IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 15, 2018, accepted November 29, 2018, date of publication December 10, 2018,
date of current version January 11, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2885979

Secure Communication in Non-Geostationary Orbit Satellite Systems: A Physical Layer Security Perspective

YEQIU XIAO[1], (Student Member, IEEE), JIA LIU[2], (Member, IEEE), YULONG SHEN[1], (Member, IEEE), XIAOHONG JIANG[3], (Senior Member, IEEE), AND NORIO SHIRATORI[4], (Life Fellow, IEEE)

[1]School of Computer Science and Technology, Xidian University, Xi'an 710071, China
[2]Center for Cybersecurity Research and Development, National Institute of Informatics, Tokyo 101-8430, Japan
[3]School of Systems Information Science, Future University Hakodate, Hakodate 041-8655, Japan
[4]Research and Development Initiative, Chuo University, Tokyo 112-8551, Japan

Corresponding authors: Jia Liu (jliu@nii.ca.jp) and Yulong Shen (ylshen@mail.xidian.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant U1536202, Grant 61571352, and Grant 61802292, in part by the Shaanxi Science and Technology Coordination and Innovation Project under Grant 2016KTZDGY05-07-01, in part by the Project of Cyber Security Establishment with Inter University Cooperation, in part by the Secom Science and Technology Foundation, in part by the National Key Research and Development Plan of China under Grant 2017YFB1400704, in part by the Fundamental Research Funds for the Central Universities, and in part by the Innovation Fund of Xidian University.

ABSTRACT Satellite communication systems serve as an indispensable component of wireless heterogeneous networks in 5G era for providing various critical civil and military applications. However, due to the broadcast nature and full accessibility of wireless medium, serious security threats exist from such systems. As an effort to address this issue, this paper, for the first time, investigates the secure communication in a non-geostationary orbit (NGSO) satellite system from a physical layer security perspective. Specifically, we focus on the downlink of an NGSO satellite which provides services to a fixed earth station and is wiretapped by a fixed eavesdropper. We first apply three types of orbiting models to characterize the movement state of the satellite. Based on the orbiting models, we then provide theoretical analysis for the secure communication performance of such a system. The expressions of two fundamental performance metrics, secrecy capacity and secrecy outage probability, are derived in a closed form for any system time. Finally, we conduct extensive simulations to validate our theoretical performance analysis and illustrate the security performance in a practical NGSO satellite communication system.

INDEX TERMS Non-geostationary orbit satellite system, physical layer security, performanceevaluation.

I. INTRODUCTION

Satellite communication (SATCOM) systems have some advantages over terrestrial communication systems, such as cost effectiveness, global availability, superior reliability and scalability, etc. [1], [2]. Thus, they serve as an indispensable component of wireless heterogeneous networks in 5G era for providing various critical civil and military applications [3], [4]. However, due to the broadcast nature and full accessibility of wireless medium, the communications through SATCOM systems are particularly vulnerable to eavesdropping attacks by unauthorized receivers. Traditionally, security of satellite communication is guaranteed by cryptographic-based techniques (e.g., encryption and decryption) on the upper layers, which rely on the computational complexity [5]. Cryptography gives a rise to high power cost resulting in shortening the satellites' lifetime. Moreover, with the rapid development of quantum computing, cryptography will encounter unprecedented challenges [6]. Therefore, cryptographic technologies are not sufficient to ensure perfect secure communication in satellite systems.

As a complementary technique of cryptographic-based methods, physical layer security (PLS) is an information-theoretic approach which exploits the fundamental characteristics of wireless medium to achieve perfect secrecy. Since PLS is promising to guarantee the everlasting security without the dependence of encryption/decryption, it has been attracting considerable attention from both academic and industrial communities recently. Based on the fundamental

results of Shannon in [7], Wyner [8] first developed the ground-breaking theories of PLS, indicating that the perfect secrecy can be achieved if the capacity of legitimate channel is superior to that of wiretap channel. Following this line, researchers have been devoted to the study of PLS under various channel models, including Gaussian wiretap channel [9], broadcast channel [10], multi-access channel [11], two-way wiretap channel [12], MIMO wiretap channel [13], and so on. Meanwhile, diverse applications of PLS in wireless communication systems have been proposed in the literature. For example, the works of [14]–[16] studied PLS for 5G wireless networks; the works of [17]–[23] discussed the cooperative jamming and relay selection strategies in two hop cooperative networks with the consideration of PHY-SCE; the works of [24]–[27] explored the PLS based routing in multi-hop wireless networks. For a detailed survey on PLS in wireless communication systems, please kindly refer to [28]–[32] and the references therein.

Despite extensive efforts have been devoted to the research of PLS in terrestrial communication systems like cellular networks and ad hoc networks, that in SATCOM systems is still largely uninvestigated. Petraki *et al.* [33] for the first time studied PLS in a geostationary satellite communication system and introduced rain fading into the analysis. Lei *et al.* [34] considered the beamforming techniques and power control under the scenario where a multi-beam satellite sends messages to multiple terrestrial users surrounded by a single eavesdropper. Later, Zheng *et al.* utilized an empirical model of rain attenuation provided by the International Telecommunication Union Recommendation (ITU-R) [35], and extended the results to a general scenario where each legitimate user is surrounded by multiple eavesdroppers [36]. To improve secrecy rate, Kalantari *et al.* [37] applied network coding technology in bidirectional multibeam satellite communications. In addition, based on the shadowed Rician model [38], some works analyzed the performance of PLS in land mobile SATCOM systems, which can be found in [39] and [40].

It is worth noting that all aforementioned works focused on the geostationary satellites, however, in reality there are also a great number of satellites moving around the earth, e.g., non-geostationary orbit (NGSO) satellites, and their PLS performance has not been understood yet. To this end, this paper, for the first time, investigates the secure communication in NGSO satellite networks from a physical layer security perspective. For the NGSO SATCOM systems, we take the satellite movements into consideration, which makes the performance evaluation a new problem different from that in the geostationary case. By introducing the mobile models of satellites, theoretical analysis is conducted which can be used to predict the performance of secure communication at any time. Moreover, the signals of SATCOM systems are usually very sensitive to the atmospheric environments due to the employment of high frequency bands (i.e., Ku, Ka, and V bands) [41]–[43], we also develop our theoretical framework with the consideration of atmospheric factors, to make the performance prediction of the communication in NGSO systems more accurate and practical.

The main contributions of this paper are identified as follows:

- We, for the first time, consider the secure communication of an NGSO SATCOM system from a physical layer security perspective. In order to make the performance analysis tractable under the scenario of non-geostationary orbit, we apply three types of orbiting models to characterize the movement state of an NGSO satellite.
- Based on the satellite orbiting models and with the full consideration of rain attenuation, we develop an analytical framework for the performance evaluation and prediction of NGSO SATCOM systems. Specifically, the expressions of two fundamental performance metrics, i.e., secrecy capacity and secrecy outage probability, are derived in closed-form.
- We conduct extensive simulations and draw a variety of figures to show that how the satellite elements and rain attenuation affect the communication security performance, which can serve as important guidelines for the configuration and operation of practical NGSO SATCOM systems.

The remainder of this paper is organized as follows. Section II introduces the system models and Section III characterizes the satellite orbiting. In Section IV, we conduct the performance analysis. Section V presents the simulation results and finally Section VI concludes this paper.

In the rest of this paper, we will use the following notations. Vectors are written as $(\vec{\cdot})$. The transposition of a matrix is written as $[\cdot]^T$ and $|\cdot|$ denotes the absolute value of a variable. Subscripts $(\cdot)_{Ear}$, $(\cdot)_{So}$, $(\cdot)_l$ and $(\cdot)_e$ represent that some coefficient is related to the earth, the satellite orbit, the legitimate earth station and the eavesdropper, respectively. $[\cdot]_{dB}$ indicates a value in decibels. $x \sim \mathcal{N}(m, \ominus)$ denotes a random variable x following the Gaussian distribution with the mean m and the variance $\ominus$. Φ is the cumulative distribution function of a random variable following the standard normal distribution and $\mathbb{P}$ is the probability operator.

II. SYSTEM MODELS

In this section, we introduce the system models involved in this study.

A. NETWORK MODEL

As illustrated in Fig. 1, in this paper we consider a satellite communication system operating over a non-geostationary orbit (NGSO), which consists of an NGSO satellite and a fixed earth station. We focus on the downlink of this system, i.e., the satellite serves as the transmitter and provides services to the earth station (legitimate receiver). The satellite has a coverage area on the earth surface which can be approximately modeled as a circle with the subsatellite point (a point on the earth vertically under the satellite) as center point and R_{Sat} as radius. The length of communication link between the

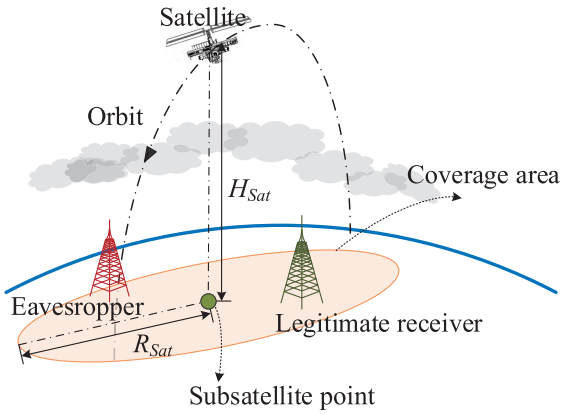


FIGURE 1. Model of NGSO satellite communication system.

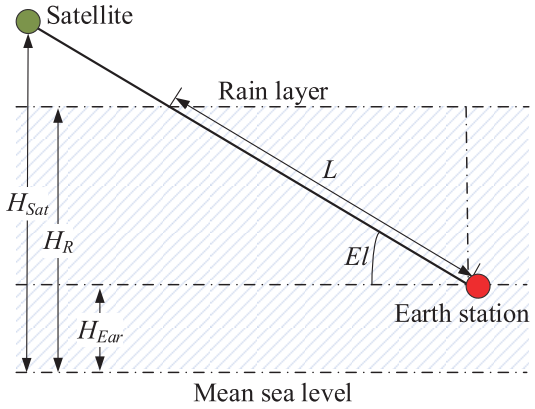


FIGURE 2. Illustration of rain attenuation.

satellite and earth station varies with the satellite orbiting and the earth rotating, therefore, the earth station cannot receive any information once it is out of the satellite coverage area. We consider that this downlink is overheard by another fixed earth station (eavesdropper). Moreover, we assume that the transmitter, receiver and eavesdropper are all equipped with a single antenna.

B. CHANNEL MODEL

In terms of channel effects, there are significant differences between satellite communication (SATCOM) links and terrestrial communication links. In order to satisfy the requirement of large channel capacity, SATCOM systems tend to operate over higher frequency bands like Ku band and Ka band, whose channel quality is sensitive to the tropospheric environments. Especially, rain is the dominant factor severely degrading the availability and performance of space-earth links. Therefore, in this paper we take both the signal attenuation caused by the free-space propagation and atmospheric environments into consideration.

1) FREE-SPACE LOSS

Free-space loss indicates the power loss resulting from the electromagnetic wave spreading in free space without reflection or diffraction. All wireless communication links suffer from the free-space loss and it can be expressed as

$$FSL = \left(\frac{4\pi\rho f}{c}\right)^2, \tag{1}$$

where ρ represents the length of the communication link, f denotes the frequency band over which the satellite system operates and c denotes the velocity of light, $c \approx 3\times10^5\ km/s$. It can be seen from formula (1) that the free-space loss in this study is time-variant and will change following the satellite orbiting.

2) RAIN ATTENUATION

Unlike terrestrial communication links which are negligibly influenced by rain attenuation, space-earth links are highly sensitive to rain attenuation. The level of rain attenuation depends on the rain rate of the region where the earth station located in. As illustrated in Fig. 2, in order to characterize the effects of rain attenuation on space-earth links $[RA]_{dB}$, we abstract the basic factors from the state-of-art empirical model proposed in ITU-R P.618-12 [35], which can be expressed as

$$[RA]_{dB} = \gamma \times L \times \beta, \tag{2}$$

where γ (dB/km) denotes the specific attenuation of rain, L denotes the slant-path length below rain height, and β denotes the proportion of the slant-path suffering from rain attenuation, which can be estimated following the steps proposed in ITU-R P.618-12 [35]. L can be computed as

$$L = \frac{H_R - H}{\sin(El)}, \tag{3}$$

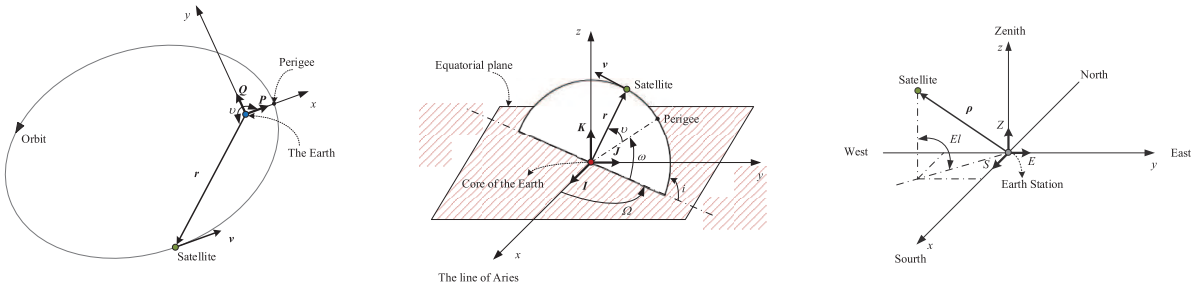
where H_{Ear} denotes the height of the earth station above mean sea level, H_R is the height of rain, and El denotes the elevation angle of the antenna at the earth station.

It is worth noting that under the scenario of non-geostationary orbit, some system parameters are time-variant, such as ρ and El. In order to characterize the system performance dynamically, we need to introduce the trajectories of satellite flying into the analysis, as shown in the next section.

For convenience, we give a list of main notations involved in this paper, as summarized in Table 1.

III. SATELLITE ORBITING MODELS

In reality, there are a great number of NGSO satellites. In order to capture the movement state of an NGSO satellite, in this section we introduce three reference frames, namely the perifocal coordinate system (PQW frame), the geocentric-equatorial coordinate system (IJK frame), and the topocentric-horizon coordinate system (SEZ frame). In addition, we also need to utilize the satellite elements, i.e., the basic information of a satellite, which are provided by the two-line elements (TLE) [1] from the U.S. National Aeronautics and Space Administration (NASA).



(a) (b) (c)

FIGURE 3. Satellite orbit and its different reference frames. (a) Perifocal coordinate system. (b) Geocentric-equatorial coordinate system. (c) Topocentric-horizon coordinate system.

TABLE 1. Main notations.

Notations	Meaning
a	Semimajor axis of an ellipse
e	Eccentricity of an ellipse
El	Antenna elevation angle
f	Frequency band that the satellite operates over
FSL	Free-space loss
G	Power gain of the antenna
H_{Ear}	Height of the earth station above mean sea level
H_{Sat}	Height of the satellite above mean sea level
R_{Sat}	Coverage radius of the satellite
i	Inclination of the satellite orbit
L	Slant-path length below rain height
LST	Local sidereal time for the earth station
n	Noise
P	Signal power
$\vec{\mathbf{r}}$	Position vector of satellite
r	Magnitude of the vector $\vec{\mathbf{r}}$
$\vec{\mathbf{R}}$	Position vector of the earth station
RA	Rain attenuation
H_R	Height of rain
β	Proportion of path suffering from rain attenuation
γ	Specific attenuation based on rain rate of the zone where the earth station is
t	Time
θ	Geocentric latitude
λ	Geographic latitude of the earth station
$\vec{\boldsymbol{\rho}}$	Range vector from the earth station to the satellite
ρ	Distance of communication from the earth station to the satellite
υ	True anomaly, the angle from perigee to the satellite position measured at the earth's center
ω	Argument of perigee of the satellite
Ω	Right ascension of the ascending node of the satellite

A. PQW FRAME

PQW frame presents the orbital plane of an artificial satellite. As shown in Fig. 3(a), PQW frame sets the center of the earth as the origin, the positive x axis passes through the perigee in the orbital plane. The positive y axis lying in the orbital plane is rotated 90° from the x axis and points to the moving direction of the satellite. $\vec{\mathbf{P}}$ and $\vec{\mathbf{Q}}$ are unit vectors of the positive x axis and the positive y axis, respectively. The positive z axis can be judged by the right-hand rule. Therefore, the position vector $\vec{\mathbf{r}}(t)$ of the satellite in PQW frame can be expressed as

$$\vec{\mathbf{r}}(t) = (r(t)\cos\upsilon(t))\,\vec{\mathbf{P}} + (r(t)\sin\upsilon(t))\,\vec{\mathbf{Q}}, \tag{5}$$

where $r(t)$ denotes the magnitude of $\vec{\mathbf{r}}(t)$, $\upsilon(t)$ denotes the true anomaly, and t denotes the system time. Furthermore, $\upsilon(t)$ can be determined by performing the procedures proposed in [1] and $r(t)$ can be calculated as

$$r(t) = \frac{a_{So}\left(1 - e_{So}^2\right)}{1 + e_{So}\cdot\cos\upsilon(t)}, \tag{6}$$

where the coefficients a_{So} and e_{So} represent the semimajor axis and the eccentricity of the satellite orbit, respectively.

B. IJK FRAME

IJK frame describes how the local geographic coordinate of an earth station changes following the earth rotation, thus it has an influence on the relative position of a satellite to the earth station. As illustrated in Fig. 3(b), the earth's core and equatorial plane act as the system's origin and the fundamental plane, respectively. $\vec{\mathbf{I}}$, $\vec{\mathbf{J}}$ and $\vec{\mathbf{K}}$ denote the unit vectors in the IJK frame, and the positive direction of $\vec{\mathbf{I}}$ points to the line of Aries. Then, we can transform the position vector of a satellite from the PQW frame to the IJK frame through a transformation matrix $\tilde{R}$ as

$$\begin{bmatrix} r_I(t) \\ r_J(t) \\ r_K(t) \end{bmatrix} = \tilde{R}\begin{bmatrix} r_P(t) \\ r_Q(t) \end{bmatrix}, \tag{6}$$

where $r_I(t)$, $r_J(t)$, and $r_K(t)$ are the components of $\vec{\mathbf{r}}(t)$ in the IJK frame and $\tilde{R}$ is expressed by (7), as shown at the bottom of this page.

$$\tilde{R} = \begin{bmatrix} \cos\Omega\cos\omega - \sin\Omega\sin\omega\cos i & -\cos\Omega\sin\omega - \sin\Omega\cos\omega\cos i \\ \sin\Omega\cos\omega + \cos\Omega\sin\omega\cos i & -\sin\Omega\sin\omega + \cos\Omega\cos\omega\cos i \\ \sin\omega\sin i & \cos\omega\sin i \end{bmatrix} \tag{7}$$

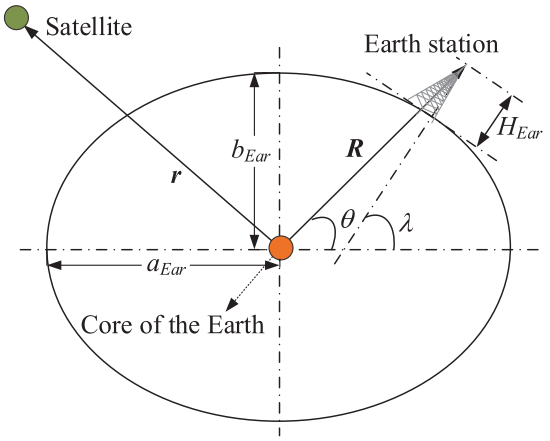


FIGURE 4. Earth station in the IJK frame.

Except for the position of a satellite, the coordinate of an earth station can be also presented in the IJK frame as Fig. 4 shows. With geographic information, an earth station's coordinate $[R_I(t), R_J(t), R_K(t)]^T$ can be written as

$$\begin{bmatrix} R_I(t) \\ R_J(t) \\ R_K(t) \end{bmatrix} = \begin{bmatrix} (K_N + H_{Ear})\cos\lambda\cos(LST(t)) \\ (K_N + H_{Ear})\cos\lambda\sin(LST(t)) \\ (K_N\left(1 - {e_{Ear}}^2\right) + H_{Ear})\sin\lambda \end{bmatrix}, \quad (8)$$

where H_{Ear} denotes the height of the earth station above mean sea level, λ denotes the geographic latitude of the earth station, LST represents the local sidereal time which is Greenwich sidereal time added by the earth station's east longitude in degree, K_N is given by $K_N = a_{Ear}/\sqrt{1 - e_{Ear}^2 \sin^2\lambda}$, a_{Ear} and e_{Ear} are the semimajor axis and the eccentricity of the earth, respectively. Then, the range vector $\vec{\boldsymbol{\rho}}(t)$ from the earth station to the satellite can be further derived as

$$\vec{\boldsymbol{\rho}}(t) = \vec{\mathbf{r}}(t) - \vec{\mathbf{R}}(t). \quad (9)$$

C. SEZ FRAME

In the SEZ frame, the position of a satellite is observed from the earth station, where the position and horizon plane of the earth station are treated as the origin and fundamental plane, respectively. As shown in Fig. 3(c), positive directions of x axis and y axis are respectively taken as the south with unit vector $\vec{\mathbf{S}}$ and the east with unit vector $\vec{\mathbf{E}}$, the unit vector $\vec{\mathbf{Z}}$ points to the zenith of the observer. The range vector $\vec{\boldsymbol{\rho}}(t)$ in the SEZ frame can be transformed from that in the IJK frame following a standard procedure as formula (10), as shown at the bottom of this page, where the geocentric latitude θ is an imaginary angle differing from the geographic latitude λ, as shown in Fig. 4. The relationship between θ and λ is given by

$$\tan\theta = \frac{K_N(1 - e_{Ear}^2) + H_{Ear}}{K_N + H_{Ear}}\tan\lambda. \quad (11)$$

The distance $\rho(t)$ between the earth station and the satellite can be derived as

$$\begin{aligned} \rho(t) &= \left(\rho_S^2(t) + \rho_E^2(t) + \rho_Z^2(t)\right)^{\frac{1}{2}} \\ &= \left(\rho_I^2(t) + \rho_J^2(t) + \rho_K^2(t)\right)^{\frac{1}{2}}. \end{aligned} \quad (12)$$

The elevation angle of the antenna in the earth station $El(t)$ can be written as

$$El(t) = \arcsin\left(\frac{\rho_Z(t)}{\rho(t)}\right). \quad (13)$$

Remark 1: It should be pointed out that single or two orbiting models cannot make the PLS performance analysis tractable. Therefore, we need to combine the three models and exploit the transforms among them to derive the exact performance expressions, as elaborated in the next section.

IV. SECURE COMMUNICATION PERFORMANCE ANALYSIS

With the help of rain attenuation-aware channel model and satellite orbiting models, in this section we analyze the secure communication performance of the NGSO SATCOM system from a PLS perspective, which is mainly characterized by the secrecy capacity and secrecy outage probability.

A. SECRECY CAPACITY

Secrecy capacity (SC) is defined as the maximum information rate at which the transmitter (satellite) can transmit data to the receiver (legitimate earth station) securely, i.e., the eavesdropper is unable to decode any information. According to Wyner's theory [8], SC is determined by the difference between the capacity of legitimate channel and that of wiretap channel. More formally, let $C_s(t)$, $C_l(t)$ and $C_e(t)$ denote the SC, the capacity of legitimate channel and wiretap channel at system time t, respectively, then $C_s(t)$ is given by

$$C_s(t) = [C_l(t) - C_e(t)]^+, \quad (14)$$

where $[x]^+ = \max\{0, x\}$.

For the NGSO SATCOM system considered in this paper, the relative position between the satellite and the earth station varies with the satellite orbiting and the earth rotating, such that the earth station or the eavesdropper cannot receive any information once it is out of the satellite coverage

$$\begin{bmatrix} \rho_S(t) \\ \rho_E(t) \\ \rho_Z(t) \end{bmatrix} = \begin{bmatrix} \sin\theta\cos(LST(t)) & \sin\theta\sin(LST(t)) & -\cos\theta \\ -\sin(LST(t)) & \cos(LST(t)) & 0 \\ \cos\theta\cos(LST(t)) & \cos\theta\sin(LST(t)) & \sin\theta \end{bmatrix} \begin{bmatrix} \rho_I(t) \\ \rho_J(t) \\ \rho_K(t) \end{bmatrix} \quad (10)$$

area. Let $H_{Sat}(t)$ denote the vertical height of the satellite above mean sea level at the system time t, then the maximum communication distance ρ_{max} can be approximated as $\rho_{max}(t) \approx \sqrt{H_{Sat}^2(t) + R_{Sat}^2}$. Regarding the value of $H_{Sat}(t)$, it can be calculated by solving (8), where it only needs to substitute the parameters (such as the coordinate) corresponding to the satellite.

We use $\rho_l(t)$ and $\rho_e(t)$ to represent the length of legitimate channel and eavesdropping channel, respectively. For $\rho_l(t) > \rho_{max}(t)$, the satellite does not transmit any information to the earth station; for $\rho_l(t) \le \rho_{max}(t)$ and $\rho_e(t) > \rho_{max}(t)$, the eavesdropper is out of the satellite coverage area, thus the secrecy capacity is equal to the capacity of legitimate channel. Let $P_l(t)$ and n_l (resp. $P_e(t)$ and n_e) denote the received signal power and noise power at the legitimate earth station (resp. eavesdropper). Since the rain fading channel between the satellite and the earth station can be regarded as an AWGN (additional white Gaussian noise) channel[1] [33], then the SC at any system time t can be formulated as (15), as shown at the bottom of this page.

It can be seen from formula (15) that for deriving $C_s(t)$, we need to determine the received signal power P_l and P_e. We use P_T to represent the power of transmitted signal and G_T to represent the antenna gain. According to the rain attenuation-aware channel model and satellite movement models developed in previous sections, P_l and P_e can be calculated as

$$\begin{aligned} P_l(t) &= \frac{P_T G_T}{FSL_l(t) \cdot 10^{\frac{1}{10}[RA_l(t)]_{dB}}} \\ &= \frac{c^2 P_T G_T}{(4\pi f)^2 \cdot 10^{\frac{1}{10}[RA_l(t)]_{dB}} \cdot \rho_l^2(t)}, \end{aligned} \tag{16}$$

and

$$\begin{aligned} P_e(t) &= \frac{P_T G_T}{FSL_e(t) \cdot 10^{\frac{1}{10}[RA_e(t)]_{dB}}} \\ &= \frac{c^2 P_T G_T}{(4\pi f)^2 \cdot 10^{\frac{1}{10}[RA_e(t)]_{dB}} \cdot \rho_e^2(t)}, \end{aligned} \tag{17}$$

where FSL is determined by formula (1), $[RA]_{dB}$ is determined by formula (2), ρ is determined by formula (12), the subscripts $(\cdot)_l$ and $(\cdot)_e$ indicate the parameters corresponding to the legitimate earth station and the eavesdropper, respectively.

[1]In future works we will consider other channel models, such as Rician channel and Shadow-Rician channel.

For simplicity of expressions in this paper, we define some symbols as follows:

$$\begin{cases} K_0(t) = \dfrac{c^2\, P_T(t) G_T}{(4\pi f)^2} & \text{(18a)} \\ K_1(t) = n_l \rho_l^2(t) \cdot 10^{\frac{[RA_l(t)]_{dB}}{10}} & \text{(18b)} \\ K_2(t) = n_e \rho_e^2(t) \cdot 10^{\frac{[RA_e(t)]_{dB}}{10}} & \text{(18c)} \\ K_3(t) = \left[n_l \rho_l^2(t)\right]_{dB} - \left[n_e \rho_e^2(t)\right]_{dB}. & \text{(18d)} \end{cases}$$

By substituting (16)-(18) into formula (15), the SC of the NGSO SATCOM system at any time can be finally determined. For the case of $\rho_l(t) \le \rho_{max}(t)$ and $\rho_e(t) \le \rho_{max}(t)$, formula (15a) can be re-written as

$$C_s(t) = \left[\log_2\left(1 + \frac{K_0(t)K_2(t) - K_0(t)K_1(t)}{K_0(t)K_1(t) + K_1(t)K_2(t)}\right)\right]^+. \tag{19}$$

For the case of $\rho_l(t) \le \rho_{max}(t)$ and $\rho_e(t) > \rho_{max}(t)$, formula (15b) can be re-written as

$$C_s(t) = \log_2\left(1 + \frac{K_0(t)}{K_1(t)}\right). \tag{20}$$

To simplify the SC expression (19) for the case of $\rho_l(t) \le \rho_{max}(t)$ and $\rho_e(t) \le \rho_{max}(t)$, we make approximations in the high SNR (signal-to-noise ratio) region. From Fig. 2, L can be expressed as $L = \frac{H_R - H_{Ear}}{H_{Sat} - H_{Ear}}\rho \overset{def}{=} \alpha\rho$, and we denote that $k_\rho = \rho_l/\rho_e$ and $k_\gamma = \gamma_l/\gamma_e$, then $C_s(t)$ in the high SNR region can be approximated by

$$\begin{aligned} C_s(t) &= \log_2\left(1 + \frac{K_0(t)}{K_1(t)}\right) - \log_2\left(1 + \frac{K_0(t)}{K_2(t)}\right) \\ &\approx \log_2\left(\frac{K_0(t)}{K_1(t)}\right) - \log_2\left(\frac{K_0(t)}{K_2(t)}\right) \\ &= \log_2\left(\frac{10^{log_{10}n_e}\, 10^{\frac{1}{10}\gamma_e\alpha_e\rho_e}}{10^{log_{10}\left(k_\rho^2 n_l\right)}\, 10^{\frac{1}{10}k_\rho\gamma_l\alpha_l\rho_e}}\right) \\ &= \log_2 10 \cdot \left(log_{10}n_e - 2log_{10}k_\rho - log_{10}n_l\right) \\ &\quad + \frac{1}{10}\log_2 10 \cdot \left(\alpha_e\rho_e - k_\rho k_\gamma \alpha_l \rho_e\right)\gamma_e. \end{aligned} \tag{21}$$

Taking the derivative of C_s with respect to γ_e in (21), we then have

$$\frac{dC_s}{d\gamma_e} = \frac{1}{10}\log_2 10\left(\alpha_e - k_\rho k_\gamma \alpha_l\right)\rho_e. \tag{22}$$

We can see that as γ_e increases, C_s will monotonically increase if $\alpha_e > k_\rho k_\gamma \alpha_l$, while it will monotonically decrease if $\alpha_e < k_\rho k_\gamma \alpha_l$.

$$C_s(t) = \begin{cases} \left[\log_2\left(1 + \dfrac{P_l(t)}{n_l}\right) - \log_2\left(1 + \dfrac{P_e(t)}{n_e}\right)\right]^+, & \rho_l(t) \le \rho_{max}(t) \wedge \rho_e(t) \le \rho_{max}(t), \quad \text{(15a)} \\ \log_2\left(1 + \dfrac{P_l(t)}{n_l}\right), & \rho_l(t) \le \rho_{max}(t) \wedge \rho_e(t) > \rho_{max}(t), \quad \text{(15b)} \\ N/A, & \rho_l(t) > \rho_{max}(t). \quad \text{(15c)} \end{cases}$$

B. SECRECY OUTAGE PROBABILITY

In this study we assume that the satellite sets the transmission rate to be arbitrarily close to the secrecy capacity, thus the event of secrecy outage refers to the case that the capacity of legitimate channel is inferior to that of wiretap channel, such that the information can be decoded by the eavesdropper. The ***secrecy outage probability (SOP)*** is defined as the probability that the event of secrecy outage happens.

We use $P_{so}(t)$ to denote the SOP at the system time t. According to the above definition, $P_{so}(t)$ can be formulated as (23), as shown at the bottom of this page. It can be seen that we only need to determine the expression of (23a). From expression (19) we can see that secrecy outage will happen when $K_2(t) \leq K_1(t)$, thus the SOP is given by

$$\begin{aligned} P_{so}(t) &= \mathbb{P}(C_s(t) = 0) = \mathbb{P}\left(K_2(t) \leq K_1(t)\right) \\ &= \mathbb{P}\left(\beta_e L_e(t)\gamma_e - \beta_l L_l(t)\gamma_l \leq K_3(t)\right). \end{aligned} \tag{24}$$

Since the surroundings of radio waves propagating can make a huge difference to the randomness of wireless channels, considering the likelihood of abnormal weather in a region, the specific attenuation which the legitimate earth station and the eavesdropper experience follows the independent and identically distributed (i.i.d) Gaussian distribution, which can be modeled as $\gamma_l \sim \mathcal{N}(\bar{\gamma}_l, \sigma_l^2)$ and $\gamma_e \sim \mathcal{N}(\bar{\gamma}_e, \sigma_e^2)$. The mean value $\bar{\gamma}_{(\cdot)}$ can be calculated by the statistic data sets from Recommendation ITU-R [44], whereas the variance $\sigma_{(\cdot)}^2$ reflects the degree of weather abnormality which can be set according to the real weather status. Therefore, expression (24) can be re-written as

$$\begin{aligned} P_{so}(t) = \int_0^{\infty} \left(\int_{-\infty}^{x+K_3(t)} \frac{e^{-\frac{(y-\beta_e L_e(t)\bar{\gamma}_e)^2}{2\beta_e^2 L_e^2(t)\sigma_e^2}}}{\sqrt{2\pi}\beta_e L_e(t)\sigma_e} dy \right) \\ \cdot \frac{1}{\sqrt{2\pi}\beta_l L_l(t)\sigma_l} e^{-\frac{(x-\beta_l L_l(t)\bar{\gamma}_l)^2}{2\beta_l^2 L_l^2(t)\sigma_l^2}} dx. \end{aligned} \tag{25}$$

We further define that

$$h(z) \triangleq \int f_{\gamma_l}(\tau) \cdot g_{\gamma_e}(\tau - z) d\tau, \tag{26}$$

where $f_{\gamma_l}(\cdot)$ and $g_{\gamma_e}(\cdot)$ represent the probability density functions of γ_l and γ_e, respectively. Equation (25) then can be finally expressed as

$$\begin{aligned} P_{so}(t) &= \frac{1}{2\pi\left(\beta_l L_l(t)\sigma_l\right) \cdot \left(\beta_e L_e(t)\sigma_e\right)} \int_{-K_3(t)}^{\infty} h(z) dz \\ &= \frac{\int_{-K_3(t)}^{\infty} \int e^{-\frac{(x-z-\beta_e L_e(t)\bar{\gamma}_e)^2}{2\beta_e^2 L_e^2(t)\sigma_e^2}} \cdot e^{-\frac{(x-\beta_l L_l(t)\bar{\gamma}_l)^2}{2\beta_l^2 L_l^2(t)\sigma_l^2}} dx dz}{2\pi\left(\beta_l L_l(t)\sigma_l\right) \cdot \left(\beta_e L_e(t)\sigma_e\right)} \\ &= \int_{-K_3(t)}^{\infty} \frac{e^{-\frac{(z-\beta_l L_l(t)\bar{\gamma}_l + \beta_e L_e(t)\bar{\gamma}_e)^2}{2(\beta_l^2 L_l^2(t)\sigma_l^2 + \beta_e^2 L_e^2(t)\sigma_e^2)}}}{\sqrt{2\pi(\beta_l^2 L_l^2(t)\sigma_l^2 + \beta_e^2 L_e^2(t)\sigma_e^2)}} dz \\ &= 1 - \Phi\left(\frac{\beta_e L_e(t)\bar{\gamma}_e - \beta_l L_l(t)\bar{\gamma}_l - K_3(t)}{\sqrt{\beta_l^2 L_l^2(t)\sigma_l^2 + \beta_e^2 L_e^2(t)\sigma_e^2}} \right), \end{aligned} \tag{27}$$

where $\Phi(\cdot)$ denotes the cumulative distribution function of the standard normal distribution.

We denote that $k_{\bar{\gamma}} = \bar{\gamma}_l / \bar{\gamma}_e$ and $y = \beta_e L_e \bar{\gamma}_e - \beta_l L_l \bar{\gamma}_l - K_3 = \left(\alpha_e - k_\rho k_{\bar{\gamma}} \alpha_l\right) \rho_e \bar{\gamma}_e - K_3$. Then, from equation (27) we can see that for $\alpha_e > k_\rho k_{\bar{\gamma}} \alpha_l$ (resp. $\alpha_e < k_\rho k_{\bar{\gamma}} \alpha_l$), as $\bar{\gamma}_e$ increases, y increases (resp. decreases) and $P_{so}(t)$ will monotonically decrease (resp. increase).

Remark 2: It is worth noting that the important rain attenuation and satellite orbiting issues have been carefully incorporated into the security performance evaluation, i.e., the derivations of SC and SOP. More significantly, our theoretical analysis can be used to not only estimate the current transmission performance, but also predict the performance of secure communication at any time, providing guidelines for the design, operation and optimization of practical NGSO SATCOM systems.

V. SIMULATION RESULTS AND DISCUSSIONS

In this section, we first conduct Monte Carlo simulations [45] to validate our theoretical performance analysis, and then provide extensive numerical results to illustrate the secure communication performance in an NGSO SATCOM system.

A. SIMULATION SETTINGS

To validate our theoretical performance analysis for the concerned NGSO SATCOM systems, a dedicated MATLAB simulator was developed to simulate the real-time communication process of an NGSO satellite with fixed earth stations, which is available at [46]. Satellite CFESAT is chosen as the transmitter in following simulations, and its satellite elements are summarized in Table 2. We set that CFESAT transmits signals over 16 GHz and its coverage radius is 4000 km.

In addition, without loss of generality, we set the altitude of legitimate fixed earth station and eavesdropper as $H_l = 0$ km and $H_e = 0$ km, respectively, and the proportion of path suffering from rain attenuation as $\beta = 0.5$. Unless otherwise specified, we randomly choose a legitimate receiver located in $(24.554°N, 46.822°E)$ and an eavesdropper located in $(8.751°N, 38.951°E)$. We simulate the communication process with rain data of January for the NGSO SATCOM system and set $\sigma_l = \sigma_e = 1$ to describe the abnormality of climate. The detailed settings of network parameters in our simulations are summarized in Table 3. Readers can

$$P_{so}(t) = \begin{cases} \mathbb{P}(C_s(t) = 0), & \rho_l(t) \leq \rho_{max}(t) \wedge \rho_e(t) \leq \rho_{max}(t), \quad (23a) \\ 0, & \rho_l(t) \leq \rho_{max}(t) \wedge \rho_e(t) > \rho_{max}(t), \quad (23b) \\ N/A, & \rho_l(t) > \rho_{max}(t). \quad (23c) \end{cases}$$

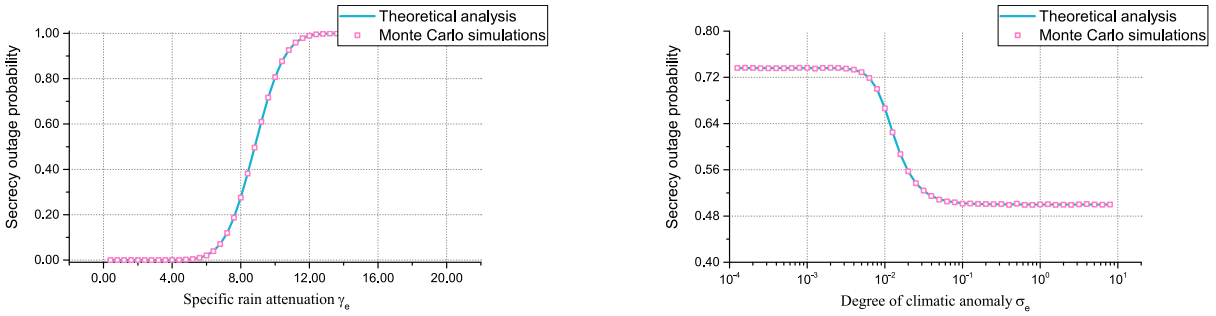


FIGURE 5. Validation of theoretical analysis. (a) Secrecy outage probability vs. specific rain attenuation of eavesdropper γ_e. (b) Secrecy outage probability vs. degree of climate abnormality of eavesdropper σ_e.

TABLE 2. Satellite elements of CFESAT from NASA.

Elements	Value
Satellite number	30777
Epoch year	2017
Epoch day	232.834166
Inclination	$i = 35.427800$
Right ascension of the ascending node	$\Omega = 40.106500$
Eccentricity	$e = 0.00623$
Argument of perigee	$\omega = 225.040700$
Mean anomaly	134.981300
Mean motion	14.23304826 rev/day
Revolution number at epoch	57791 rev

TABLE 3. Parameter settings.

Parameters	Value
Satellite	CFESAT
Start time of simulation	12:00 PM, Jan.1, 2018
Simulation period	2 days
Sampling frequency	1 per minute
Data sets of rain rate	January
Transmitting power	$P_T = 200$ watts
Gain of transmitting antenna	$G_T = 48.2$ dB
Frequency	$f = 16$ GHz
Radius of coverage area	$R_{Sat} = 4000$ km
Location of legitimate receiver	$(24.554°N, 46.822°E)$
Location of eavesdropper	$(8.751°N, 38.951°E)$
Noise power	$n_l = 1$ watt, $n_e = 1$ watt
Proportion of path suffering from rain attenuation	$\beta_l = 0.5$, $\beta_e = 0.5$
Degree of climatic anomaly	$\sigma_l = 1$, $\sigma_e = 1$

also flexibly perform our MATLAB simulator with any other desired parameter settings, such as the information of satellite, locations of earth stations, transmitting power, and so on.

B. VALIDATION

We conduct Monte Carlo simulations for the secrecy outage probability of the concerned NGSO SATCOM system at 19:01 PM on Jan. 2, 2018 (UTC), and the corresponding simulation and theoretical results are summarized in Fig. 5. Fig. 5(a) illustrates the behavior of SOP with the variation of specific rain attenuation γ_e. We can see that the simulation results match nicely with the theoretical curve, which indicates that our theoretical analysis is highly efficient to evaluate the secure communication performance of a NGSO SATCOM system. It can be also observed from Fig. 5(a) that the SOP decreases with the growth of γ_e (this is due to the reason that $\alpha_e - k_\rho k_{\bar{\gamma}} \alpha_l > 0$ holds at this simulation time), and the speed of such decrease is rapid with γ_e ranging from 5 dB/km to 12 dB/km.

Fig. 5(b) shows the simulated and theoretical SOP versus the climate abnormality σ_e. We can see that the simulation results match well with the theoretical curve, validating the effectiveness of our performance evaluation for the NGSO SATCOM system. Another observation from Fig. 5(b) is that a larger degree of climate abnormality will lead to the decrease of SOP at this moment, and severe abnormal precipitation of eavesdropper can drive the SOP to be about 0.5. Comparing the results in Fig. 5(a) and Fig. 5(b), it indicates that the impact of specific rain attenuation is more serious than that of climate abnormality on the secure communication performance of a NGSO SATCOM system.

C. DISCUSSIONS

Since rain attenuation is a dominant factor which influences the communication in an NGSO SATCOM system, we conduct extensive simulations to explore its effects on the PLS performance. All series of simulations start from the same spatial state that the coordinates of the satellite, legitimate earth station and eavesdropper are respectively identical with their coordinates at 12:00 PM on Jan. 1, 2018. Each simulation lasts for 2880 minutes, and during such a simulation period CFESAT orbits the earth about 30 times.

Fig. 6 presents the performance of secrecy capacity and SOP in different months. We can see that both the behaviors exhibit the periodicity, but they just experience two cycles during 2880 minutes (such a phenomenon can be also seen in the figures later). This is due to the reason that the coordinates of earth stations also vary with the earth rotation in space. It is known that the rain rate in each month is different,

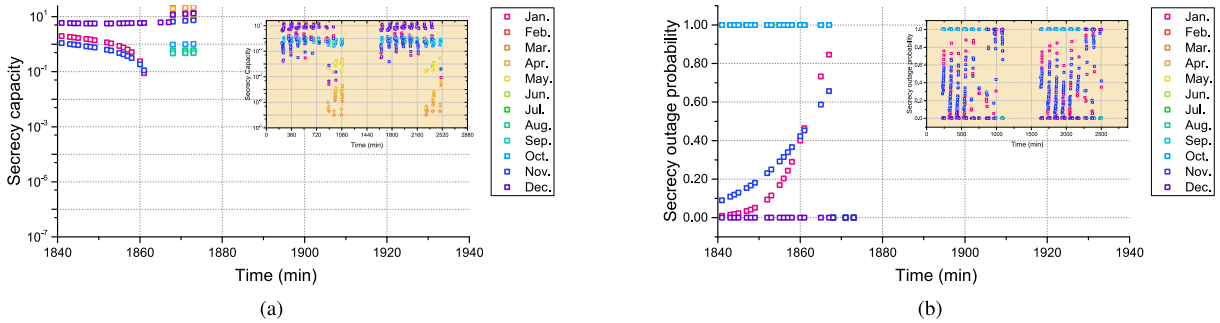


FIGURE 6. Performance of secrecy capacity and SOP in different months. (a) Secrecy capacity. (b) Secrecy outage probability.

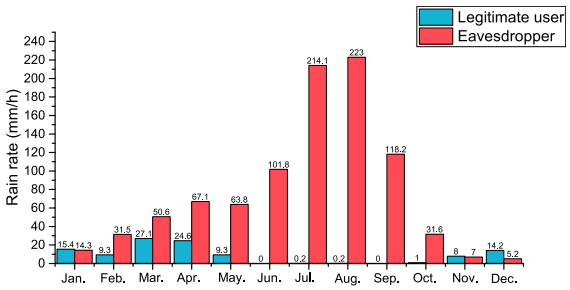


FIGURE 7. Precipitation of each month.

so Fig. 6 describes the PLS performance under different rain rate situations, and such performance obviously presents distinctive seasonal features. In this simulation, the legitimate earth station is located in a region with a hot desert climate, which experiences very little rainfall, especially in summer, while the eavesdropper is located in a region with a tropical savanna climate, which has distinct wet and dry seasons. For a more intuitive understanding of the two climates, we summarize in Fig. 7 the average precipitation of each month in the two regions.

We can discover from Fig. 6 that the secrecy capacity of the system is higher in summer than that in winter, this is because that the eavesdropper has a lower channel capacity in the monsoon season from June to August. Regarding the SOP, we find that except January and November, it approaches to either 0 or 1. This is due to the reason that the rain rates of the legitimate receiver and eavesdropper are almost the same in January and November, but a huge gap exists in other months. Another empirical acquirement from Fig. 6 and Fig. 7 is that the SOP tends to be 0 if the rain rate of the legitimate receiver is less than half of that of the eavesdropper. The changes of SOP in January and November result from the variations of distances between the satellite CFESAT and the two earth stations.

We then explore how the abnormal weather influences the PLS performance of the NGSO SATCOM system. Fig. 8 presents the secrecy capacity and secrecy outage probability under different degrees of weather abnormality in the region of eavesdropper earth station. In this simulation, we use the mean value $\bar{\gamma}_e$ instead of the instantaneous value γ_e to obtain an average secrecy capacity. Therefore, the secrecy capacity with different values of σ_e is the same, and we only plot its behaviors with $\sigma_e = 10$ in Fig. 8(a). Regarding the SOP performance, we can see from Fig. 8(b) that the weather abnormality will incur a distinct impact. When the system has a low SOP, for example, the relative location of the legitimate earth station is superior to that of the eavesdropper, a larger value of σ_e can lead to an increase of SOP; otherwise, if the system has a high SOP, a larger value of σ_e can results in a decrease of SOP. Moreover, SOP will be driven to about 0.5 as σ_e is large enough. It suggests that the PLS performance of an NGSO SATCOM system can be improved through some technologies such as artificial rain dispersal for the legitimate earth station, and cloud seeding which enhances the precipitation for the eavesdropper.

We further draw Fig. 9 to show how the transmission frequency influences the PLS performance of the NGSO SATCOM system. We can see that the impact of transmission frequency on secrecy capacity and secrecy outage probability is somewhat sophisticated. As the transmission frequency increases, the PLS performance is sometimes improved and sometimes deteriorated. For example, with a higher transmission frequency, the system has a lower SC and a higher SOP at about 1080 minute, while it can achieve a higher SC and a lower SOP at about 1840 minute. It is known from [47] that the specific rain attenuation will increase as the transmission frequency increases. Thus, a larger f will lead to a larger γ_e ($\bar{\gamma}_e$), and further results in a larger C_s and a smaller P_{so} if $\alpha_e > k_\rho k_\gamma \alpha_l$, while a smaller C_s and a larger P_{so} if $\alpha_e < k_\rho k_\gamma \alpha_l$. It is worth noting that usually $\alpha_e > k_\rho k_\gamma \alpha_l$ holds on the condition that the relative position of the eavesdropper is superior to that of legitimate earth station, i.e., the PLS performance of the system is poor. Therefore, we obtain an empirical guideline for the practical operation that it is better for the satellite to transmit signals using a high frequency when the eavesdropping situation is serious, while using a low frequency if the legitimate transmitting is in a superior condition.

Finally, we consider a potential eavesdropper which could be located in any place on the earth, and draw the PLS performance corresponding to the eavesdropper's location on a global map, as shown in Fig. 10. In this figure, the

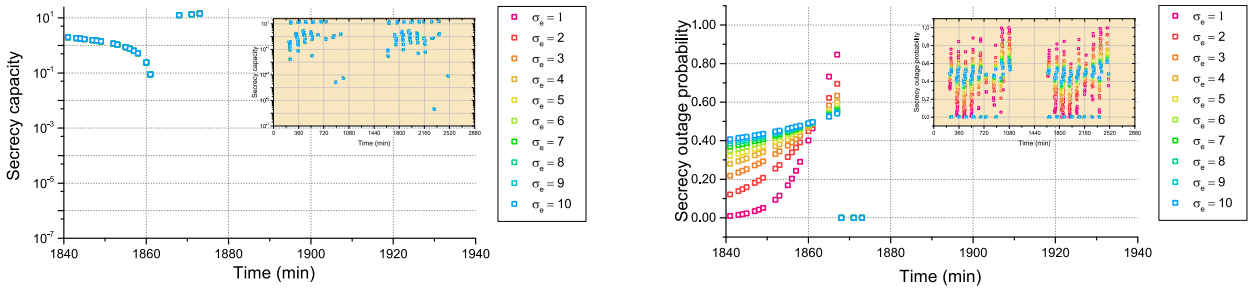


FIGURE 8. Influence of abnormal weather on PLS performance. (a) Secrecy capacity. (b) Secrecy outage probability.

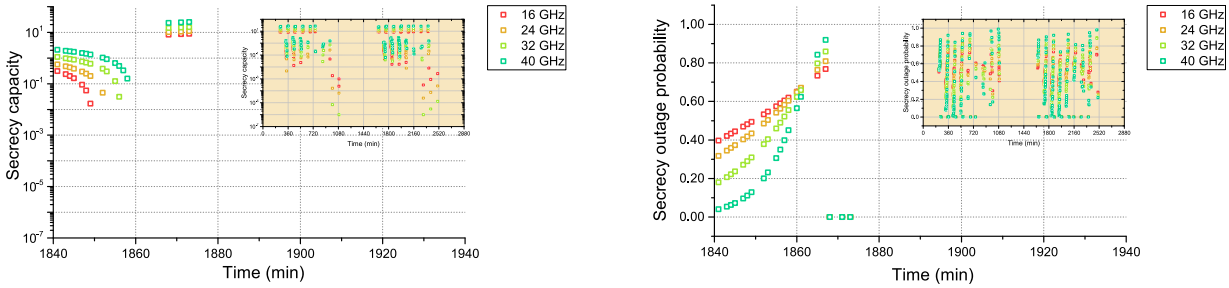


FIGURE 9. Influence of frequency on PLS performance. (a) Secrecy capacity. (b) Secrecy outage probability.

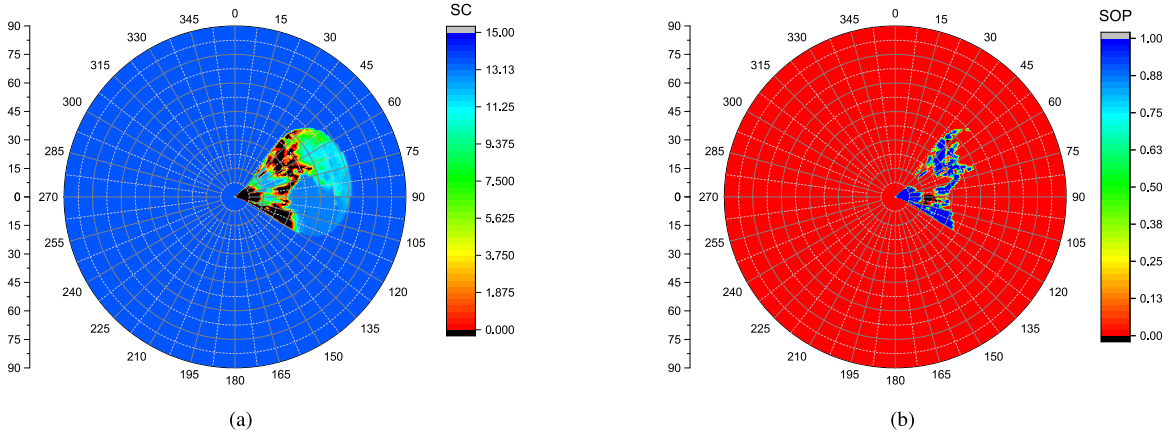


FIGURE 10. PLS performance map of CFESAT. (a) Secrecy capacity. (b) Secrecy outage probability.

system time is 17:26 PM on Jan. 2, 2018, and the subsatellite point of CFEAST is at (16.42°S, 59.91°E). We can see from Fig. 10(a) and Fig. 10(b) that the secrecy capacity and SOP can keep their best in most of regions on the map. This is because that the eavesdropper located in such regions is out of the coverage of CFESAT. It is obvious that the PLS performance becomes poor as the eavesdropper approaches the location of the legitimate earth station, which inspires us to build a conservation zone around the legitimate earth station in the practical system configuration. It is worth noting that the PLS performance map for any satellite, any location of an earth station and any system time can be drawn through running our simulator, and such a map is helpful for the real operation in an NGSO SATCOM system.

VI. CONCLUSION

This paper studied, for the first time, the performance of a satellite communication system operating over a non-geostationary orbit, from a physical layer security perspective. In order to characterize the movement state of an NGSO satellite, we introduced three types of satellite orbiting models. With the help of these models and full consideration of rain attenuation, we analyzed the PLS performance of the concerned system in terms of secrecy capacity and secrecy

outage probability, deriving their expressions in closed-from. The effectiveness of our performance analysis has been validated by simulations. Our theoretical results can be applied to predict the system PLS performance at any time and provide guidelines for the practical system configuration and operation.

REFERENCES

[1] D. Roddy, *Satellite Communications, (Professional Engineering)*, 4th ed. New York, NY, USA: McGraw-Hill, 2006.

[2] P. Chini, G. Giambene, and S. Kota, "A survey on mobile satellite systems," *Int. J. Satellite Commun.*, vol. 28, no. 1, pp. 29–57, Jan./Feb. 2009.

[3] B. G. Evans, O. Onireti, T. Spathopoulos, and M. A. Imran, "The role of satellites in 5G," in *Proc. 7th Adv. Satellite Multimedia Syst. Conf., 13th Signal Process. Space Commun. Workshop (ASMS/SPSC)*, 2014, pp. 197–202.

[4] M. Shafi *et al.*, "5G: A tutorial overview of standards, trials, challenges, deployment, and practice," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 6, pp. 1201–1221, Jun. 2017.

[5] W. Stallings, *Introduction Cryptography and Network Security: Principles and Practice*. Upper Saddle River, NJ, USA: Pearson, 2017.

[6] J.-P. Aumasson, "The impact of quantum computing on cryptography," *Comput. Fraud, Secur.*, vol. 2017, no. 6, pp. 8–11, 2017.

[7] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

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

[9] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[10] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[11] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[12] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[13] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[14] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[15] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1204–1219, Mar. 2016.

[16] Z. Qin, Y. Liu, Z. Ding, Y. Gao, and M. Elkashlan, "Physical layer security for 5G non-orthogonal multiple access in large-scale networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6.

[17] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[18] I. Krikidis, J. S. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[19] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[20] J. P. Vilela, P. C. Pinto, and J. Barros, "Position-based jamming for enhanced wireless secrecy," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 616–627, Sep. 2011.

[21] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 878–881, Jun. 2012.

[22] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Process. Lett.*, vol. 22, no. 8, pp. 1147–1151, Aug. 2015.

[23] L. Tang, H. Chen, and Q. Li, "Social tie based cooperative jamming for physical layer security," *IEEE Commun. Lett.*, vol. 19, no. 10, pp. 1790–1793, Oct. 2015.

[24] J. Yao, S. Feng, X. Zhou, and Y. Liu, "Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 753–764, Feb. 2016.

[25] Y. Xu, J. Liu, Y. Shen, X. Jiang, and T. Taleb, "Security/qos-aware route selection in multi-hop wireless ad hoc networks," in *Proc. IEEE ICC*, May 2016, pp. 1–6.

[26] Y. Xu, J. Liu, O. Takahashi, N. Shiratori, and X. Jiang, "SOQR: Secure optimal QoS routing in wireless ad hoc networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2017, pp. 1–6.

[27] Y. Xu, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Physical layer security-aware routing and performance tradeoffs in ad hoc networks," *Comput. Netw.*, vol. 123, pp. 77–87, Aug. 2017.

[28] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[29] R. Bassily *et al.*, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sep. 2013.

[30] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[31] L. J. Rodríguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: State of the art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015.

[32] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.

[33] D. K. Petraki, M. P. Anastasopoulos, and S. Papavassiliou, "Secrecy capacity for satellite networks under rain fading," *IEEE Trans. Dependable Secure Comput.*, vol. 8, no. 5, pp. 777–782, Sep./Oct. 2011.

[34] J. Lei, Z. Han, M. Á. Vazquez-Castro, and A. Hjorungnes, "Secure satellite communication systems design with individual secrecy rate constraints," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 661–671, Sep. 2011.

[35] *Propagation Data and Prediction Methods Required for the Design of Earth-Space Telecommunication Systems*, document P.618-13, ITU-R, Geneva, Switzerland, 2017.

[36] G. Zheng, P.-D. Arapoglou, and B. Ottersten, "Physical layer security in multibeam satellite systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 852–863, Feb. 2012.

[37] A. Kalantari, G. Zheng, Z. Gao, Z. Han, and B. Ottersten, "Secrecy analysis on network coding in bidirectional multibeam satellite communications," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1862–1874, Sep. 2015.

[38] 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.

[39] K. An, M. Lin, T. Liang, J. Ouyang, C. Yuan, and Y. Li, "Secure transmission in multi-antenna hybrid satellite-terrestrial relay networks in the presence of eavesdropper," in *Proc. IEEE Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2015, pp. 1–5.

[40] K. An, M. Lin, T. Liang, J. Ouyang, and H. Chen, "Average secrecy capacity of land mobile satellite wiretap channels," in *Proc. IEEE Int. Conf. Wireless Commun., Signal Process. (WCSP)*, Oct. 2016, pp. 1–5.

[41] R. K. Crane, *Propagation Handbook for Wireless Communication System Design*. Boca Raton, FL, USA: CRC Press, 2003.

[42] A. D. Panagopoulos, P.-D. M. Arapoglou, and P. G. Cottis, "Satellite communications at KU, KA, and V bands: Propagation impairments and mitigation techniques," *IEEE Commun. Surveys Tuts.*, vol. 6, no. 3, pp. 2–14, 3rd Quart., 2004.

[43] P.-D. Arapoglou, K. Liolis, M. Bertinelli, A. Panagopoulos, P. Cottis, and R. De Gaudenzi, "MIMO over satellite: A review," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 1, pp. 27–51, 1st Quart. 2011.

[44] *Characteristics of Precipitation for Propagation Modelling*, document P.837-7, ITU-R, Geneva, Switzerland, 2017.

[45] K. Binder and D. Heermann, *Monte Carlo Simulation in Statistical Physics: An Introduction*. New York, NY, USA: Springer, 2010.

[46] Y. Xiao and J. Liu. (2018). *MATLAB Code for the Study of PHY-SEC in NGSO SATCOM Systems*. [Online]. Available: https://www.researchgate.net/profile/Jia_Liu100/contributions, doi: 10.13140/RG.2.2.18376.37128.

[47] *Specific Attenuation Model for Rain for Use in Prediction Methods*, document P.838-3, ITU-R, Geneva, Switzerland, 2005.

YEQIU XIAO received the B.Eng. degree in computer science and technology and the M.Eng. degree in computer software and theory from Xidian University, Xi'an, China, in 2013 and 2016, respectively, where she is currently pursuing the Ph.D. degree in computer system architecture. Her current research interests include the physical layer security in wireless communications.

JIA LIU (S'16–M'18) received the Ph.D. degree from the School of Systems Information Science, Future University Hakodate, Japan, in 2016. He is currently an Assistant Professor with the Center for Cybersecurity Research and Development, National Institute of Informatics, Japan. His research interests include mobile ad hoc networks, 5G communication systems, D2D communications, and cybersecurity. He has published over 20 technical papers in premium international journals and conferences, such as the IEEE TWC, IEEE TVT, *Computer Networks*, *Ad Hoc Networks*, *Computer Communications*, IEEE ICC, and IEEE WCNC.

YULONG SHEN received the B.S. and M.S. degrees in computer science and Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2002, 2005, and 2008, respectively. He is currently a Professor with the School of Computer Science and Technology, Xidian University, where he is also an Associate Director of the Shaanxi Key Laboratory of Network and System Security and a member of the State Key Laboratory of Integrated Services Networks. His research interests include wireless network security and cloud computing security. He has also served on the technical program committees of several international conferences, including ICEBE, INCoS, CIS, and SOWN.

XIAOHONG JIANG (M'03–SM'08) received the B.S., M.S., and Ph.D. degrees from Xidian University, China, in 1989, 1992, and 1999, respectively. He was an Associate Professor with Tohoku University, from 2005 to 2010. He is currently a Full Professor with Future University Hakodate, Japan. His research interests include computer communications networks, mainly wireless networks and optical networks, network security, and routers/switches design. He has published over 300 technical papers in premium international journals and conferences, which include over 70 papers published in the top IEEE journals and top IEEE conferences, like the IEEE/ACM TRANSACTIONS ON NETWORKING, the IEEE JOURNAL OF SELECTED AREAS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, and the IEEE INFOCOM. He is a member of IEICE. He received the Best Paper Award at the IEEE HPCC 2014, IEEE WCNC 2012, IEEE WCNC 2008, IEEE ICC 2005-Optical Networking Symposium, and IEEE/IEICE HPSR 2002.

NORIO SHIRATORI is currently a Professor with Chuo University, Tokyo, and an Emeritus Professor with Tohoku University, Sendai, Japan. He has published more than 15 books and over 600 refereed papers in computer science and related fields. He is a Life Fellow of the IEEE. He is also a Fellow of the Japan Foundation of Engineering Societies, the Information Processing Society of Japan (IPSJ), and the Institute of Electronics, Information and Communication Engineers (IEICE). He was a former President of IPSJ, from 2009 to 2011. He was an IEICE Honorary Member, in 2012, and an IPSJ Honorary Member, in 2013. He was a recipient of the Minister of MEXT Award from the Japanese Government, in 2016, the Science and Technology Award from the Ministry of Education, Culture, Sports, Science and Technology, in 2009, the IEICE Achievement Award, in 2001, the IEICE Contribution Award, in 2011, the IPSJ Contribution Award, in 2008, the IPSJ Memorial Prize Winning Paper Award, in 1985, the IPSJ Best Paper Award, in 1997, the IEICE Best Paper Award, in 2001, the IEEE 5th SCE01 Best Paper Award, in 2001, the IEEE ICPADS 2000 Best Paper Award, in 2000, and the IEEE 12th ICOIN Best Paper Award.