduling Scheme

Kefeng Guo, *Student Member*, *IEEE*, Kang An, *Member*, *IEEE*, Xiaogang Tang, Yuzhen Huang, *Member*, *IEEE*, Gan Zheng, *Senior Member*, *IEEE*, and Theodoros A. Tsiftsis, *Senior, Member*, *IEEE*

***Abstract*—In this paper, we investigate the physical layer security of a multiuser satellite communication system in the presence of multiple eavesdroppers. Particularly, we propose a threshold-based scheduling scheme among the multiple legitimate users, where the geographically clustered eavesdroppers with both the colluded and collaborated eavesdropping scenarios are assumed. Specifically, the closed-form expression for the secrecy outage probability (SOP) is derived for the passive eavesdropping scenario when the channel state information (CSI) of the eavesdroppers is unavailable. In order to get insights of the proposed scheduling scheme at high signal-to-noise ratios (SNRs), the asymptotic analysis for the SOP is also obtained. Moreover, the reduced percentage with respect to number of user examination is also given, which validates the simplicity and efficiency of our proposed scheme compared to the traditional approaches. Numerical results suggest that with the proposed scheme, a comparable system performance with regard to the maximal selection (MS) scheme can be achieved.**

***Index Terms*—Secrecy outage probability (SOP), satellite-terrestrial network, threshold-based scheduling.**

I. Introduction

DUE to the ability of seamless connectivity and high data rate, satellite communication (SatCom) has been viewed as a key element to bring real-time, higher capacity communication and wider coverage in the connection and deployment of smart grid, Internet-of-Thing (IoT), wireless sensor networks, space-based cloud for big data, Vehicular ad-hoc networks and etc (see [1], [2] and the references therein). However, owing to the inherent nature of broadcasting and a huge area of coverage, SatComs are easily to be exposed to various security issues. Traditionally, the security issues in SatComs are addressed by encryption in the upper layers, such as the Advanced Encryption Standard (AES) [3]. However, the absolute security can not be perfectly guaranteed by the traditional encryption method with the increasing ability of the eavesdropper's computation and decoding [4], [5]. Moreover, it is recognized that such protocols e.g. tunneling though may lead to significant transmission overhead in clear detriment of quality of service (QoS). Different from the traditional cryptographic techniques, physical layer security (PLS) provides a prospective approach to secure the wireless networks by detecting the inherent randomness of wireless fading channels at the physical layer. The information-theoretic basis in PLS, such as average secrecy capacity (ASC), secrecy outage probability (SOP) and etc are the fundamentals for the transmission of confidential data over wireless channels [6]. In [7], the authors analyzed the non-zero probability of secrecy capacity, SOP and ASC for the SatComs in the Shadowed-Rician (SR) channel. In [8], the authors investigated the secrecy performance of a hybrid satellite-terrestrial relay network.

However, it is worth to note that future SatCom systems are required to provide high information transfer rate to a large number of users at a reasonable cost and preferable QoS [9]. To its regret, the aforementioned works on PLS in SatComs merely considered the cases with a single legitimate user and eavesdropper, which is an unrealistic assumption and quite limited in practical scenarios. Moreover, the multiuser transmission in SatComs also results in a higher opportunities for the leakage of confidential messages, thus increasing the risk of being eavesdropped. In [10], the authors proposed a novel optimization problem to satisfy the need to frame multiple users per transmission. In [11], the authors studied the problem of precoding, scheduling and link adaptation in mobile interactive SatComs.

In this paper, by considering the satellite links undergo SR fading and the impacts of satellite beam pattern and path loss, a threshold-based scheduling scheme is proposed to enhance the secrecy performance of a multiuser satellite communication system while maintaining low implementation complexity. In an effort to quantify the system performance and validate the proposed scheme, exact and asymptotic SOP, along with the reduced percentage with respect to the number of legitimate user examination, are derived, respectively. Numerical results have been obtained to evaluate the validity of the analytical

This work was supported by the Research Project of NUDT under grant ZK18-02-11, also supported by the National Science Foundation of China (No. 61401508) and the Jiangsu Provincial Natural Science Foundation of China (No. 20150719).

K. Guo and X. Tang are with the School of Space Information, Space Engineering University, Beijing 101407, China; X. Tang is also with the School of Mechanical Engineering, Xi'an Jiaotong University, Xi'an, 710049, China (e-mail: guokefeng.cool@163.com; titantxg@163.com).

K. An is with the National University of Defense Technology, Nanjing 210007, China (e-mail:ankang@nuaa.edu.cn).

Y. Huang is with the Artificial Intelligence Research Center, National Innovation Institute of Defense Technology, Beijing 100039, China (e-mail: yzh_huang@sina.com).

G. Zheng is with the Wolfson School of Mechanical, Electrical, and Manufacturing Engineering, Loughborough University, Loughborough LE113TU, U.K. (e-mail: g.zheng@lboro.ac.uk).

T. A. Tsiftsis is with the School of Electrical and Information Engineering, Jinan University (Zhuhai Campus), Zhuhai, 519070, China (e-mail: theodoros.tsiftsis@gmail.com).

Corresponding Author: Xiaogang Tang, Email: titantxg@163.com.

results as well as the superiority of the proposed scheme.

II. System Model

Let us consider a multiuser downlink wiretap satellite network, where a satellite (Alice) equipped with single antenna, N_B legitimate terrestrial users (Bobs) in the presence of N_E eavesdroppers (Eves). On the assumption that all the Bobs and Eves are equipped with single antenna, which is practical in certain multiuser scenarios such as wireless sensors, Internet-of-thing (IoT) and broadcasting networks. Without loss of generality, we assume that the main links and the eavesdroppers' links are subject to independent and non-identically distributed (i.n.i.d) block SR fading[1]. For notational convenience, the channel coefficient between the satellite and the i-th legitimate user is denoted as h_{bi}, and the channel coefficient between the satellite and the j-th eavesdropper is termed as h_{ej}. By exploiting time division multiple access (TDMA) scheme, only a single scheduled legitimate user is in service at each time slot. Let $s(t)$ denote the confidential signal transmit by the satellite satisfying $E\left[|s(t)|^2\right]=1$, the signals received at the i-th Bob and the j-th Eve are, respectively, written as

$$y_{bi}(t)=\sqrt{P}h_{bi}s(t)+n_{bi}(t), \tag{1a}$$

$$y_{ej}(t)=\sqrt{P}h_{ej}s(t)+n_{ej}(t), \tag{1b}$$

where P presents the transmit power at Alice, $n_{bi}(t)$ and $n_{ej}(t)$ are the additive white Gaussian noise (AWGN) at the i-th Bob and the j-th Eve with zero mean and variance δ_{bi}^2, δ_{ej}^2, respectively. Specifically, h_{bi} and h_{ej} can be uniformly written as

$$h_P=Q_P g_P, P\in\{bi,ej\}, \tag{2}$$

where g_P is the channel coefficient following SR fading [13], [14], [15], and Q_P is the scaling parameter including various practical effects, such as free space loss (FSL) and on-board beam gain, which is given by

$$Q_P=C\sqrt{F_{t,P}F_{r,P}}/\left(4\pi f d_P\sqrt{K_W T_W}\right), \tag{3}$$

where C is the light velocity, f is the frequency of the carrier, d_P is the propagation distance. $K_W=1.38\times10^{-23}$J/m the Boltzman constant, T_W is the receive noise temperature, and W denotes the carrier bandwidth. Meanwhile, $F_{r,P}$ presents the receiving gain, and $F_{t,P}$ presents the beam gain of the satellite, which can be nearly given by [16]

$$F_{t,P}=F_{\max}\left(\frac{J_1(x)}{2x}+36\frac{J_3(x)}{x^3}\right)^2, \tag{4}$$

where F_{max} denotes the maximal satellite beam gain and $x=2.07123\sin\theta/\sin\theta_{3\text{dB}}$, where θ is the angle between the location of the corresponding receiver and the beam carrier with respect to the satellite, and $\theta_{3\text{dB}}$ is the 3-dB angle, J_1 and J_3 present the first kind bessel function of order 1 and 3 [17], respectively.

[1]The Shadowed-Rician model that is proposed originally by Loo has found wide applications in different frequency bands such as the UHF-band, L-band, S-band, and Ka-band [12], has been widely employed in many existing works [13], [14].

From (1a) and (1b), the instantaneous received SNR at the i-th Bob and the j-th Eve can be, respectively, given by

$$\gamma_{bi}=\overline{\gamma}_{bi}|g_{bi}|^2, \tag{5a}$$

$$\gamma_{ej}=\overline{\gamma}_{ej}|g_{ej}|^2, \tag{5b}$$

where $\bar{\gamma}_{bi}=PQ_{bi}^2/\delta_{bi}^2$ is the average SNR of the satellite to the i-th Bob link and $\bar{\gamma}_{ej}=PQ_{ej}^2/\delta_{ej}^2$ that of the satellite to the j-th Eve link.

III. Secrecy Performance Analysis

In this section, a comprehensive analysis on the secrecy performance of the system based on the proposed threshold-based scheme.

A. Preliminaries

Owing to every Eve has access to the source signal, several diversity combining schemes can be applied to strengthen the wiretapping. Without loss of generality, we consider a worse-case scenario where the eavesdroppers are geographically located in clustering environment. Hence, a colluded and collaborated eavesdropping can be implemented among the multiple Eves. By considering the maximal ratio combining (MRC) linear processing scheme among the Eves, we obtain the equivalent instantaneous SNR of Eves as

$$\gamma_e=\sum_{j=1}^{N_E}\gamma_{ej}. \tag{6}$$

Before analyzing the secrecy performance of the system, we first give the cumulative density function (CDF) of γ_{bi} and the probability density function (PDF) of γ_e [18], respectively, as

$$F_{\gamma_{bi}}(x)=1-\alpha_b\sum_{k_b=0}^{m_b-1}\sum_{v=0}^{k_b}\frac{\varsigma(k_b)(k_b!)}{v!\Delta_b^{k_b-v+1}}x^v e^{-\Delta_b x}, \tag{7a}$$

$$f_{\gamma_e}(x)=\sum_{k_{e1}=0}^{m_e-1}\cdots\sum_{k_{eN_E}=0}^{m_e-1}\Xi(N_E)\,x^{\Lambda_e-1}e^{-\Delta_e x}, \tag{7b}$$

where $\varsigma(k_b)=\frac{(-\sigma_b)^{k_b}(1-m_b)_{k_b}}{(k_b!)^2\bar{\gamma}_{bi}^{k_b+1}}$ with $(\cdot)_n$ is the Pochhammer symbol [17], $\Delta_b=\frac{\beta_b-\sigma_b}{\bar{\gamma}_{bi}}$, $\alpha_l=\left(\frac{2b_l m_l}{2b_l m_l+\Omega_l}\right)^{m_l}/2b_l$, $\beta_l=1/2b_l$, $\sigma_l=\frac{\Omega_l}{2b_l(2b_l m_l+\Omega_l)}$ with Ω_l, $2b_l$ and m_l ($l\in\{bi,e\}$) are the average power of line-of-sight (LOS), multiple path components and the fading severity parameters, respectively,

$$\Xi(N_E)=\prod_{p=1}^{N_E}\varsigma(k_e)\alpha_e^{N_E}\prod_{q=1}^{N_E-1}B\left(\sum_{s=1}^{q}k_s+q,k_{q+1}+1\right), \tag{8}$$

and $\Lambda_e=\sum_{p=1}^{N_E}k_p+N_E$, where $B(.,.)$ denotes the Beta function [17].

Traditional scheduling schemes select the best user to be served based on the channel state information (CSI) examination of each user, which requires computationally demanding iterative process [11]. Given the constrained feedback resources and limited on-board processing capability in the

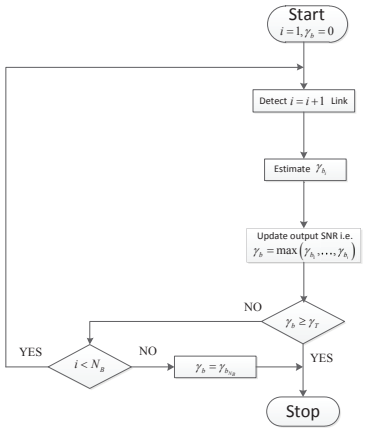


Fig. 1. Diagram of the proposed scheduling scheme

satellite network, we design a threshold-based user scheduling scheme for the secure transmission for SatComs in the presence of multiple Eves. Our proposed scheme can be explained as follows:

- Firstly, without loss of generality, we assume that $\gamma_{b\langle 1\rangle} = \min\{\gamma_{b1}, \gamma_{b2}, \ldots, \gamma_{bN_B}\}$ and $\gamma_{b\langle N_B\rangle} = \max\{\gamma_{b1}, \gamma_{b2}, \ldots, \gamma_{bN_B}\}$, i.e., $\gamma_{b\langle 1\rangle} < \cdots < \gamma_{b\langle i\rangle} < \cdots < \gamma_{b\langle N_B\rangle}$. A scheduling threshold γ_T is set, Alice first check the SNR $\gamma_{b\langle 1\rangle}$, if $\gamma_{b\langle 1\rangle} > \gamma_T$, this transmitted link is selected, no other link will be checked, i.e., $\gamma_b = \gamma_{b\langle 1\rangle}$.
- Secondly, if $\gamma_{b\langle 1\rangle} < \gamma_T$, Alice will check the left $N_B - 2$ Bobs' links, if $\gamma_{b\langle i\rangle} > \gamma_T$, the i-th Bob link will be chosen, i.e., $\gamma_b = \gamma_{b\langle i\rangle}$ Otherwise, the Alice will examine the $(i+1)$-th link.
- Thirdly, if $\gamma_{b\langle N_B-1\rangle} > \gamma_T$, this (N_B-1)-th link will be chosen, if not, Alice will not check the N_B-th link, the N_B-th link will be directly chosen as the transmitted link no matter what the SNR is, i.e., $\gamma_b = \gamma_{b\langle N_B\rangle}$.

According to the detailed scheduling scheme, we can obtain the following scheduling process as Fig. 1.

Lemma 1. *Based on the aforementioned analysis and assuming all the Bobs' links having the identical fading parameters, we can obtain the CDF of γ_b as*

$$F_{\gamma_b}(x) = \begin{cases} 1 - \sum_{i=0}^{N_B-1} \left[F_{\gamma_{bi}}(\gamma_T)\right]^i \left[1 - F_{\gamma_{bi}}(x)\right], x \geq \gamma_T \\ \left[F_{\gamma_{bi}}(\gamma_T)\right]^{N_B-1} F_{\gamma_{bi}}(x), x < \gamma_T, \end{cases} \tag{9}$$

where $F_{\gamma_{bi}}(x)$ has been derived in (7a).

Proof: See Appendix A. ∎

IV. Secrecy Outage Probability

The knowledge of eavesdroppers' CSI is commonly unavailable at the satellite, thus the transmission rate can not be adapted according to the CSI. In this case, the SOP, which is defined as the probability that the secrecy capacity falls below a predefined secrecy rate R_0, is mathematically formulated as

$$P_{out}(R_0) = \Pr(C_S < R_0), \tag{10}$$

where $R_0 = \log_2(1+\gamma_0)$, γ_0 is the outage threshold of the system, $C_S = C_B - C_E$, $C_B = \log_2(1+\gamma_b)$, and $C_E = \log_2(1+\gamma_e)$. By substituting these equations into (10), it can be expressed as

$$\begin{aligned} P_{out}(R_0) &= \Pr[\gamma_b < \gamma_0 + (\gamma_0+1)\gamma_e] \\ &= \int_0^\infty F_{\gamma_b}(\gamma_0 + (\gamma_0+1)x) f_{\gamma_e}(x)\, dx. \end{aligned} \tag{11}$$

From (9), we know that the proposed scheduling scheme relies on the predefined threshold γ_T, here we recommend a boundary point $H(\gamma_T) = \frac{\gamma_T - \gamma_0}{\gamma_0+1}$ to make SOP more tractable. Hence, the SOP can be rewritten as

$$P_{out}(R_0) = \begin{cases} \underbrace{\int_0^{H(\gamma_T)} F_{\gamma_b}(Y(x)) f_{\gamma_e}(x)\, dx}_{I_1} \\ + \underbrace{\int_{H(\gamma_T)}^\infty F_{\gamma_b}(Y(x)) f_{\gamma_e}(x)\, dx}_{I_2}, H(\gamma_T) \geq 0 \\ \underbrace{\int_0^\infty F_{\gamma_b}(Y(x)) f_{\gamma_e}(x)\, dx}_{I_3}, H(\gamma_T) < 0, \end{cases} \tag{12}$$

where $Y(x) = \gamma_0 + (\gamma_0+1)x$.

By substituting (7b) and (9) into I_1, I_2 and I_3, they can be derived, respectively, as (13), (14), and (15), which are at the top of next page, where

$$F_{\gamma_{bi}}(\gamma_T) = 1 - \alpha_b \sum_{k_b=0}^{m_b-1} \sum_{l=0}^{k_b} \frac{\varsigma(k_b)(k_b!)}{l!\Delta_b^{k_b-l+1}} \gamma_T^l e^{-\Delta_b \gamma_T}. \tag{16}$$

A. Asymptotic Secrecy Outage Probability

Although the exact expression of SOP has been obtained, it is hard to derive more insights from (12). Therefore, in what follows, the asymptotic analysis for the SOP will be derived. In the high SNR regime, which means that $\overline{\gamma}_{bi} \to \infty$. Hence, only the first summation term of $F_{\gamma_{bi}}(x)$ should be taken into consideration, since it momentously affects the overall performance while all the other terms approach zero. Accordingly, (7a) can be further expressed as

$$F_{\gamma_{bi}}^\infty(x) = \frac{\alpha_b}{\overline{\gamma}_{bi}} x + o(x), \tag{17}$$

where $o(x)$ is the high order infinitesimal of x.

Lemma 2. *In order to analyze the diversity order and coding gain conveniently, the asymptotic SOP can be expressed as*

$$P_{out}(R_0) = \Phi\left(\frac{1}{\overline{\gamma}_{bi}}\right)^\Psi, \tag{18}$$

where the secrecy diversity order $\Psi = 1$ and the secrecy coding gain is

$$\Phi = \begin{cases} I_1^\infty \overline{\gamma}_{bi} + I_2^\infty \overline{\gamma}_{bi}, H(\gamma_T) \geq 0 \\ I_3^\infty \overline{\gamma}_{bi}, H(\gamma_T) < 0. \end{cases}$$

Proof: See Appendix B. ∎

$$I_1 = \left[F_{\gamma_{bi}}(\gamma_T)\right]^{N_B-1} \sum_{k_{e1}=0}^{m_e-1} \cdots \sum_{k_{eN_E}=0}^{m_e-1} \Xi(N_E) \left\{ \frac{\gamma\left(\Lambda_e, H(\gamma_T)\Delta_e\right)}{\Delta_e^{\Lambda_e}} - \alpha_b \sum_{k_b=0}^{m_b-1} \sum_{v=0}^{k_b} \sum_{s=0}^{v} \binom{v}{s} \times \frac{\varsigma(k_b)(k_b!)\gamma_0^{v-s}(\gamma_0+1)^s}{v!\Delta_b^{k_b-v+1} e^{\Delta_b\gamma_0}\left[\Delta_e+\Delta_b(\gamma_0+1)\right]^{s+\Lambda_e}} \gamma\left(s+\Lambda_e, \left[\Delta_e+\Delta_b(\gamma_0+1)\right] H(\gamma_T)\right) \right\}, \tag{13}$$

$$I_2 = \sum_{k_{e1}=0}^{m_e-1} \cdots \sum_{k_{eN_E}=0}^{m_e-1} \Xi(N_E) \left\{ \frac{\Gamma\left(\Lambda_e, H(\gamma_T)\Delta_e\right)}{\Delta_e^{\Lambda_e}} - \sum_{i=0}^{N_B-1} \left[F_{\gamma_{bi}}(\gamma_T)\right]^i \alpha_b \sum_{k_b=0}^{m_b-1} \sum_{v=0}^{k_b} \sum_{t=0}^{v} \binom{v}{t} \times \frac{\varsigma(k_b)(k_b!)\gamma_0^{v-t}(\gamma_0+1)^t}{v!\Delta_b^{k_b-v+1} e^{\Delta_b\gamma_0}\left[\Delta_e+\Delta_b(\gamma_0+1)\right]^{t+\Lambda_e}} \Gamma\left(t+\Lambda_e, \left[\Delta_e+\Delta_b(\gamma_0+1)\right] H(\gamma_T)\right) \right\}, \tag{14}$$

$$I_3 = \sum_{k_{e1}=0}^{m_e-1} \cdots \sum_{k_{eN_E}=0}^{m_e-1} \Xi(N_E) \left\{ \frac{(\Lambda_e-1)!}{\Delta_e^{\Lambda_e}} - \sum_{i=0}^{N_B-1} \left[F_{\gamma_{bi}}(\gamma_T)\right]^i \alpha_b \sum_{k_b=0}^{m_b-1} \sum_{v=0}^{k_b} \sum_{p=0}^{v} \binom{v}{p} \frac{\varsigma(k_b)(k_b!)\gamma_0^{v-p}(\gamma_0+1)^p (p+\Lambda_e-1)!}{v!\Delta_b^{k_b-v+1} e^{\Delta_b\gamma_0}\left[\Delta_e+\Delta_b(\gamma_0+1)\right]^{p+\Lambda_e}} \right\}. \tag{15}$$

V. Average Number of Legitimate User Examinations

According to the proposed scheduling scheme, once an user is acceptable, the other users will be not checked. Hence the average user examinations' number can be written as

$$N^A = \sum_{i=0}^{N_B-1} \left[F_{\gamma_{bi}}(\gamma_T)\right]^i. \tag{19}$$

As it is fact that $F_{\gamma_{bi}}(\gamma_T) \leq 1$, we can obtain that

$$N^A = \frac{1-\left[F_{\gamma_{bi}}(\gamma_T)\right]^{N_B}}{1-F_{\gamma_{bi}}(\gamma_T)}. \tag{20}$$

From (20), we find that N^A is decided by N_B and $F_{\gamma_{bi}}(\gamma_T)$. When $N_B \to \infty$, $N^A = 1/\left[1-F_{\gamma_{bi}}(\gamma_T)\right]$. So in this assumption, if we want to have a smaller N^A, γ_T should be larger.

Furthermore, from a more intuitive perspective, we employ the reduced percentage in terms of the number of legitimate user examinations (RPN) to justify the advantage of the proposed scheme, which can be expressed as

$$\begin{aligned} RPN &= 1 - N^A/N_B \\ &= 1 - \left\{1-\left[F_{\gamma_{bi}}(\gamma_T)\right]^{N_B}/\left[1-F_{\gamma_{bi}}(\gamma_T)\right]\right\}/N_B. \end{aligned} \tag{21}$$

VI. Numerical Representative Results

In this section, we perform numerical results for the above-mentioned secrecy analysis and validate the proposed scheme through Monte-Carlo (MC) simulations. The system parameters are given in Table I [16] and the shadowing coefficients of the satellite channel are provided in Table II [13], respectively. Without loss of generality, we set $\delta_{bi}^2 = \delta_{ej}^2 = 1$ and in all the plots we denote $\overline{\gamma}_{bi} = \overline{\gamma}_b$.

Fig. 2 plots the SOP of the considered system versus $\overline{\gamma}_b$ with γ_T=10dB and $\overline{\gamma}_e$ =10dB for AS. As shown in this figure, we can observe that the MC simulation results are tight across the analytical results versus the whole SNRs. Besides we find that at high SNRs, the asymptotic results are the same with the MC simulations results, which prove the correctness of our analysis. Furthermore, just as we analyzed before, the secrecy diversity remains one and the key system parameters, including γ_T, N_B and N_E, influence the system performance by affecting the secrecy coding gain. We observe that the secrecy coding gain will be lower when a larger N_B or γ_T is presented. In addition, we can also find that the secrecy coding gain will be degraded when N_E is larger.

TABLE I
SYSTEM PARAMETERS

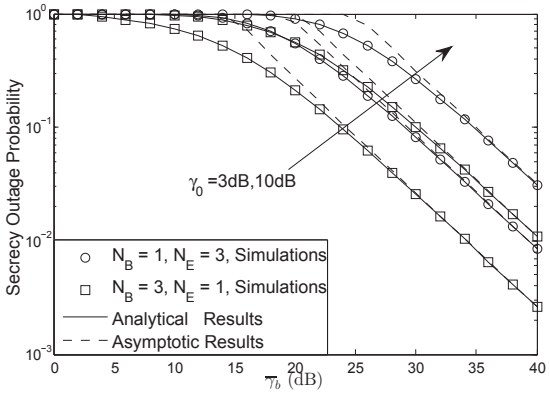
Parameters	Value
Satellite Orbit	GEO
Frequency band	f=2GHz
3dB angle	$\theta_{3\text{dB}} = 0.8°$
Maximal Beam Gain	$F_{max} = 48dB$
Receive Gain	$F_{r,J} = 4dB$
link bandwidth	$W = 15$MHz
Noise Temperature	300°K

TABLE II
CHANNEL PARAMETERS

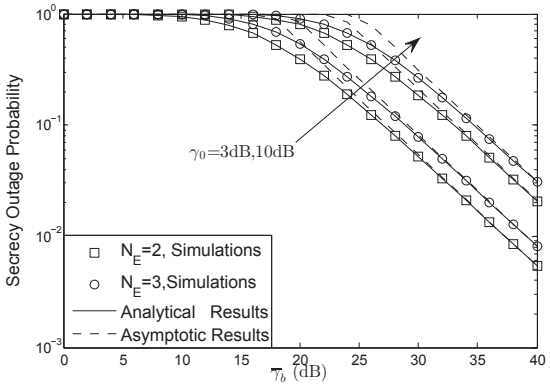
Shadowing	m_P	b_P	Ω_P
Frequent heavy shadowing (FHS)	1	0.063	0.0007
Average shadowing (AS)	5	0.251	0.279
Infrequent light shadowing (ILS)	10	0.158	1.29

Fig. 3 depicts the SOP versus γ_T with $\overline{\gamma}_b$ =40dB for different shadowing scenarios. From the figure, we know that the optimal value of γ_T which means the lowest SOP will change according to different channel shadowing severities. The heavier channel shadowing is, the smaller γ_T will be. Moreover, we can obtain that the SOP will be larger with the increasing SNR of the eavesdropper.

Fig. 4 provides the reduced percentage in terms of the number of user examinations versus γ_T with different N_B and $\overline{\gamma}_b$ for FHS. As illustrated in this figure, we compare our proposed scheme with the maximal selection (MS) scheme (which is the best scheduling scheme [10], [11]). Intuitively, we can find that the reduced percentage of MS scheme is always zeros (the users that are not used), which means that



(a) Different N_B and N_E.



(b) Different N_E with N_B=3.

Fig. 2. The SOP versus $\overline{\gamma}_b$ with γ_T=5dB for AS.

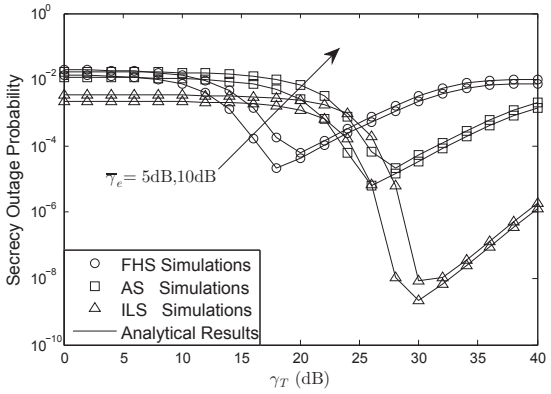


Fig. 3. The SOP versus γ_T with $\overline{\gamma}_b$ =40dB for different shadowing scenarios.

all users will be examined when choosing the suitable user. However, the reduced percentage of our proposed scheme depends on the value of γ_T, when γ_T is large enough, the reduced percentage will decrease to zero. Whereas, when reviewing the results derived from Fig. 3, the lowest SOP occurs with a special γ_T. In this special γ_T, the corresponding reduced percentage is higher enough, which validates the advantage of our proposed scheme.

VII. Conclusions

In this paper, we have proposed a scheduling scheme based on the predefined threshold for the security enhancement

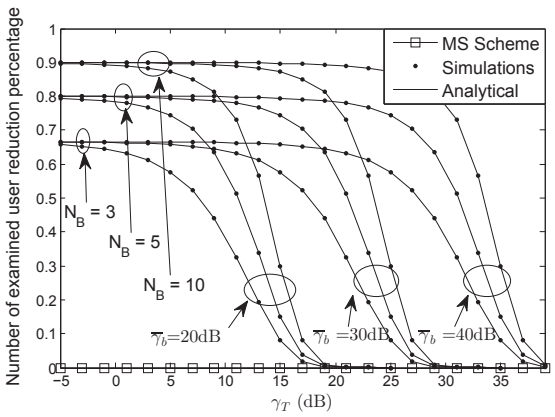


Fig. 4. The number of examined users reduction percentage versus γ_T with different N_B and $\overline{\gamma}_b$ for FHS.

in multiuser satellite communication networks with multiple eavesdroppers. Specifically, the closed-form expression for the secrecy outage probability has been derived. Besides, to get more insights at high SNRs, the asymptotic SOP for the considered network has also been obtained. Moreover, the average number of user examinations is also given, which validate the simplification of our proposed scheduling scheme. Numerical results have pointed out that our work has given a computationally efficient method to evaluate the secrecy performance of satellite networks.

Appendix A
Proof of Lemma 1

Based on the proposed scheduling scheme, we can get the CDF of γ_b as

$$F_{\gamma_b}(x) = \begin{cases} \sum_{i=2}^{N_B} \{\Pr[\max\{\gamma_{b1},\gamma_{b2},\ldots,\gamma_{b(i-1)}\} < \gamma_T, \&\gamma_T \le \gamma_{bi} < x] \\ +\Pr(\max\{\gamma_{b1},\gamma_{b2},\ldots,\gamma_{bN_B}\} < \gamma_T) \\ +\Pr(\gamma_T \le \gamma_{b1} < x)\}, x \ge \gamma_T \\ \Pr(\max\{\gamma_{b1},\gamma_{b2},\ldots,\gamma_{b(N_B-1)}\} < \gamma_T) \\ \times \Pr(\gamma_{bN_B} < x), x < \gamma_T. \end{cases} \tag{22}$$

Since all of the satellite links undergo independent identically distributed (i.i.d) SR fading, (22) can be rewritten as

$$F_{\gamma_b}(x) = \begin{cases} \sum_{i=2}^{N_B} \left\{ \left[F_{\gamma_{b_i}}(\gamma_T)\right]^{i-1} \left[F_{\gamma_{b_i}}(x) - F_{\gamma_{b_i}}(\gamma_T)\right] \right\} \\ +\left[F_{\gamma_{b_i}}(x) - F_{\gamma_{b_i}}(\gamma_T)\right] + \left[F_{\gamma_{b_i}}(\gamma_T)\right]^{N_B}, x \ge \gamma_T \\ \left[F_{\gamma_{b_i}}(\gamma_T)\right]^{N_B-1} F_{\gamma_{b_i}}(x), x < \gamma_T. \end{cases} \tag{23}$$

After some simplification, (23) can be rewritten as (9). The proof is completed.

Appendix B
Proof of Lemma 2

In order to investigate the asymptotic analysis, we should obtain the asymptotic expressions for I_1, I_2 and I_3.

$$I_1^{\infty}=\frac{\alpha_b}{\bar{\gamma}_{bi}}\left[F_{\gamma_{bi}}^{\infty}\left(\gamma_T\right)\right]^{N_B-1}\sum_{k_{e1}=0}^{m_e-1}\cdots\sum_{k_{eN_E}=0}^{m_e-1}\Xi\left(N_E\right)\left\{\frac{\gamma_0\gamma\left(\Lambda_e,H\left(\gamma_T\right)\Delta_e\right)}{\Delta_e^{\Lambda_e}}+\frac{\left(\gamma_0+1\right)\gamma\left(\Lambda_e+1,H\left(\gamma_T\right)\Delta_e\right)}{\Delta_e^{\Lambda_e+1}}\right\},\tag{24a}$$

$$I_2^{\infty}=\sum_{k_{e1}=0}^{m_e-1}\cdots\sum_{k_{eN_E}=0}^{m_e-1}\Xi\left(N_E\right)\times\left\{\left\{1-\sum_{i=0}^{N_B-1}\left[F_{\gamma_{bi}}^{\infty}\left(\gamma_T\right)\right]^i\left(1-\frac{\alpha_b}{\bar{\gamma}_{bi}}\gamma_0\right)\right\}\frac{\Gamma\left(\Lambda_e,H\left(\gamma_T\right)\Delta_e\right)}{\Delta_e^{\Lambda_e}}+\frac{\alpha_b\left(\gamma_0+1\right)\sum_{i=0}^{N_B-1}\left[F_{\gamma_{bi}}^{\infty}\left(\gamma_T\right)\right]^i}{\bar{\gamma}_{bi}\Delta_e^{\Lambda_e+1}\Gamma^{-1}\left(\Lambda_e+1,H\left(\gamma_T\right)\Delta_e\right)}\right\},\tag{24b}$$

$$I_3^{\infty}=\sum_{k_{e1}=0}^{m_e-1}\cdots\sum_{k_{eN_E}=0}^{m_e-1}\Xi\left(N_E\right)\times\left\{\left\{1-\sum_{i=0}^{N_B-1}\left[F_{\gamma_{bi}}^{\infty}\left(\gamma_T\right)\right]^i\left(1-\frac{\alpha_b}{\bar{\gamma}_{bi}}\gamma_0\right)\right\}\frac{\left(\Lambda_e-1\right)!}{\Delta_e^{\Lambda_e}}+\frac{\alpha_b\left(\gamma_0+1\right)\sum_{i=0}^{N_B-1}\left[F_{\gamma_{bi}}^{\infty}\left(\gamma_T\right)\right]^i\Lambda_e!}{\bar{\gamma}_{bi}\Delta_e^{\Lambda_e+1}}\right\}.\tag{24c}$$

By substituting (17) and (7b) into (13), (14) and (15), the asymptotic I_1, I_2 and I_3 can be obtained, respectively, shown as (24a), (24b) and (24c) which are shown at the top of this page, where $F_{\gamma_{bi}}^{\infty}\left(\gamma_T\right)\approx\frac{\alpha_b}{\bar{\gamma}_{bi}}\gamma_T$.

Recalling (18), it can be seen that we just need the equation with relation with $\bar{\gamma}_{bi}$, so I_1^{∞}, I_2^{∞} and I_3^{∞} can be rewritten as

$$I_1^{\infty}=\frac{\alpha_b}{\bar{\gamma}_{bi}}\left[F_{\gamma_{bi}}^{\infty}\left(\gamma_T\right)\right]^{N_B-1}\sum_{k_{e1}=0}^{m_e-1}\cdots\sum_{k_{eN_E}=0}^{m_e-1}\Xi\left(N_E\right)\times\left\{\frac{\gamma_0\gamma\left(\Lambda_e,H\left(\gamma_T\right)\Delta_e\right)}{\Delta_e^{\Lambda_e}}+\frac{\left(\gamma_0+1\right)\gamma\left(\Lambda_e+1,H\left(\gamma_T\right)\Delta_e\right)}{\Delta_e^{\Lambda_e+1}}\right\},\tag{25a}$$

$$I_2^{\infty}=\sum_{k_{e1}=0}^{m_e-1}\cdots\sum_{k_{eN_E}=0}^{m_e-1}\frac{\Xi\left(N_E\right)\alpha_b\left(\gamma_0+1\right)\sum_{i=0}^{N_B-1}\left[F_{\gamma_{bi}}^{\infty}\left(\gamma_T\right)\right]^i}{\bar{\gamma}_{bi}\Delta_e^{\Lambda_e+1}\Gamma^{-1}\left(\Lambda_e+1,H\left(\gamma_T\right)\Delta_e\right)},\tag{25b}$$

$$I_3^{\infty}=\sum_{k_{e1}=0}^{m_e-1}\cdots\sum_{k_{eN_E}=0}^{m_e-1}\frac{\Xi\left(N_E\right)\alpha_b\left(\gamma_0+1\right)\sum_{i=0}^{N_B-1}\left[F_{\gamma_{bi}}^{\infty}\left(\gamma_T\right)\right]^i\Lambda_e!}{\bar{\gamma}_{bi}\Delta_e^{\Lambda_e+1}}.\tag{25c}$$

Then, by substituting (25) into (18), the proof is completed.

REFERENCES

[1] M. K. Arti, and S. K. Jindal, "OSTBC transmission in shadowed-Rician land mobile satellite links," *IEEE Trans. Veh. Tech.*, vol. 65, no. 7, pp. 5771-5777, Jul. 2016.

[2] B. Li, Z. Fei, et al, "Robust chance-constrained secure transmission for cognitive satellite-terrestrial networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4208-4219, May. 2018.

[3] D. K. Petraki, M. P. Anastasopoulos, and S. Papavassiliou, "Secrecy capacity for satellite networks under rain fading," *IEEE Trans. Dependable Secure computing.*, vol. 8, no. 5, pp. 778-783, Sep. 2011.

[4] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[5] K. An, et al, "On the secrecy performance of land mobile satellite systems," IEEE Access, vol. 6, pp. 39606-39620, July 2018.

[6] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," *IEEE Trans. Commun.*, vol. 63, no. 8, pp. 2959-2971, Aug. 2015.

[7] K. Guo, B. Zhang, Y. Huang, and D. Guo, "Secure performance analysis of satellite communication networks in Shadowed Rician channel," *in Proc ISSPIT 2016*, Dec. 2016, Limassol. Cyprus, pp. 156-159.

[8] V. Bankey and P. K. Upadhyay, "Secrecy Outage Analysis of Hybrid Satellite-Terrestrial Relay Networks with Opportunistic Relaying Schemes," *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, Jun. 2017, Sydney, NSW, pp. 1-5.

[9] L. Zhen, H. Qin, et al, "Random access preamble design and detection for mobile satellite communication systems," *IEEE J. Sel. Area Commun.*, vol. 36, no. 2, pp. 280-291, Feb. 2018.

[10] D. Christopoulos, S. Chatzinotas et al, "Multicast multigroup precoding and user scheduling for frame-based satellite communications," *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 4695-4707, Apr. 2015.

[11] M. A. Vazquez, M. R. B. Shankar, C. Kourogiorgas, P.-D. Arapoglou, V. Icolari, S. Chatzinotas, A. D. Panagopoulos, and A. I. P-Neria, "Precoding, scheduling and link adaptation in mobile interactive multibeam satellite systems," *IEEE J. Sel. Area Commun.*, publised online.

[12] 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 Trans. Wireless Commun.*, vol. 2, no. 3, pp. 519-528, May. 2003.

[13] K. An, M. Lin, J. Ouyang, and W. P. Zhu, "Secure transmission in cognitive satellite terrstrial networks," *IEEE J. Sel. Area*, vol. 34, no. 11, pp. 3025-3037, Nov. 2016.

[14] K. Guo, K. An, B. Zhang, Y. Huang, and G. Zheng, "Outage analysis of cognitive hybrid satellite-terrestrial networks with hardware impairments and multi-primary users," *IEEE Wireless Commun. Lett.*, publised online.

[15] K. An, M. Lin, T. Liang, J.-B. Wang, J. Wang, Y. Huang, and A. L. Swindlehurst, "Performance analysis of multi-antenna hybrid satellite-terrestrial relay networks in the presence of interference," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4390-4404, Nov. 2015.

[16] K. An, et al, "Performance limits of cognitive FSS and terrestrial FS for Ka-band," IEEE Trans. Aerospace and Electronic Systems, to be published, Dec. 2018.

[17] I. S. Gradshteyn, I. M. Ryzhik, et al, "Table ofintegrals, series and products," *7thed. Amsterdam*, Boston: Elsevier, 2007.

[18] N. I. Miridakis, D. D. Vergados, and A. Michalas, "Dual-hop communication over a satellite relay and shadowed Rician channels," *IEEE Trans. Veh. Tech.*, vol. 64, no. 9, pp. 4031-4040, Sep. 2015.