Physical Layer Security for Multiuser Satellite Communication Systems With Threshold-Based Scheduling Scheme

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

Abstract—Satellite communication (SatCom) has attracted much attention due to its inherent characteristics. Security issues have gained severe concerns in SatCom since it is susceptible to be illegally eavesdropped by malicious ground stations within large-scale wireless coverage. In this paper, we investigate the physical layer security of a multiuser SatCom system in the presence of multiple eavesdroppers. Particularly, we propose a threshold-based scheduling scheme, where the geographically clustered eavesdroppers with both the colluded and collaborated eavesdropping scenarios are assumed. Specifically, 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. Moreover, we obtain a closed-form expression for the average secrecy capacity (ASC) of the considered system under the proposed user scheduling scheme. In order to get further insights of the proposed scheduling scheme at high signal-to-noise ratios (SNRs), the asymptotic analysis for the SOP and ASC is also demonstrated. 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 deduce that with the proposed scheme, a comparable system performance with regard to the maximal selection (MS) scheme can be achieved.

Index Terms—Satellite communication (SatCom), secrecy outage probability (SOP), average secrecy capacity (ASC), 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 a plethora of applications such as smart grid, Internet-of-Thing (IoT), wireless sensor networks, space-based cloud for big data, vehicular ad-hoc networks etc (see [1], [2] and the references therein). It is viewed as a key element in emergency rescue, such as earthquake, fire disaster and transoceanic communication that the terrestrial communication can not cover [3], [4]. SatCom is the key point of the beyond 5 generation (B5G) networks, which has already attracted much attention [5]–[7].

A. Background

Nevertheless, owing to the inherent nature of satellite broadcasting and coverage of huge areas, SatComs are easily to be exposed to various security issues. Secure information transmission has aroused extensive interest from the wireless communications community in order to prevent eavesdroppers from taking advantage of the broadcast nature of radio propagation medium to intercept confidential messages. Conventionally, various cryptographic protocols have been developed and applied in the upper layers to achieve transmission security on the assumption of an error-free link in the physical layer. However, the limitations behind these cryptographic protocols lie in secret key distribution and management, as well as its extreme computational complexity of mathematical operations [8]. Alternatively, physical layer security (PLS) has been introduced as an attractive method to guarantee secure transmission by exploiting the distinct characteristics of wireless channels (e.g., fading or noise). The concept of PLS was first introduced in Shannon’s pioneering work [9] from an information theoretic perspective.
Subsequently, wiretap channel was introduced in [10], where it demonstrated that perfect security can be obtained when the quality of legitimate channel is superior to that of the wiretap channel. Traditionally, the security issues in SatComs are also addressed by encryption, such as the advanced encryption standard (AES) [11], [12]. However, the absolute security cannot be perfectly guaranteed by the traditional encryption method with the increasing ability of the eavesdropper’s computation and decoding [13]. Moreover, PLS provides a prospective approach in the SatComs when compared with such protocols e.g. tunneling may lead to significant transmission overhead in clear detriment of quality of service (QoS).

B. Related Works

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 [14]. In [15], the authors analyzed the non-zero probability of secrecy capacity, SOP and ASC for the SatComs in the Shadowed-Rician (SR) channel. In [16], the authors investigated the secrecy performance of a hybrid satellite-terrestrial relay network.

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 [17]. However, 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 [18], the authors proposed a novel optimization problem to satisfy the need to frame multiple users per transmission. In [19], the authors studied the problem of pre-coding, scheduling and link adaptation in mobile interactive SatComs.

However, the former works mainly considered a single legitimate user and a single eavesdropper. In practical scenes, multiple legitimate users and eavesdroppers is a common scene in satellite communication systems [20]–[24]. In [21], the secrecy performance of SatComs was analyzed with multiple legitimate users and a single eavesdropper in the SatComs. In [22] and [23], the secrecy performance of SatComs with multiple legitimate users and one eavesdropper was analyzed. In [24], the ASC was analyzed for the satellite communication systems with a proposed legitimate users scheduling. In [25], the authors analyzed the secrecy performance for satellite communication systems with one user and one eavesdropper. In [26], the authors obtained the closed-form expressions for the SOP and ASC of the considered network with maximal ratio combining (MRC) scheme using in the legitimate user and analyzed the PLS. In [27], the authors analyzed the PLS for the SatComs with multiple legitimate users and channel estimation errors. In [28], the authors investigated the outage performance for the decode-and-forward (DF) satellite relaying network with multiple legitimate users and threshold-based scheme. In [29] and [30], the authors analyzed the secrecy performance for the integrated satellite terrestrial relay networks with multiple eavesdroppers and multiple legitimate users with a single terrestrial relay. However, until now, there is few published paper analyzing the secrecy performance for satellite communication system with multiple legitimate users and multiple eavesdroppers on the foundation of user scheduling. In [16] and [31], the authors analyzed the secrecy problem in hybrid satellite-terrestrial relay networks with multiple legitimate users, multiple eavesdroppers and multiple terrestrial relays.

C. Our Contributions

In this paper, by considering the satellite links undergo SR fading and the impacts of satellite beam pattern and path loss on deploying reliable SatComs, 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 SOP and ASC, asymptotic SOP and ASC, along with the reduced percentage with respect to the number of legitimate user examination, are derived, respectively.

The main contributions of this paper is summarized as follows:

- We provide a secrecy satellite communication model with multiple users. Particularly, a new user-scheduling scheme is proposed to enhance the secrecy system performance.
- We derive the closed-form expressions for the SOP based on the proposed user scheduling scheme, which provide efficient ways to evaluate the SOP.
- To gain the impact of the proposed user scheduling scheme on the ASC, the closed-form expressions for the ASC are also derived, which give the useful methods to estimate ASC.
- In order to obtain the secrecy performance at high signal-to-noise ratios (SNRs), the asymptotic expressions for SOP and ASC of the considered system are obtained to show the secrecy diversity order and coding gain.
- The average number of legitimate user examinations is also derived to show the advantage of our proposed user scheduling scheme.

The rest of this paper is organized as follows. Section II introduces the system model followed by the problem formulation. In Section III, the secrecy performance analysis of the considered system is conducted. In particular, the analytical expressions for the OP and ASC are derived. In addition, the asymptotic expressions of the OP and ASC under the high SNR assumption are also given in Section III. In Section IV, the average number of legitimate user examinations is given. In Section V, some numerical results are provided to validate the analytical performance evaluation. In Section VI, a brief summary of our work in this paper is given.

Notations: Vectors are represented by lowercase bold typeface letters, $(\cdot)^H$ denotes the Hermitian transpose, $|\cdot|$ represents the Euclidean norm of a vector, $|\cdot|$ stands for the absolute value of a complex scalar, $\exp(\cdot)$ is the exponential function, $E[\cdot]$ denotes the expectation operator, $CN(\alpha, \mathbf{B})$ represents
the complex Gaussian distribution of a random vector \( \mathbf{a} \) and covariance matrix \( \mathbf{B} \), \( \mathbf{B}^{M \times N} \) stands for an \( M \)-by-\( N \) dimensional complex positive semi-definite matrix. \( f_x(\cdot) \) and \( F_x(\cdot) \) denote the probability density function (PDF) and the cumulative distribution function (CDF) of random variable \( x \), respectively. The abbreviations and acronyms are given in Table I.

II. SYSTEM MODEL

As illustrated in Fig. 1, we 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 Bobs and Eves are equipped with single antenna, which is practical in certain multiuser scenarios such as wireless sensors, IoT and broadcasting networks.\(^1\) 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

\[^1\text{We should note that, in order to simplify the analysis, we assume that all nodes are equipped with a single antenna in this paper. However, the following analysis is still fit for the case that all nodes are equipped with multiple antennas. It is very interesting for us to investigate the case that the satellite is equipped with multiple antennas in our future work. Nevertheless, our presented results will serve as a benchmark of the secrecy system performance and provide useful guidelines for the secrecy land mobile satellite (LMS) communication systems.}\]

SR fading.\(^2\) For notational convenience, the channel coefficient between the satellite and the \( i \)-th legitimate user is denoted as \( h_{b_i} \), and the channel coefficient between the satellite and the \( j \)-th eavesdropper is termed as \( h_{e_j} \). 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 transmitted by the satellite satisfying \( \mathbb{E}[|s(t)|^2] = 1 \), the signals received at the \( i \)-th Bob and the \( j \)-th Eve are, respectively, written as

\[
y_{b_i}(t) = \sqrt{P} h_{b_i} s(t) + n_{b_i}(t),
\]

\[
y_{e_j}(t) = \sqrt{P} h_{e_j} s(t) + n_{e_j}(t),
\]

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

\[
h_P = Q_P g_P, P \in \{b_i, e_j\},
\]

\(^2\text{The SR model that is proposed originally by Loo has found wide applications in different frequency bands such as the UHF-band, L-band, S-band, and Ka-band}\)

where \( g_P \) is the channel coefficient following SR fading [33], [34], [35], 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

\[
Q_P = \frac{C \sqrt{F_{r_P} F_{r_P}}}{4\pi f d_P \sqrt{K_W T_W}},
\]

where \( C \) is the light velocity, \( f \) is the frequency of the carrier, \( d_P \) is the propagation distance. \( K_W = 1.38 \times 10^{-23} \text{J/m} \) is the Boltzman constant, \( T_W \) is the receive noise temperature, and \( W \) denotes the carrier bandwidth. Meanwhile, \( F_{r_P} \) presents the receiving gain.
According to [36], the antenna gain for the Earth Station (ES) with parabolic antenna can be approximately expressed as

\[
F_{r,p}(dB) = \begin{cases} \bar{G}_{\text{max}}, & 0^\circ < \beta < 1^\circ \\ 32 - 25 \log \beta, & 1^\circ < \beta < 48^\circ \\ -10, & 48^\circ < \beta \leq 180^\circ, \end{cases}
\]

where \(\bar{G}_{\text{max}}\) is the maximum beam gain at the boresight, and \(\beta\) is the off-boresight angle.

\(F_{i,p}\) presents the beam gain of the satellite, which can be nearly given by [37]

\[
F_{i,p} = F_{\text{max}} \left( \frac{J_1(x)}{2x} + \frac{36J_3(x)}{x^3} \right)^2,
\]

where \(F_{\text{max}}\) denotes the maximal satellite beam gain and \(x = 2.07123 \sin \theta / \sin \theta_{3dB}\), where \(\theta\) is the angle between the location of the corresponding receiver and the beam carrier with respect to the satellite, and \(\theta_{3dB}\) is the 3 dB angle, \(J_1\) and \(J_3\) present the first kind bessel function of order 1 and 3, respectively [38]. In order to get the best system performance, hence we set \(\theta = 0\), as a result of \(F_{i,p} \approx F_{\text{max}}\). On this foundation, we could obtain \(h_p = Q_{\text{max}}^p g_p\) with \(Q_{\text{max}}^p = \frac{C\sqrt{F_{\text{max}} F_{r,p}}}{2\pi f_p q K_W T_W}\).

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

\[
\begin{align*}
\gamma_{bi} & = \theta_{bi} |g_{bi}|^2, \\
\gamma_{ej} & = \theta_{ej} |g_{ej}|^2,
\end{align*}
\]

where \(\theta_{bi} = P|Q_{bi}|^2/\delta_{bi}^2\) is the average SNR of the satellite to the \(i\)-th Bob link and \(\theta_{ej} = P|Q_{ej}|^2/\delta_{ej}^2\) 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 are derived.

#### 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 MRC linear processing scheme among Eves, we obtain the equivalent instantaneous SNR of Eves as

\[
\gamma_e = \sum_{j=1}^{N_E} \gamma_{ej},
\]

where \(\bar{Q}_{qi}/\bar{\delta}_{qi}^2\) is the average SNR of the satellite to the \(i\)-th Bob link and \(\bar{Q}_{ej}/\bar{\delta}_{ej}^2\) that of the satellite to the \(j\)-th Eve link.

Before analyzing the secrecy performance of the system, we first give the CDF of \(\gamma_{bi}\) and the PDF of \(\gamma_e)\) [39], respectively, as

\[
F_{\gamma_{bi}}(x) = 1 - \alpha_b \sum_{k_b=0}^{m_b=1} \frac{\zeta(k_b) (k_b)!}{\Gamma(k_b+1)} x^{k_b} e^{-\Delta_{b} x},
\]

\[
f_{\gamma_{ei}}(x) = \sum_{k_e=0}^{m_e=1} \cdots \sum_{k_e=N_E=0} \zeta(N_E) x^{N_E-1} e^{-\Delta_{e} x},
\]

where \(\zeta(k_b) = \frac{(-\alpha_b)^{k_b} (1-m_b)^{k_b}}{k_b!^{m_b}}\) with \((\cdot)^{m}\) is the Pochhammer symbol [38], \(\Delta_e = 1/(\bar{\theta}_{ei})\), \(\alpha_l = (\frac{2b_l m_l}{2b_l m_l + 4l})^{\frac{1}{2b_l}}\), \(\beta_l = 1/(2b_l)\), \(\sigma_l = \frac{\Omega_l}{2b_l (2b_l m_l + 1)}\) with \(\Omega_l\), \(2b_l\) and \(m_l(l \in \{b_i; e\})\) are the average power of line-of-sight (LOS), multiple path components and the fading severity parameters, respectively.

\[
F_{\gamma_{ej}}(x) = \prod_{p=1}^{N_E} \zeta(k_e) \alpha_{N_E} \prod_{q=1}^{N_E-1} B \left( \sum_{s=1}^{q} k_s + q, k_{q+1} + 1 \right),
\]

and \(\Lambda_e = \sum_{p=1}^{N_E} k_p + N_E\), where \(B(\cdot, \cdot)\) denotes the Beta function [38].

Traditional scheduling schemes select the best user to be served based on the CSI examination of each user, which requires computationally demanding iterative process [19]. Given the constrained feedback resources and limited on-board processing capability in the 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, a scheduling threshold \(\gamma_T\) is set. Alice first check the SNR \(\gamma_{bi}\), if \(\gamma_{bi} \geq \gamma_T\), this transmitted link is selected, no other link will be checked, i.e., \(\gamma_b = \gamma_{bi}\).
- Secondly, if \(\gamma_{bi} < \gamma_T\), Alice will check the left \(N_B - 2\) Bobs’ links, if \(\gamma_{bi} > \gamma_T\), the \(i\)-th Bob link will be chosen, i.e., \(\gamma_b = \max_{j \in \{1,i\}} (\gamma_{bji})\). Otherwise, Alice will examine the \((i+1)\)-th link.
- Thirdly, if \(\gamma_{bi} \geq \gamma_{bi-1}\), \(i > 1\), the \((NB-1)\)-th link will be chosen. Otherwise, Alice will not check the \(N_B\)-th link and choose the \(N_B\)-th link directly as the transmitted link no matter what the SNR is, i.e., \(\gamma_b = \gamma_{bN_B}\). According to the detailed scheduling scheme, we can obtain the following scheduling process as Fig. 2.

**Theorem 1.** Based on the aforementioned analysis and assuming all Bobs’ links having the identical fading parameters, we can obtain the CDF of \(\gamma\) as

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

where \(F_{\gamma_{bi}} (x)\) has been derived in (8a).

**Proof:** See Appendix A.
where $R_0 = \log_2(1 + \gamma_0)$, $\gamma_0$ 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 (11), it can be expressed as

$$P_{\text{out}} (R_0) = \Pr \left[ \gamma_b < \gamma_0 + (\gamma_0 + 1) \gamma_e \right] = \int_0^\infty F_{\gamma_b} (\gamma_0 + (\gamma_0 + 1) \gamma_e) dx. \quad (12)$$

From (10), we know that the proposed scheduling scheme relies on the predefined threshold $\gamma_T$, here we recommend a boundary point $H(\gamma_T) = \frac{\gamma_T - \gamma_0}{\gamma_0 + 1}$ to make SOP more tractable.\(^5\) Hence, the SOP can be rewritten as

$$P_{\text{out}} (R_0) = \begin{cases} 
\int_0^{H(\gamma_T)} F_{\gamma_b} (Y(x)) f_{\gamma_b} (x) \, dx \\
\int_{H(\gamma_T)}^\infty F_{\gamma_b} (Y(x)) f_{\gamma_b} (x) \, dx, H(\gamma_T) \geq 0 \\
\int_0^\infty F_{\gamma_b} (Y(x)) f_{\gamma_b} (x) \, dx, H(\gamma_T) < 0,
\end{cases} \quad (13)$$

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

By substituting (8b) and (10) into $I_1$, $I_2$ and $I_3$, they can be derived, respectively, as (14), (15), and (16), which are shown at the bottom of this page, where

$$F_{\gamma_b} (\gamma_T) = 1 - \alpha_b \sum_{k_b=0}^{m_b-1} \sum_{k_e=N_b=0}^{m_e-1} \frac{\zeta(k_b) (k_b!)}{v! \Delta^e b_{k_b+1}^{\sum_k} \Delta^e_b} e^{-(\gamma_0 + 1) x} \frac{\Gamma(\Delta_e, \gamma_T H(\gamma_T))}{\Gamma(\Delta_e, \gamma_T H(\gamma_T))}. \quad (17)$$

\(^4\)The main channel condition here is that $C_B > C_E$, which emphasizes the fact the main channel must be better that the wiretap channel, irrespective of the eavesdroppers computational power, which is another motivation to exploit cooperative communications to provided this much-desired advantages.

\(^5\)Due to the fact that the switched threshold $\gamma_T$ is incorporated in the CDF of $\gamma_b$ as shown in (10) there exists relationship between the term $\gamma_0 + (\gamma_0 + 1) x$ and $\gamma_T$ in (12), i.e., $\gamma_0 + (\gamma_0 + 1) x > \gamma_T$ or $\gamma_0 + (\gamma_0 + 1) x < \gamma_T$. To facilitate the analysis in (12), hence we introduce a bound point as $H(\gamma_T) = \frac{\gamma_T - \gamma_0}{\gamma_0 + 1}$. 

---

**Fig. 2.** Diagram of the proposed scheduling scheme.

**B. 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 $R_0$ [14], is mathematically formulated as

$$P_{\text{out}} (R_0) = \Pr (C_S < R_0), \quad (11)$$

The following equations are derived, respectively, as (14), (15), and (16), shown at the bottom of this page.
C. Average Secrecy Capacity

In this subsection, in order to investigate the secrecy performance deeply, we analyze the ASC of the considered system.

By recalling the definition of the achieved secrecy rate, we can obtain

\[
C_S = \int_0^\infty \int_z^\infty \frac{f_{\gamma_n}(z)}{1+z} \left[ \int_z^\infty f_{\gamma_b}(x) dx \right] dz
\]

\[
= \frac{1}{\ln 2} \int_0^\infty \frac{F_{\gamma_n}(z)}{1+z} [1 - F_{\gamma_b}(z)] dz
\]

\[
= \frac{1}{\ln 2} \int_0^\infty F_{\gamma_b}(z) [1 - F_{\gamma_n}(z)] dz
\]

\[
+ \frac{1}{\ln 2} \int_0^\infty F_{\gamma_n}(z) [1 - F_{\gamma_b}(z)] dz.
\]

Next, the closed-form expression for (19) can be obtained in the following Theorem 2.

**Theorem 2.** The ASC of the considered system is

\[
C_S = C_1 + C_2,
\]

where \(C_1\) and \(C_2\) are given in (23) and (24) shown at the bottom of this page, with \(H_1(a, b, c)\) and \(H_2(a, b, c)\) are, respectively, as follows:

\[
H_1(a, b, c) = \int_0^a \frac{\exp(-bx)x^c}{1+x} dx
\]

\[
H_2(a, b, c) = \int_a^\infty \frac{\exp(-bx)x^c}{1+x} dx
\]

\[
= \exp(b) \sum_{t_i=0}^c \left( \frac{c}{t_i} \right)(-1)^{c-t_i} b^{-t_i} \times [\Gamma(t_1, b) - \Gamma(t_1, b(a+1))],
\]

and

\[
H_1(a, b, c) = \int_0^\infty \frac{\exp(-bx)x^c}{1+x} dx
\]

\[
= \exp(b) \sum_{t_i=0}^c \left( \frac{c}{t_i} \right)(-1)^{c-t_i} [b^{-t_i}\Gamma(t_1, b(a+1))],
\]

where \(\Gamma(\cdot, \cdot)\) is the incomplete gamma function [38, eq. 8.35].

**Proof:** See Appendix B.

D. Asymptotic Analysis

1) Asymptotic Secrecy Outage Probability: Although the exact expression of SOP has been obtained, it is hard to derive more insights from (13). Therefore, in what follows, the asymptotic analysis for the SOP will be derived. In the high SNR regime, i.e., \(\gamma_{hi} \to \infty\). Hence, only the first summation term of \(F_{\gamma_{hi}}(x)\) should be taken into consideration, since it momentarily affects the overall performance while all the other terms approach zero. Accordingly, (8a) can be further expressed as [27]

\[
F_{\gamma_{hi}}(x) = \frac{\alpha_b}{\gamma_{hi}} x + o(x),
\]

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

**Theorem 3.** In order to analyze the diversity order and coding gain conveniently, the asymptotic SOP can be expressed as

\[
P_{out}(R_0) = \Phi \left( \frac{1}{\gamma_{hi}} \right)^\Psi,
\]

where \(\Psi\) is the high order infinitesimal of \(\psi\).
where the secrecy diversity order \( \Psi = 1 \) and the secrecy coding gain is
\[
\Phi = \begin{cases} 
T^\infty \bar{\gamma}_b + T^\infty \bar{\gamma}_e, & H(\gamma_T) \geq 0 \\
T^\infty \bar{\gamma}_b, & H(\gamma_T) < 0.
\end{cases}
\]

Proof: See Appendix C.

2) Asymptotic Average Secrecy Capacity: In what follows, to evaluate the impact of key system parameters on the average secrecy capacity in depth, we also look into the ASC at high SNRs. To this end, we give two representative issues to characterize the asymptotic ASC, i.e., the high SNR slope and the high SNR power offset. Also, the CDF of \( \gamma_e \) is given by
\[
F_{\gamma_e}(x) = 1 - \eta_{\gamma_e}(x)
= 1 - \frac{m_e - 1}{k_e} \sum_{k_e=0}^{m_e-1} \frac{\varepsilon}{t!} \sum_{t=0}^{\Lambda_e - 1} (N_E) (\Lambda_e - 1)! x^t e^{-\Delta_e x},
\]
where
\[
\eta_{\gamma_e}(x) = \frac{m_e - 1}{k_e} \sum_{k_e=0}^{m_e-1} \frac{\varepsilon}{t!} \sum_{t=0}^{\Lambda_e - 1} (N_E) (\Lambda_e - 1)! x^t e^{-\Delta_e x}.
\]

Theorem 4. The ASC in high SNR regime is derived as
\[
C^\infty_S = w_1 - w_2,
\]
where \( w_1 \) and \( w_2 \) are given as
\[
w_1 = \frac{\alpha_b}{\ln 2} \sum_{k_b=0}^{m_b-1} \zeta(k_b) H_3(k_b + 1, \Delta_b),
\]
and \( \psi(\cdot) \) is the digamma function \([38, \text{eq. 8.36}]\).

Proof: See Appendix D.

To obtain further insights, we investigate the high SNR slope and the high SNR power offset, as two important parameters affecting the ASC at high SNRs. Hence, we rewrite the asymptotic ASC in (29) in a general form as \([14, 24]\)
\[
C^\infty_S = S_\infty \left( \ln(\bar{\gamma}_b) - T_\infty \right),
\]
where \( S_\infty \) is the high SNR slope in bits/s/Hz and \( T_\infty \) is the high SNR power offset in 3 dB units.

We first express the high SNR slope as
\[
S_\infty = \lim_{\bar{\gamma}_b \to \infty} \frac{C^\infty_S}{S_\infty}.
\]
By substituting (30) into (35), it can be easily extracted that
\[
S_\infty = 1.
\]
From (36), we can conclude that the key parameters, such as the number of the legitimate users, the number of the eavesdroppers, the fading severity parameters and the switching threshold \( \gamma_r \), have no effect on the high SNR slope.

In the following, the high SNR power offset \( T_\infty \) as
\[
T_\infty = \lim_{\bar{\gamma}_b \to \infty} \left( \ln(\bar{\gamma}_b) - \frac{C^\infty_S}{S_\infty} \right).
\]
It is clear from (37) that the effects of the main channel and the eavesdropper’ channel on the asymptotic ASC rely on \( T_\infty \).

By inserting (36) and (29) into (37), we obtain \( T_\infty \) as
\[
T_\infty = T^b_\infty + T^c_\infty,
\]
where
\[
T^b_\infty = \frac{\alpha_b}{\ln 2} \sum_{k_b=0}^{m_b-1} \zeta(k_b) \Gamma(k_b) [\psi(k_b) - \ln(\beta_b - \alpha_b)],
\]
and
\[
T^c_\infty = w_2.
\]

Remark 1: From the above analysis, we find that the high SNR power offset is independent of \( \bar{\gamma}_b \) and the contributions of the main channel and eavesdropper channel to \( T_\infty \) are characterized by \( T^b_\infty \) and \( T^c_\infty \), respectively. In particular, \( T^c_\infty \) quantifies the loss of ASC due to eavesdropping and as \( T^c_\infty \) increases with \( N_E \) with ASC decreasing.

IV. 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
\[
N^A = \sum_{i=0}^{N_B-1} \left[ F_{\gamma_b_i}(\gamma_T) \right]^i.
\]
As it is fact that \( F_{\gamma_b_i}(\gamma_T) \leq 1 \), we can obtain that
\[
N^A = 1 - \left[ F_{\gamma_b}(\gamma_T) \right]^{N_B}.
\]
Table II

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

Table III

| Shadowing                          | $m_P$ | $b_P$ | $\Omega_P$ |
|------------------------------------|-------|-------|------------|
| 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       |

From (42), we find that $N^A$ is decided by $N_B$ and $F_{\gamma_b}(\gamma_T)$. When $N_B \to \infty$, $N^A = 1/[1 - F_{\gamma_b}(\gamma_T)]$. So in this assumption, if we want to have a smaller $N^A$, $\gamma_T$ 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

$$RPN = 1 - N^A/N_B$$

$$= 1 - \left\{ 1 - \left[ F_{\gamma_b}(\gamma_T) \right]^{N_B} / \left[ 1 - F_{\gamma_b}(\gamma_T) \right] \right\} / N_B.$$

(43)

V. 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 by Matlab. The system parameters are given in Table II [37] and the shadowing coefficients of the satellite channel are provided in Table III [33], respectively. Without loss of generality, we set $\delta_2^b = \delta_2^e = 1$ and in all the plots we denote $\bar{\gamma}_b = \bar{\gamma}_e$. Moreover, the SR channel and the MC approach $10^{10}$ iterations for Figs. 1–3 and Figs. 5–8, besides $10^{11}$ iterations for Fig. 4.

Fig. 3 plots the SOP of the considered system versus $\gamma_b$ with $\gamma_T = 5$ dB and $\gamma_T = 10$ dB 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 $\gamma_T$, $N_B$ 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 $\gamma_T$ is presented. In addition, we can also find that the secrecy coding gain will be degraded when $N_E$ is larger.

Fig. 4 depicts the SOP versus $\gamma_T$ with $\gamma_b = 40$ dB for different shadowing scenarios. From the figure, we know that the optimal value of $\gamma_T$ which means the lowest SOP will change according to different channel shadowing severities. The heavier channel shadowing is, the smaller $\gamma_T$ will be. Moreover, we can obtain
Fig. 5. The ASC versus different $\bar{\gamma}_b$, different $\bar{\gamma}_e$ and different channel shadowing with $\gamma_T=5\,\text{dB}$, $N_E=1$ and $N_B=3$. That the SOP will be larger with the increasing SNR of the eavesdropper.

Fig. 5 provides the ASC versus different $\bar{\gamma}_b$, different $\bar{\gamma}_e$ and different channel shadowing with $\gamma_T=5\,\text{dB}$, $N_E=1$ and $N_B=3$. We can find that, the ASC will increase to be infinity when $\bar{\gamma}_b$ grows infinity. Moreover, we observe that when $\bar{\gamma}_E$ is larger, the ASC will be lower in the case of larger eavesdroppers’ power. At end, the ASC will be larger when the channel is under light shadowing.

Fig. 6 examines the ASC versus different $\bar{\gamma}_b$, different $N_E$ and different $\gamma_T$ with $\bar{\gamma}_e=5\,\text{dB}$ and $N_B=3$: FHS. It can be seen that, when $\gamma_T$ is larger, the ASC is improved, for the reason that better legitimate user’s link is selected. More interestingly, we derive that when $\gamma_b$ is larger enough, the values for different $\gamma_T$ cases are same, because when $\gamma_b$ is larger enough, every legitimate user’s link is better enough to overcome $\gamma_T$, which means every link is better enough. Lastly, it is noted that when $N_E$ is larger, the ASC will be lower.

Fig. 7 plots the ASC versus different $\bar{\gamma}_b$, different $N_B$ and different $\gamma_T$ with $\bar{\gamma}_e=5\,\text{dB}$ and $N_E=1$: FHS. We still find that when $\gamma_b$ is larger enough, at high SNRs, the values of ASC for different cases are same, which also means that all links are the suitable links to transmit the signals. However, when $\gamma_b$ is lower, there is a turning point showing that at lower SNRs (before the turning point), we should set $\gamma_T$ larger, at high SNRs (behind the turning point, not larger enough), the lower $\gamma_T$ is suitable.

Fig. 8 provides the reduced percentage in terms of the number of user examinations versus $\gamma_T$ with different $N_B$ and $\bar{\gamma}_b$ for FHS. As illustrated in this figure, we compare our proposed scheme with the maximal selection (MS) scheme (which is the best scheduling scheme [18], [19]). Intuitively, we can find that the reduced percentage of MS scheme is always zeros, which means that all users will be examined when choosing the suitable user. However, the reduced percentage of our proposed scheme depends on the value of $\gamma_T$, when $\gamma_T$ 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 $\gamma_T$. In this special $\gamma_T$, the corresponding reduced percentage is higher enough, which validates the advantage of our proposed scheme.
VI. CONCLUSION

In this paper, we have proposed a scheduling scheme based on the predefined threshold for the security enhancement of multiuser satellite communication networks with multiple eavesdroppers. Next, closed-form expressions for the SOP and ASC of the considered system have been derived. To get more insights at high SNRs, asymptotic expressions for the SOP and ASC have also been obtained. Moreover, the average number of user examinations were also given, which validated the simplification of our proposed scheduling scheme. We found that when the SNR of the system was larger enough, $\gamma_T$ and $N_B$ did not affect the ASC. Nevertheless at lower SNRs, it had serious effects. Finally, numerical results have pointed out that our work has given a computationally efficient method to evaluate the secrecy performance of SatComs.

APPENDIX A

PROOF OF THEOREM 1

Based on the proposed scheduling scheme, we can get the CDF of $\gamma_b$ as

$$F_{\gamma_b}(x) = \begin{cases} \sum_{i=2}^{N_b} \left\{ \operatorname{Pr} \left[ \max \{ \gamma_{b1}, \gamma_{b2}, \ldots, \gamma_{b(i-1)} \} < \gamma_T, \& \gamma_T \leq \gamma_b < x \right] \ight. \\
+ \operatorname{Pr} \left( \max \{ \gamma_{b1}, \gamma_{b2}, \ldots, \gamma_{bN_b} \} < \gamma_T \right) \\
+ \operatorname{Pr} \left( \gamma_T \leq \gamma_b < x \right), x \geq \gamma_T \\
\times \operatorname{Pr} \left( \gamma_b N_b < x \right), x < \gamma_T. \end{cases}$$

(44)

Since all of the satellite links undergo independent identically distributed (i.i.d) SR fading, (44) can be rewritten as

$$F_{\gamma_b}(x) = \begin{cases} \sum_{i=2}^{N_b} \left\{ \left[ F_{\gamma_{hi}}(\gamma_T) \right]^{-1} \left[ F_{\gamma_{hi}}(x) - F_{\gamma_{hi}}(\gamma_T) \right] \right\} \\
+ \left[ F_{\gamma_{hi}}(x) - F_{\gamma_{hi}}(\gamma_T) \right] + \left[ F_{\gamma_{hi}}(\gamma_T) \right]^{N_b-1}, x \geq \gamma_T \\
\left[ F_{\gamma_{hi}}(\gamma_T) \right]^{N_b-1} F_{\gamma_{hi}}(x), x < \gamma_T. \end{cases}$$

(45)

After some simplification, (45) can be rewritten as (10). The proof is completed.

APPENDIX B

PROOF OF THEOREM 2

Before doing this, with the help of [39], we first give the CDF of $\gamma_e$ as

$$F_{\gamma_e}(x) = 1 - \sum_{k_e=0}^{m_e-1} \cdots \sum_{k_e N_e=0}^{m_e-1} \frac{\Xi(N_E)(\Lambda_e - 1)!}{t! \Delta_e^{\Lambda_e-t}} x^t e^{-\Delta_e x}$$

(46)

From (19) and (20), we can obtain that

$$C_1 = \frac{1}{\ln 2} \int_0^{\gamma_T} \frac{F_{\gamma_b}(z)}{1 + z} \left[ 1 - F_{\gamma_b}(z) \right] dz$$

(47)

Then, by substituting the second part of (10) and (46) into (47), (47) can be rewritten as

$$C_1 = \frac{1}{\ln 2} \left( J_1 + J_2 - J_3 - J_4 \right)$$

(48)

where

$$J_1 = \int_0^{\gamma_T} \frac{\left\{ 1 - \left[ F_{\gamma_{hi}}(\gamma_T) \right]^{N_b-1} \right\} }{1 + x} dx$$

(49)

$$J_2 = \left[ F_{\gamma_{hi}}(\gamma_T) \right]^{N_b-1} \sum_{k=0}^{m_b-1} \sum_{k=0}^{m_b-1} \frac{\alpha_b \left( k_b \right) \left( k_b! \right)}{t! \Delta_b^{k_b-t+1}} \int_0^{\gamma_T} \frac{x^t e^{-\Delta_b x}}{1 + x} dx.$$ 

(50)

With the help of [24, eq. 48], $Q_1$ can be obtained as

$$Q_1 = H_1(\gamma_T, \Delta_b, l).$$

(51)

Then with the similar methods, $J_3$ and $J_4$ can be derived as

$$J_3 = \sum_{k_e=0}^{m_e-1} \cdots \sum_{k_e N_e=0}^{m_e-1} \sum_{t=0}^{\Lambda_e-1} \frac{\Xi(N_E)(\Lambda_e - 1)!}{t! \Delta_e^{\Lambda_e-t}} \int_0^{\gamma_T} \frac{x^t e^{-\Delta_e x}}{1 + x} dx$$

(52)

$$J_4 = \left[ F_{\gamma_{hi}}(\gamma_T) \right]^{N_b-1} \sum_{k=0}^{m_b-1} \sum_{k=0}^{m_b-1} \frac{\alpha_b \left( k_b \right) \left( k_b! \right)}{t! \Delta_b^{k_b-t+1}} \sum_{k_e=0}^{m_e-1} \cdots \sum_{k_e N_e=0}^{m_e-1} \sum_{t=0}^{\Lambda_e-1} \frac{\Xi(N_E)(\Lambda_e - 1)!}{t! \Delta_e^{\Lambda_e-t}} H_1(\gamma_T, \Delta_e, t),$$

(53)

Then by substituting (49), (50), (52) and (53) into (48), (23) will be derived.
Now, we refer to $C_2$. Also from (10) and (46), $C_2$ is given by

$$C_2 = \frac{1}{\ln 2} \int_{\gamma_T}^{\infty} \frac{F_{\gamma_2}(z)}{1 + z} [1 - F_{\gamma_2}(z)] \, dz. \quad (54)$$

Then by inserting the first part of (10) and (46) into (54), (54) can be rewritten as

$$C_2 = \frac{1}{\ln 2} (J_5 - J_6), \quad (55)$$

where $J_5$ and $J_6$ are, respectively, given by

$$J_5 = \sum_{i=0}^{N_B-1} \left[ F_{\gamma_i}^{\infty} \right] \sum_{k_i=0}^{m_i-1} \sum_{l=0}^{k_i} \alpha_i \delta \left( k_i, k_i! \right) \left( 1 + \nu_i \right) \int_{\gamma_T}^{\infty} \frac{x^l e^{-\Delta x}}{1 + x} \, dx. \quad (56)$$

With the help of [24, eq. 50], $Q_2$ can be rewritten as

$$Q_2 = \frac{H_2 (\gamma_T, \Delta_b, l).} {\Delta_b + \Delta_b, l + t}. \quad (57)$$

Then, using the same ways, $J_6$ is obtained as

$$J_6 = \sum_{i=0}^{N_B-1} \left[ F_{\gamma_i}^{\infty} \right] \sum_{k_i=0}^{m_i-1} \sum_{l=0}^{k_i} \alpha_i \delta \left( k_i, k_i! \right) \left( 1 + \nu_i \right) \int_{\gamma_T}^{\infty} \frac{x^l e^{-\Delta x}}{1 + x} \, dx. \quad (58)$$

Finally, taking $C_1$ and $C_2$ into (20), the proof is completed.

**Appendix C**

**Proof of Theorem 3**

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

By substituting (25) and (8b) into (14), (15) and (16), the asymptotic $I_1$, $I_2$ and $I_3$ can be obtained, respectively, shown as

$$I_1 = \frac{\alpha_b}{\gamma_{b_i}} \left[ F_{\gamma_i}^{\infty} \right] \sum_{i=0}^{N_i-1} \sum_{k_i=0}^{m_i-1} \sum_{l=0}^{k_i} \alpha_i \delta \left( k_i, k_i! \right) \left( 1 + \nu_i \right) \left( \gamma_{b_i} \right) \frac{T_i}{\gamma_{b_i}^{\Delta b_i}} \frac{\Delta b_i}{\Delta b_i + 1} \left( \Delta b_i + 1, H (\gamma_T) \Delta b_i \right), \quad (59)$$

$$I_2 = \sum_{i=0}^{N_i-1} \sum_{k_i=0}^{m_i-1} \sum_{l=0}^{k_i} \alpha_i \delta \left( k_i, k_i! \right) \left( 1 + \nu_i \right) \left( \gamma_{b_i} \right) \frac{T_i}{\gamma_{b_i}^{\Delta b_i}} \frac{\Delta b_i}{\Delta b_i + 1} \left( \Delta b_i + 1, H (\gamma_T) \Delta b_i \right), \quad (60)$$

$$I_3 = \sum_{i=0}^{N_i-1} \sum_{k_i=0}^{m_i-1} \sum_{l=0}^{k_i} \alpha_i \delta \left( k_i, k_i! \right) \left( 1 + \nu_i \right) \left( \gamma_{b_i} \right) \frac{T_i}{\gamma_{b_i}^{\Delta b_i}} \frac{\Delta b_i}{\Delta b_i + 1} \left( \Delta b_i + 1, H (\gamma_T) \Delta b_i \right). \quad (61)$$

Next, $w_1$ and $w_2$ will be derived. Recalling (20), it can be rewritten as

$$C_S = \frac{1}{\ln 2} \int_{0}^{\infty} \frac{1 - \eta_{\gamma}(z)}{1 + z} \, dz = w_1 - w_2, \quad (65)$$

where

$$w_1 = \frac{1}{\ln 2} \int_{0}^{\infty} \ln (1 + z) \, f_{\gamma_2}(x) \, dx, \quad (66a)$$

$$w_2 = \frac{1}{\ln 2} \int_{0}^{\infty} \eta_{\gamma}(z) \, dz f_{\gamma_2}(x) \, dx. \quad (66b)$$
We should note that when \( \gamma_b \) is large enough, we obtain
\[
\ln(1 + x) \approx \ln x \quad [14], [27]
\]
and the SNR of every Bob’s transmitted link is good enough to receive the signal, hence we have
\[
f_{\gamma_b}(x) = \alpha_{n} \sum_{k_b=0}^{m_b-1} \zeta(k_b) x^{k_b} \exp(-\Delta_b x). \quad (67)
\]
Then, with the help of (67), (66a) and [38, eq. 4.352.1], \( w_1 \) will be derived.
To obtain the asymptotic expression for \( w_2 \), we change the order of integration in (66b) as
\[
w_2 = \frac{1}{2} \ln \int_0^\infty \eta_e(z) \left[ 1 - F_{\gamma_b}(z) \right] dz. \quad (68)
\]
We can easily get that \( F_{\gamma_b}(z) \approx 0 \) when \( \gamma_b \to \infty \). Then by substituting (28) into (68), and after some algebraic manipulations, \( w_2 \) will be derived with the help of [38, eq. 3.353.5].
The proof is completed.

REFERENCES

[1] K. Y. Jo, *Satellite communications network design and analysis*. Norwood, MA, USA: Artech House, 2011.
[2] K. Pabst et al., “Relay-based deployment concepts for wireless and mobile broadband radio,” *IEEE Commun. Mag.*, vol. 42, no. 9, pp. 80–89, Sep. 2004.
[3] M. K. Ari 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.
[4] B. Li, Z. Fei, Z. Chu, F. Zhou, K. K. Wong, and P. Xiao, “Robust chance-constrained secure transmission for cognitive satellite-terrestrial networks,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 4208–4219, May. 2018.
[5] J. Liu, Y. Shi, Z. M. Fadlullah, and N. Kato, “Space-air-ground integrated network: A survey,” *IEEE Commun. Surveys Tut.*, vol. 20, no. 4, pp. 2714–2741, May 2018.
[6] J. Liu, Y. Shi, L. Zhaom T. Cao, W. Sun, and N. Kato, “Joint placement of controllers and gateways in SDN-enabled 5G satellite-integrated network,” *IEEE J. Sel. Areas Commun.*, vol. 36, no. 2, pp. 221–232, Feb. 2018.
[7] Y. Shi, J. Liu, Z. M. Fadlullah, and N. Kato, “Cross-layer data delivery in satellite-aerial-terrestrial communication,” *IEEE Wireless Commun.*, vol. 25, no. 3, pp. 138–143, Jul. 2018.
[8] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. MaLaughlin, “Wireless information theoretic security,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[9] C. E. Shannon, “Communication theory of secrecy systems,” *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[10] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[11] D. K. Petrok, M. P. Anastasopoulos, and S. Papavassiliou, “Secrecy capacity for satellite networks under rain fading,” *IEEE Trans. Dependable Comput.*, vol. 8, no. 5, pp. 778–783, Sep. 2011.
[12] B. Li, Z. Fei, C. Zhou, and Y. Zhang, “Physical layer security in information networks: A survey,” *IEEE Internet Things J.*, vol. 7, no. 1, pp. 33–52, Sep. 2019.
[13] K. An, T. Liang, X. Yan, and G. Zhong, “On the secrecy performance of land mobile satellite systems,” *IEEE Access*, vol. 6, pp. 39606–39620, 2018.
[14] 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.
[15] K. Guo, B. Zhang, Y. Huang, and D. Guo, “Secure performance analysis of satellite communication networks in Shadowed Rician channel,” in *Proc. Int. Symp. Signal Process. Inf. Technol.*, Limassol, Cyprus, May. 2016.
[16] V. Bankey and P. K. Upadhyay, “Secrecy outage analysis of hybrid satellite-terrestrial relay networks with opportunistic relaying schemes,” in *Proc. IEEE 85th Veh. Technol. Conf.*, Jun. 2017, pp. 1–5.
Kefeng Guo (Member, IEEE) received the B.S. degree from the Beijing Institute of Technology, Beijing, China, in 2012, the M.S. degree from the PLA University of Science and Technology, Nanjing, China, in 2015, and the Ph.D. degree from the Army Engineering University of PLA, Chongqing, China, in 2018. He is currently a Lecturer with the School of Space Information, Space Engineering University, Beijing. He has authored or coauthored more than 40 research papers in international journals and conferences. His research interests include cooperative relay networks, MIMO communications systems, multiuser communication systems, satellite communication, hardware impairments, cognitive radio, NOMA technologies, and physical layer security.

Dr. Guo has been the TPC member of many IEEE-sponsored conferences, such as IEEE ICC, IEEE GLOBECOM, and IEEE WCNC.

Kang An (Member, IEEE) received the B.S. degree from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2011, the M.S. degrees from the PLA University of Science and Technology, Nanjing, and the Ph.D. degree from the Army Engineering University of PLA, Chongqing, China, in 2017. He is currently a Full Professor and the Head of College of Communications Engineering, Army Engineering University of PLA, Nanjing. He has authored and coauthored more than 80 conference and journal papers and has been granted over 20 patents in his research areas. He was a Reviewer for several journals in communication field. His current research interests include communication antijamming technologies, satellite communication, cognitive radio, and physical layer security.

Bangning Zhang received the B.S. and M.S. degrees from the Institute of Communications Engineering, Nanjing, China, in 1984 and 1987, respectively. He is currently a Full Professor and the Head of College of Communications Engineering, Army Engineering University of PLA, Nanjing. He has authored and coauthored more than 80 conference and journal papers and has been granted over 20 patents in his research areas. He was a Reviewer for several journals in communication field. His current research interests include communication antijamming technologies, microwave technologies, satellite communications systems, cooperative communications, and physical layer security.

Yuzhen Huang (Member, IEEE) received the B.S. degree in communications engineering and the Ph.D. degree in communications and information systems from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2008 and 2013, respectively. He has been with the Artificial Intelligence Research Center, National Innovation Institute of Defense Technology, where he is currently an Associate Professor. He is also a Postdoctoral Research Associate with the School of Information and Communication, Beijing University of Posts and Telecommunications, Beijing, China. He has authored or coauthored more than 90 research papers in international journals and conferences. His research interests include channel coding, MIMO communications systems, cooperative communications, physical layer security, and cognitive radio systems. He is an Associate Editor for the KSII Transactions on Internet and Information Systems. He and his coauthors were the recipient of the Best Paper Award at the WCSP 2013, and the IEEE Communications Letters Exemplary Reviewer Certificate, in 2014.

Xiaogang Tang (Member, IEEE) received the M.S. degree from Xi’an Jiaotong University, Xi’an, China in 2002, where he is currently working toward the Ph.D. degree. He is currently an Assistant Professor at Xi’an Jiaotong University and Space Engineering University, Beijing, China. His research interests include spread spectrum system, pattern recognition, signal processing, and satellite communication. He has authored or coauthored several research papers in scholarly journals in the above research areas and has participated in several conferences.

Gan Zheng (Senior Member, IEEE) received the B.Eng. and M.Eng. degrees in electronic and information engineering from Tianjin University, Tianjin, China, in 2002 and 2004, respectively and the Ph.D. degree in electrical and electronic engineering from The University of Hong Kong, Hong Kong, in 2008. He is currently a Reader of signal processing for wireless communications with the Wolfson School of Mechanical, Electrical and Manufacturing Engineering, Loughborough University, Loughborough, U.K. His research interests include machine learning for communications, UAV-communications, mobile edge caching, full-duplex radio, and wireless power transfer. He is currently an Associate Editor for the IEEE Communications Letters and IEEE Wireless Communications Letters. He is the first recipient of the 2013 IEEE Signal Processing Letters Best Paper Award, the 2015 GLOBECOM Best Paper Award, and the 2018 IEEE Technical Committee on Green Communications & Computing Best Paper Award. He was listed as a Highly Cited Researcher by Thomson Reuters/Clarivate Analytics in 2019.

Theodoros A. Tsiftsis (Senior Member, IEEE) was born in Lamia, Greece, in 1970. He received the B.Sc. degree in physics from the Aristotle University of Thessaloniki, Thessaloniki, Greece in 1993, the M.Sc. degree in digital systems engineering from the University of Economics and Business, Athens, Greece, in 2000, and the Ph.D. degree in electrical engineering from the University of Patras, Patras, Greece, in 2006. He is currently a Professor with the School of Intelligent Systems Science & Engineering, Jinan University, Zuhai, China, and also a Honorary Professor with Shandong Jiaotong University, Jinan, China. His research interests include the broad areas of cognitive radio, communication theory, wireless powered communication systems, optical wireless communication, and ultra-reliable low-latency communication.

Dr. Tsiftsis was a Senior or Associate Editor in the Editorial Boards of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE Communications Letters, IET Communications, and IEICE TRANSACTIONS ON COMMUNICATIONS. He is currently an Area Editor for Wireless Communications II of the IEEE TRANSACTIONS ON COMMUNICATIONS and an Associate Editor of the IEEE TRANSACTIONS ON MOBILE COMPUTING. He has been appointed to a two-year term as an IEEE Vehicular Technology Society Distinguished Lecturer, Class 2018.