Article

Key Generation Method Based on Multi-Satellite Cooperation and Random Perturbation

Yinuo Hao ¹, Pengcheng Mu ², Huiming Wang ² and Liang Jin ^{1,*}

¹ Wireless Communication Technology Office, Information Engineering University, Zhengzhou 450002, China; dzy1996@stu.xjtu.edu.cn

² School of Information and Communications Engineering, Xi'an Jiaotong University, Xi'an 710049, China; pcmu@mail.xjtu.edu.cn (P.M.); hmwang@mail.xjtu.edu.cn (H.W.)

* Correspondence: jl@mail.ndsc.com.cn

Abstract: In low-earth-orbit (LEO) satellite-to-ground communication, the size of satellite antennae is limited and the satellite motion trajectory is predictable, which makes the channel state information (CSI) of the satellite-to-ground channel easy to leak and impossible to use to generate a physical layer key. To solve these problems, we propose a key generation method based on multi-satellite cooperation and random perturbation. On the one hand, we use multi-satellite cooperation to form a constellation that services users, in order to increase the equivalent aperture of satellite antennae and reduce the correlation between the legal channel and the wiretap channel. On the other hand, according to the endogenous characteristics of satellite motion, a random perturbation factor is proposed, which reflects the randomness of the actual channel and ensures that the CSI of the legal channel is not leaked due to the predictability of satellite motion trajectory. Simulation results show that the proposed method can effectively reduce the leakage of the legal channel's CSI, which makes the method of physical layer key generation safe and feasible in the LEO satellite-to-ground communication scene.

Keywords: physical layer security; key generation; LEO satellite-to-ground communication

Citation: Hao, Y.; Mu, P.; Wang, H.; Jin, L. Key Generation Method Based on Multi-Satellite Cooperation and Random Perturbation. *Entropy* **2021**, *23*, 1653. <https://doi.org/10.3390/e23121653>

Academic Editors: Eirik Rosnes, Alexandre Graell i Amat and Hsuan-Yin Lin

Received: 13 October 2021

Accepted: 3 December 2021

Published: 8 December 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

With the development of wireless communication technology, LEO satellite communication technology has become an important part of global wireless communication [1,2]. Compared with ground communication, LEO satellite communication has wider coverage and larger communication capacity. Compared with geostationary earth orbit (GEO) satellite communication, LEO satellite communication has lower delay and transmission loss [3,4]. Therefore, the study of LEO satellite communication is of far-reaching significance for building 6G Space-Air-Ground Integrated Networks (SAGINs) and meeting the seamless global coverage of future communication networks [5–8].

However, due to the wide coverage and broadcasting characteristics of wireless LEO satellite communications, the satellite-to-ground signals can be freely transmitted within hundreds of kilometers on the ground, which allows eavesdroppers, ultra-long distances away, to wiretap the CSI of the legal channel.

At present, there are two main methods to solve the security problems in LEO satellite communications:

1. **Traditional Cryptography:** Traditional cryptography generates secret keys through a cryptographic algorithm, and then distributes them to legitimate users to encrypt the plaintext. This method uses the computational complexity of cryptographic algorithms to ensure the security of cipher text. Actually, encryption and decryption calculations in this method require a lot of computing resources. Additionally, key management and distribution rely on complex protocol architecture. So, it is not suitable for LEO satellite communication systems with limited computing resources,

rapid changes in network topology, and massive access to users. Further, with the rapid development of advanced computing technology, this method based on computational complexity faces challenges in terms of reliability and robustness [9].

2. Physical Layer Security (PLS): Physical layer security uses the endogenous characteristics of the wireless channel, such as time varying, randomness and uniqueness, to directly extract the secret key. This method has the advantages of simple cryptographic calculations and no additional overhead on key management and distribution [10,11], which is suitable for LEO satellite communication systems. Therefore, the use of PLS technology to solve the security problems in LEO satellite communication has attracted great attention from many scholars.

At present, research on physical layer security technology for satellite-to-ground communication is concentrated on physical layer security transmission, mainly including the following three aspects [9]:

1. Security Performance Analysis: For example, ref. [12] analyzed the security performance of a satellite-to-ground communication network with a legitimate user and eavesdropper. This paper also proposed the closed expressions of confidential capacity probability, confidential interruption probability and average confidentiality probability.
2. Transmission Power Optimization: For example, ref. [13] proposed a transmission power optimization method for multi-antenna satellite communication based on PLS, which can effectively prevent eavesdroppers from wiretapping communication signals.
3. Security Rate Maximum: For example, ref. [14] used the PLS method to optimize the beamforming vector by combining the uplink and downlink time allocation according to the requirements of different target receivers for different speeds and data transmission rates, which can maximize the system security rate.

According to existing research, the physical layer key generation technology for LEO satellite communication scenarios has not been extensively studied. This is mainly due to the following two reasons:

1. The Insecurity of Satellite Trajectory: Different from the electromagnetic wave propagation conditions of the ground scenario, satellite-to-ground communication includes two parts: the space segment and the telephone segment. The CSI of the satellite-to-earth channel is directly related to the position of satellites and ground receivers [3,15]. Due to the openness of satellite motion parameters, satellite orbits are predictable, which means eavesdroppers can directly obtain the position of satellites and ground receivers. This leads to the revelation of the legal channel's CSI and insecurity of physical layer key sources.
2. The Insecurity of Satellite Signals: Due to the limited size, satellite antennae always have a small equivalent aperture and a wide signal beam in long-distance satellite-to-ground communication. When satellite signals reach the ground, they can be regarded as far-field parallel lights [16]. Therefore, each satellite signal can cover numerous ground receivers within a range of hundreds of kilometers, and each satellite-to-ground channel is highly correlated with another. This means eavesdroppers can easily obtain the CSI of the legal channel by estimating relevant channels. In this case, the physical layer key generation method is impractical.

To solve the above problems, we proposed a model of multi-satellite cooperation and random perturbation in a satellite-to-ground communication system, and put forward a key generation method based on it. The main contributions are as follows:

- We proposed a multi-satellite coordination model to solve the problem that the channels between a single satellite and multiple ground receivers have strong correlations.
- We introduced a satellite perturbation factor into the channel model to restore the endogenous randomness of the satellite-to-ground channel, which can improve the randomness of the channel and prevent eavesdroppers from predicting the satellite position precisely.

- Based on the above model, we proposed a key generation method to generate secret keys from the satellite-to-ground channel, which includes four parts: channel estimation, quantify, information negotiation and privacy magnification.
- To verify the feasibility of the proposed method, we simulated and analyzed the randomness and safety of the generated key. The simulation results show that the proposed model has endogenous randomness and the proposed key generation method is feasible.

2. System Model

As shown in Figure 1, we consider a LEO satellite-to-ground communication network model, including N LEO satellites, a legitimate user Bob and an eavesdropper Eve. Each node is equipped with a single antenna. Bob hopes to extract secret keys from satellite-to-ground channels, and Eve passively eavesdrops on the process without interfering with the key generation process.

Figure 1. System model.

When the satellites move along the orbits, define two complex random variables h_k and g_k as the channel from the k th satellite to Bob and Eve, respectively. Define the mean of h_k and g_k is 0, and the variance of them is $\sigma_{h_k}^2 = \sigma_h^2$ and $\sigma_{g_k}^2 = \sigma_g^2$, $k \in \{1, 2, \dots, N\}$. Define the position shifts of satellites on ideal orbits caused by the gravitational force of stars, sunlight pressure and other factors as the perturbation factor. Considering the impact of satellite perturbation in the actual satellite communication scenario, we introduce the perturbation offset phase $\Delta\varphi = \{\Delta\varphi_1, \dots, \Delta\varphi_k\}$ and $\Delta\theta = \{\Delta\theta_1, \dots, \Delta\theta_k\}$. The actual channel from the k th satellite to Bob and Eve can be defined as $h_k e^{-j\pi \sin \Delta\varphi_k}$ and $g_k e^{-j\pi \sin \Delta\theta_k}$, respectively, where $\Delta\varphi \sim U(-\frac{\pi}{2}, \frac{\pi}{2})$ and $\Delta\theta \sim U(-\frac{\pi}{2}, \frac{\pi}{2})$. The channel from N satellites to Bob and Eve can be defined, respectively, as $\vec{h} = [h_1 e^{-j\pi \sin \Delta\varphi_1}, h_2 e^{-j\pi \sin \Delta\varphi_2}, \dots, h_N e^{-j\pi \sin \Delta\varphi_N}]$ and $\vec{g} = [g_1 e^{-j\pi \sin \Delta\theta_1}, g_2 e^{-j\pi \sin \Delta\theta_2}, \dots, g_N e^{-j\pi \sin \Delta\theta_N}]$. Obviously, the perturbation factor is a random and unpredictable factor, which indicates the unique endogenous attributes of satellites that differ from other communication entities.

In the LEO satellite-to-ground communication system, the electromagnetic wave signals sent by satellites need to penetrate outer space and the atmosphere to reach the ground, which is affected by many factors during the propagation process, such as the atmospheric effect, large-scale fading, the multi-path effect, shadow fading, and Doppler Le frequency shift. According to [17], the satellite-to-ground channel can be divided into two parts: the space segment and the ground segment, which represents satellite-to-ground propagation and ground-to-environment propagation, respectively.

1. Space Segment

The transmission of signals in the space segment is mainly affected by the atmospheric effect. The envelope and phase of the signal obey the normal distribution, which can be expressed by

$$P_a(r_a) = \frac{1}{\sqrt{2\pi\sigma_a^2}} \exp\left[-\frac{(r_a - \mu_a)^2}{2\sigma_a^2}\right] \quad (1)$$

$$P_a(\varphi_a) = \frac{1}{\sqrt{2\pi\eta_a^2}} \exp\left[-\frac{(\varphi_a - u_a)^2}{2\eta_a^2}\right] \quad (2)$$

where r_a and φ_a represent the envelope and phase of the signal, and μ_a and u_a represent the mean of the envelope and phase, and σ_a^2 and η_a^2 represent the variance of the envelope and phase.

2. Ground Segment

Affected by the multi-path effect, the signal in the ground segment can be expressed as the sum of the LOS component and the multi-path component, which can be expressed as

$$r \exp(j\theta) = z \exp(j\Phi_z) + s \exp(j\Phi_s) \quad (3)$$

where r and θ represent the amplitude and phase of received signals, z and Φ_z represent the amplitude and phase of the LOS component, s and Φ_s represent the amplitude and phase of the multi-path component.

According to the influence of shadow fading on the LOS component, the three states of (3) and their probability distributions are as follows:

When the LOS component is not blocked, the signal obeys the Rice distribution:

$$P_{Rice}(r) = \frac{r}{w_0} \cdot \exp\left(-\frac{r^2 + A^2}{w_0}\right) I_0\left(\frac{Ar}{w_0}\right) \quad (A \geq 0, r \geq 0) \quad (4)$$

where $w_0 = \varepsilon[r^2]$ represents the average power of the multi-path component, A represents the power of the LOS component, and $I_0(\cdot)$ represents the zero-order Bessel function of the first kind.

When the LOS component is partially blocked, the signal obeys the Loo distribution:

$$P_{Loo}(r) = \int_0^\infty \frac{1}{z} \exp\left[-\frac{(\ln z - \mu)^2}{2\sigma_0^2} - \frac{r^2 + z^2}{2\sigma_0^2}\right] \cdot I_0\left(\frac{rz}{w_0}\right) dz \quad (5)$$

where μ and σ_0 represent the mean and variance of log-normal distribution.

When the LOS component is completely blocked, the signal obeys the Rayleigh distribution:

$$P_{Ray1}(r) = \frac{r}{w_0} \cdot \exp\left(-\frac{r^2}{2w_0}\right) \quad (r \geq 0) \quad (6)$$

In order to describe the long-term dynamic characteristic of the channel, the above three states can be described by a Markov process, which can be given by

$$P(r) = \omega_1 P_{Ray1}(r) + \omega_2 P_{Loo}(r) + \omega_3 P_{Rice}(r) \quad (7)$$

where ω_i represents the probability that the system is in state i . Considering the channel characteristics of the space segment and the ground segment, the phase and envelope of the LEO satellite-to-ground channel can be expressed as

$$P_{all}(r) = P_a(r_a) \cdot P(r) \quad (8)$$

$$P_{all}(\varphi) = P_a(\varphi_a) \cdot P(\varphi) \quad (9)$$

It can be seen from (3) that the existence of the LOS path means the satellite-to-ground communication scenario cannot meet the channel uniqueness principle. Even if the distance between Eve and Bob is much longer than half of the wavelength, there is still a strong correlation between the legal channel and the wiretap channel.

3. Secret Key Generation Method

Based on the above system model and typical point-to-point physical layer key generation method, we proposed a key generation method for LEO satellite-to-ground communication scenarios, which includes four parts: channel estimation, quantify, information negotiation and privacy magnification [18–20].

3.1. Channel Estimation

3.1.1. Channel Estimation of Bob

Define x as the pilot transmitted from satellites to Bob. The signal received by Bob and Eve can be given by [21,22]

$$y_b = \begin{bmatrix} h_1 e^{-j\pi \sin \Delta \varphi_1} & \dots & h_N e^{-j\pi \sin \Delta \varphi_N} \end{bmatrix} \begin{bmatrix} x \\ \vdots \\ x \end{bmatrix} + n_b \quad (10)$$

$$= \sum_{k=1}^N h_k e^{-j\pi \sin \Delta \varphi_k} x + n_b$$

$$y_e = \begin{bmatrix} g_1 e^{-j\pi \sin \Delta \theta_1} & \dots & g_N e^{-j\pi \sin \Delta \theta_N} \end{bmatrix} \begin{bmatrix} x \\ \vdots \\ x \end{bmatrix} + n_e \quad (11)$$

$$= \sum_{k=1}^N g_k e^{-j\pi \sin \Delta \theta_k} x + n_e$$

where n_b and n_e denote the additive white Gaussian noise of Bob and Eve with mean 0 and variance σ_n^2 , respectively. According to the reciprocity of the wireless channel, Bob and Eve can use pilot signals sent by satellites to estimate the channel [23]. The channel estimation results of Bob and Eve can be expressed as

$$\tilde{h} = \frac{x^*}{\|x\|^2} y_b = \sum_{k=1}^N h_k e^{-j\pi \sin \Delta \varphi_k} + \frac{x^*}{\|x\|^2} n_b \quad (12)$$

$$\tilde{g} = \frac{x^*}{\|x\|^2} y_e = \sum_{k=1}^N g_k e^{-j\pi \sin \Delta \theta_k} + \frac{x^*}{\|x\|^2} n_e \quad (13)$$

where x^* is the conjugation of x and $\|m + ni\| = \sqrt{m^2 + n^2}$ ($m, n \in R$).

3.1.2. Channel Estimation of Satellites

Define a as the pilot transmitted from Bob to satellites. Due to the reciprocity of uplink and downlink channels, the signal of k th satellite received can be given by

$$y_k = h_k e^{-j\pi \sin \Delta \varphi_k} a + n_{bk} \quad (14)$$

where n_{bk} represents the additive white Gaussian noise from k th satellite to Bob. The channel estimation results of k th satellite can be expressed as

$$\tilde{h}_k = h_k e^{-j\pi \sin \Delta \varphi_k} + \frac{a^*}{\|a\|^2} n_{bk} \quad (15)$$

In order to obtain the same key source for both the sending and receiving ends, each satellite needs to share the channel estimation results obtained by itself to all satellites

through the inter-satellite communication link. When information sharing between the satellites is completed, the key source obtained by each satellite can be expressed as

$$\tilde{z} = \sum_{n=1}^k \left(\tilde{h}_k e^{-j\pi \sin \Delta \varphi_k} + \frac{a^*}{\|a\|^2} n_{bk} \right) \quad (16)$$

Since this process transmits signals through the inter-satellite link, Eve cannot eavesdrop on relevant information.

From (12) and (16), it can be seen that both satellites and Bob have obtained the sum of CSI of N satellite-to-ground channels, which has intrinsic security attributes of time varying and randomness. In the proposed method, we used the sum of CSI as key source for physical layer key generation.

3.2. Quantify

After channel estimation, a continuous signal can be quantized into discrete signals by determining the quantization threshold. In order to maximize the information entropy after quantization, we adopted the method of equal probability quantization, so that the probability of samples falling into each quantization interval is equal.

Moreover, the amplitude and phase information are quantized separately, considering the distribution that they obey. Since Eve cannot obtain key source with the same distribution as Bob, she cannot obtain a quantitative result consistent with Bob.

3.3. Information Negotiation

In order to ensure that legitimate communication parties obtain a consistent key, information negotiation techniques based on protocol are usually used [24]; or an error-correcting code. In order to reduce the time of information exchange, we select a Low-Density Parity Check code (LDPC) with a code length of 2000 for information negotiation, which uses the error correction capability of LDPC to correct the inconsistent bits between the quantization results.

3.4. Privacy Magnification

To enhance the bit mismatch ratio (BMR) between the key generated by legal users and Eve, we use the hash function of the SHA256 algorithm for privacy amplification [25]. Although this procedure cannot increase the randomness of the original key, it avoids the possibility of weak keys causing loopholes in the encryption algorithm.

4. Theoretical Analysis

4.1. Equivalent Near-Field Model Analysis

Due to the limited size of satellite antennae and the long distance from the satellite to the ground, satellite signals are far-field parallel light when they reach Bob and Eve. Taking the k th satellite signal as an example, the far-field parallel light modeling of Bob and Eve is shown in Figure 2, where d denotes the distance between Bob and Eve, and θ_k denotes the angle between the direction of the k th satellite signal and the normal. As shown in Figure 2, the channel between the k th satellite and Eve can be given by

$$g_k = h_k e^{-j \frac{2\pi d \sin \theta_k}{\lambda}} \quad (17)$$

where λ denotes the wavelength. In the far-field model, define $d = \lambda/2$, then

$$g_k = h_k e^{-j\pi \sin \theta_k} \quad (18)$$

Figure 2. Far-field parallel light model.

Theorem 1. *In the far-field model, the larger the number and spacing of satellites, the larger the equivalent aperture of satellite antennae, the narrower the signal beam, and the lower the correlation between the channel from satellite to Bob and Eve. In this case, the far-field model can be equivalent to the near-field model for analysis.*

Proof of Theorem 1. According to the actual communication scenario, we model the N satellites with an overall line model. l is the satellite spacing distance (100–120 km), L is the linear array length, λ is the wavelength, and H is the distance between the line array and Bob (1000–2000 km). The LEO satellite-to-ground communication frequency is in the ka band (29.1–29.3 GHz). The equivalent antenna aperture of the uniform linear array can be expressed by [26]:

$$\rho_0 = \frac{L}{\lambda} = \frac{(N-1) \cdot l}{\lambda} \quad (19)$$

□

According to the definition of the electromagnetic near-field model and the far-field model, when $H \geq 2\rho_0^2/\lambda_{\min}$, this system can be considered as a far-field model. Conversely, when $H < 2\rho_0^2/\lambda_{\min}$, this system can be considered as a near-field model [26]. Substituting the relevant parameters above into (19), it can be seen that $H \ll 2\rho_0^2/\lambda_{\min}$, in which case the terminal distance can be degenerated from the far-field model to the near-field model. Therefore, a constellation composed of multiple satellites can be equivalent to an antenna with a super-large aperture, and the equivalent aperture increases as the number of satellites and the distance between adjacent satellites increase. In the near-field model, due to the spatial uniqueness of the wireless channel, Eve cannot obtain the relevant information of the legal channel. In this case, Bob can use the sum of N satellite-to-earth channels to generate the physical layer key.

4.2. Security Analysis

In the physical layer key generation method, the security of the key source comes from the legal channel cannot be eavesdropped on. In order to prove that the proposed method can guarantee the security of the legal channel and further study the influence of number of satellites and the perturbation factor on it, we analyzed the security of the legal channel in this section.

According to the definition of the correlation coefficient, define A and B as two complex random variables, and $\rho(A, B)$ as the correlation coefficient between A and B [27,28]. When $\|\rho(A, B)\| \leq 0.3$, two variables can be considered as uncorrelated. $\rho(A, B)$ can be given by

$$\rho(A, B) = \frac{\text{Cov}(A, B)}{\sqrt{\text{Var}[A]} \sqrt{\text{Var}[B]}} \quad (20)$$

where $\text{Cov}(A, B)$ indicates the covariance of A and B , and $\text{Var}[\cdot]$ indicates the variance of a random variable.

4.2.1. Influence of Satellite Number

The correlation coefficient between the legal channel $\tilde{h}$ and the wiretap channel $\tilde{g}$ can be given by

$$\begin{aligned}\rho(\tilde{h}, \tilde{g}) &= \frac{\text{Cov}(\tilde{h}, \tilde{g})}{\sqrt{\text{Var}[\tilde{h}]} \sqrt{\text{Var}[\tilde{g}]}} \\ &= \frac{N\sigma_h^2[(\mu_c^3 + \mu_c\mu_s^2) + j(\mu_s^3 + \mu_c^2\mu_s)]}{\sqrt{N[\sigma_h^2(\sigma_c^2 + \mu_c^2 + \sigma_s^2 + \mu_s^2)] + \frac{1}{\|x\|^2}\sigma_h^2} \sqrt{N[\sigma_s^2(\sigma_c^2 + \mu_c^2 + \sigma_s^2 + \mu_s^2)] + \frac{1}{\|x\|^2}\sigma_h^2}}\end{aligned}\quad (21)$$

μ_c and σ_c^2 are the mean and variance of $\cos(\pi \sin \alpha_k)$ and μ_s and σ_s^2 are the mean and variance of $\sin(\pi \sin \alpha_k)$, where $k \in \{1, 2, \dots, N\}$ and $\alpha_k \in \{\Delta\varphi_k, \Delta\theta_k, \theta_k\}$. The derivation process of (21) is provided in Appendix A.

When $N = 1$, this indicates that in the case of a single satellite, Eve can infer the CSI of the legal channel through the wiretap channel. At this time, since the electrical size of the satellite antennae when it is normalized to the wavelength is very small, the satellite-to-ground communication model is a far-field parallel light model, and Bob cannot use the satellite-to-ground channel between herself and the LEO satellite to generate secret keys.

When $N > 1$, $\|\rho(\tilde{h}, \tilde{g})\|$ decreases as N increases. When the number of satellites N is large enough, the legal channel and the wiretap channel are regarded as uncorrelated, and Eve cannot infer the CSI of the legal channel through the wiretap channel. Bob can use the satellite-to-ground channel between herself and the LEO satellite to generate secret keys.

4.2.2. Influence of the Perturbation Factor

Due to the openness of satellite motion parameters, eavesdroppers can predict the current theoretical position of the satellite when it moves along the orbit, thereby obtaining the CSI of the legal channel. To ensure that Eve cannot obtain the CSI of the legal channel in this way, we consider the channel phase shift caused by the random perturbation of the satellite, and introduce a random perturbation factor to express the endogenous randomness of the satellite-to-ground channel, which can also ensure the security of the key source. We analyze the impact of the perturbation factor on the security of the key source in this section.

Define h' as the legal channel information obtained by Eve by calculating the satellite trajectory, which can be expressed as

$$h' = \sum_{k=1}^N h_k \quad (22)$$

The correlation coefficient between the legal channel $\tilde{h}$ and the channel calculated by Eve h' can be expressed as

$$\begin{aligned}\rho(\tilde{h}, h') &= \frac{\text{Cov}(\tilde{h}, h')}{\sqrt{\text{Var}[\tilde{h}]} \sqrt{\text{Var}[h']}} \\ &= \frac{N\sigma_h^2(\mu_c - j\mu_s)}{\sqrt{N[\sigma_h^2(\sigma_c^2 + \mu_c^2 + \sigma_s^2 + \mu_s^2)] + \frac{1}{\|x\|^2}\sigma_h^2} \sqrt{N\sigma_h^2}}\end{aligned}\quad (23)$$

The derivation process of (23) is provided in Appendix B. When $N = 1$, since the satellite-to-ground channel is not affected by the multi-path effect when there is only a single satellite, the random perturbation of the satellite only changes the phase of one main path. At this time, the predicted channel and the actual channel only differ by one phase, and the security of the key source cannot be guaranteed.

When $N > 1$, $\|\rho(\tilde{h}, h')\|$ decreases as N increases. If $\|\rho(\tilde{h}, h')\| \leq 0.3$, Eve cannot obtain the CSI of the legal channel by calculating satellite trajectory. The above analysis indicates that one phase shift caused by a single perturbation factor is meaningless, and

only the superposition of different phase shifts caused by multiple perturbation factors is reliable. Therefore, by introducing the perturbation factor method, the security of the key source in the multi-satellite cooperative communication system can be guaranteed. In this case, the superposition of multiple perturbation factors causes drastic changes in the channel phase, which greatly increases the randomness and time-varying nature of the satellite-to-ground channel.

5. Simulation Analysis

In order to verify the effectiveness and feasibility of the proposed method, we conducted a series of simulation experiments in MATLAB R2016a environment to analysis the randomness and security of the generated key. We use the Monte Carlo method to conduct 10,000 experiments, and each experiment randomly generates channel and noise data to ensure the accuracy of the experiment. The simulation conditions are as follows:

1. The number of LEO satellites is $N = 4$.
2. Signal-to-noise ratio is $SNR = 20$ dB.
3. $\sigma_h^2 = 1$, $\sigma_n^2 = 0.01$.
4. The satellites are evenly distributed on a circular arc centered on Bob with a radius of 2000 km, the distance between adjacent satellites is 110 km.
5. The satellite-to-ground communication frequency is 29.3 GHz (ka band).

5.1. Randomness Analysis

We use the NIST [29] suite of statistical tests to test the randomness of the key. There are 15 items in NIST test totally, and all items return a p -value to summarize the strength of the evidence against the null hypothesis. When the p -value is larger than the chosen significance level ($\alpha \in [0.001, 0.01]$), the sequence is accepted as random.

In this paper, due to the extremely long sequence (larger than 10^6) required in some test items which are not available in the current simulation, we run 8 items (over half of all the 15 test) to evaluate the randomness of the key sequence, which still satisfies NIST's requirements [29,30]. Moreover, we choose α as 0.01 and perform 8 NIST tests for 100,000 trials, where each key has a length of 256 bits. The test results are shown in Table 1. It can be seen that the key generated by the proposed method has passed the NIST test, which indicates that the key has high randomness.

Table 1. p -values of the NIST statistical test.

Environment	Pass Ratio	p -Value
Frequency	1.00000	0.911413
Block Frequency	0.96972	0.719747
Cumulative Sums(Fwd)	1.00000	0.419021
Cumulative Sums(Rev)	1.00000	0.595549
Runs	0.97731	0.289667
Longest Run	0.99651	0.798139
FFT	0.99892	0.213309
Serial	1.00000	0.616305, 0.41902

5.2. Security Analysis

Figure 3 simulates the relationship between the distance from Bob to Eve and $\|\rho(\tilde{h}, \tilde{g})\|$ in the case of different satellite numbers. It can be seen from Figure 3 that in the case of a single satellite communication scene, when Eve is within 97 km from Bob, the correlation coefficient of the two channel estimation results is close to 1, and the correlation information of the legal channel can be obtained at any position within 110 km.

Figure 3. Correlation coefficient distance.

Define $d_{\min}$ as the minimum distance between Eve and Bob when $\|\rho(\tilde{h}, \tilde{g})\| \leq 0.3$ is satisfied. $d_{\min}$ keeps decreasing with the number of satellites. When $N = 1$, $d_{\min} = 110$ km. When $N = 4$, $d_{\min}$ decreases to 83 m. The results show that Bob's safety distance can be effectively reduced by increasing the number of satellites, making it feasible for Bob to use satellite-to-ground channels to generate physical layer keys.

In order to prove that the proposed model in this paper can guarantee the security of the legal channel, we analyze the amplitude and phase of the ground receiving signal in the satellite-to-ground communication models with a single satellite or four satellites when Bob and Eve are 83 m away. Figures 4 and 5 show the change curve of the received signal's amplitude/phase in the time domain and the frequency domain, respectively. It can be seen from Figure 4a,b and Figure 5a,b that when $N = 1$ and $d = 83$, the amplitude and phase of the signals received by Bob and Eve have a strong correlation in time and frequency. Figure 4c,d and Figure 5c,d indicate that when the distance between Bob and Eve is constant, while the number of satellites increases, the amplitude and phase of the received signals of Bob and Eve are both uncorrelated in time and frequency.

Figure 4. Amplitude/phase time. (a) $N = 1$, $d = 83$; (b) $N = 1$, $d = 83$; (c) $N = 4$, $d = 83$; (d) $N = 4$, $d = 83$.

Figure 5. Amplitude/phase frequency. (a) $N = 1, d = 83$; (b) $N = 1, d = 83$; (c) $N = 4, d = 83$; (d) $N = 4, d = 83$.

The simulation results show that the proposed method can effectively reduce the correlation between the signals received by Bob and Eve, and ensure that the CSI of the legal channel cannot be eavesdropped on. At the same time, due to the random perturbation factor introduced, the changes in channel amplitude and phase caused by satellite perturbation can be expressed precisely, which ensures that the proposed method has practical feasibility.

6. Conclusions

This paper mainly studies the physical layer key generation method in LEO satellite-to-ground scenarios. Aiming at the problem that the legal channel information is easy to leak in LEO satellite-to-ground communication scenarios, a physical layer key generation method based on multi-satellite cooperation random perturbation is proposed. In this method, the method of multi-satellite cooperation is used to increase the equivalent aperture of satellite antennae and reduce the safety distance of legal users. At the same time, the perturbation factor is introduced in channel modeling to increase the randomness of the actual channel and prevent eavesdroppers from obtaining legal channel information by predicting the position of satellite movement. The simulation results show that the method proposed in this paper can realize physical layer key generation in LEO satellite-to-ground communication scenarios, and as the number of satellites increases, the security distance of legal users can be reduced from hundreds of kilometers to tens of meters. The proposed method provides a good solution to generation of a physical layer key in the LEO satellite-to-ground communication scenario, and provides a new idea for the application of PLS in 6G SAGINs.

Author Contributions: Conceptualization, L.J.; data curation, H.W.; formal analysis, Y.H.; investigation, P.M.; methodology, P.M., H.W. and L.J.; project administration, L.J.; resources, L.J.; software, Y.H., P.M. and H.W.; validation, Y.H.; writing—original draft, Y.H.; writing—review and editing, P.M., H.W. and L.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by NSFC (61521003), the Key Universities and Academic Disciplines Construction Project, and the National Defense Science and Technology Innovation Special Zone (18-163-00-TS-004-082-01).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is contained within the article.

Acknowledgments: We thank Honghao Zheng and Jianlei Zhao for Writing—review & editing.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Define $X = X^R + jX^I$ as a complex random variable, where $X \in \{h_k, g_k, n_b, n_e\}$. X^R and X^I represent the real and imaginary parts of X , respectively. In the same way as [31–33], define X^R and X^I as independent and identically distributed. The mean and variance of X^R and X^I can be given by

$$E[X] = E[X^R] + jE[X^I] = 0 \quad (\text{A1})$$

$$\text{Var}[X] = 2\text{Var}[X^I] = 2\text{Var}[X^R] \quad (\text{A2})$$

where $E[\cdot]$ indicates the mean of a random variable.

From (12) and (13), $\tilde{h}$ and $\tilde{g}$ can be given by

$$\begin{aligned} \tilde{h} &= \sum_{k=1}^N h_k e^{-j\pi \sin \Delta \varphi_k} + \frac{x^*}{\|x\|^2} n_b \\ &= \sum_{k=1}^N [(h_k^R + jh_k^I)(\cos(\pi \sin \Delta \varphi_k) - j \sin(\pi \sin \Delta \varphi_k))] + \frac{x^*}{\|x\|^2} n_b \\ &= \left[\sum_{k=1}^N (h_k^R \cos(\pi \sin \Delta \varphi_k) + h_k^I \sin(\pi \sin \Delta \varphi_k)) \right] \\ &\quad + j \left[\sum_{k=1}^N (-h_k^R \sin(\pi \sin \Delta \varphi_k) + h_k^I \cos(\pi \sin \Delta \varphi_k)) \right] + \frac{x^*}{\|x\|^2} n_b \end{aligned} \quad (\text{A3})$$

$$\begin{aligned} \tilde{g} &= \sum_{k=1}^N g_k e^{-j\pi \sin \Delta \theta_k} + \frac{x^*}{\|x\|^2} n_e \\ &= \sum_{k=1}^N [(g_k^R + jg_k^I)(\cos(\pi \sin \Delta \theta_k) - j \sin(\pi \sin \Delta \theta_k))] + \frac{x^*}{\|x\|^2} n_e \\ &= \left[\sum_{k=1}^N (g_k^R \cos(\pi \sin \Delta \theta_k) + g_k^I \sin(\pi \sin \Delta \theta_k)) \right] \\ &\quad + j \left[\sum_{k=1}^N (-g_k^R \sin(\pi \sin \Delta \theta_k) + g_k^I \cos(\pi \sin \Delta \theta_k)) \right] + \frac{x^*}{\|x\|^2} n_e \end{aligned} \quad (\text{A4})$$

Define h^R, h^I, g^R and g^I as

$$\begin{cases} h^R = \sum_{k=1}^N (h_k^R \cos(\pi \sin \Delta \varphi_k) + h_k^I \sin(\pi \sin \Delta \varphi_k)) \\ h^I = \sum_{k=1}^N (-h_k^R \sin(\pi \sin \Delta \varphi_k) + h_k^I \cos(\pi \sin \Delta \varphi_k)) \end{cases} \quad (\text{A5})$$

$$\begin{cases} g^R = \sum_{k=1}^N (g_k^R \cos(\pi \sin \Delta \theta_k) + g_k^I \sin(\pi \sin \Delta \theta_k)) \\ g^I = \sum_{k=1}^N (-g_k^R \sin(\pi \sin \Delta \theta_k) + g_k^I \cos(\pi \sin \Delta \theta_k)) \end{cases} \quad (\text{A6})$$

From (A3) and (A4), (A5) and (A6) can be derived as

$$\tilde{h} = h^R + jh^I + \frac{x^*}{\|x\|^2} n_b \quad (\text{A7})$$

$$\tilde{g} = g^R + jg^I + \frac{x^*}{\|x\|^2} n_e \quad (A8)$$

Since h^R and h^I are independent of n_b , from (A7), the variance of $\tilde{h}$ can be given by

$$\begin{aligned} \text{Var}[\tilde{h}] &= \text{Var}[h^R + jh^I] + \text{Var}\left[\frac{x^*}{\|x\|^2} n_b\right] \\ &= \text{Var}[h^R] + \text{Var}[h^I] + \frac{x^*}{\|x\|^2} \left(\frac{x^*}{\|x\|^2}\right)^* \text{Var}[n_b] \\ &= \text{Var}[h^R] + \text{Var}[h^I] + \frac{1}{\|x\|^2} \text{Var}[n_b] \end{aligned} \quad (A9)$$

In a similar way to (A9), the variance of $\tilde{g}$ can be given by

$$\text{Var}[\tilde{g}] = \text{Var}[g^R] + \text{Var}[g^I] + \frac{1}{\|x\|^2} \text{Var}[n_e] \quad (A10)$$

From (A5), the variance of h^R in (A9) can be given by

$$\begin{aligned} \text{Var}[h^R] &= \sum_{k=1}^N \text{Var}[h_k^R \cos(\pi \sin \Delta \varphi_k) + h_k^I \sin(\pi \sin \Delta \varphi_k)] \\ &= \sum_{k=1}^N (\text{Var}[h_k^R \cos(\pi \sin \Delta \varphi_k)] + \text{Var}[h_k^I \sin(\pi \sin \Delta \varphi_k)] \\ &\quad + 2\text{Cov}(h_k^R \cos(\pi \sin \Delta \varphi_k), h_k^I \sin(\pi \sin \Delta \varphi_k))) \end{aligned} \quad (A11)$$

Since h_k^R , h_k^I and $\Delta \varphi_k$ are independent of each other,

$$\begin{aligned} \text{Cov}(h_k^R \cos(\pi \sin \Delta \varphi_k), h_k^I \sin(\pi \sin \Delta \varphi_k)) &= E[h_k^R \cos(\pi \sin \Delta \varphi_k) \cdot h_k^I \sin(\pi \sin \Delta \varphi_k)] - E[h_k^R \cos(\pi \sin \Delta \varphi_k)] E[h_k^I \sin(\pi \sin \Delta \varphi_k)] \\ &= E[h_k^R] E[h_k^I] E[\cos(\pi \sin \Delta \varphi_k) \sin(\pi \sin \Delta \varphi_k)] - E[h_k^R] E[h_k^I] E[\sin(\pi \sin \Delta \varphi_k)] E[\cos(\pi \sin \Delta \varphi_k)] \\ &= 0 \end{aligned} \quad (A12)$$

So, (A11) can be derived as

$$\text{Var}[h^R] = \sum_{k=1}^N (\text{Var}[h_k^R \cos(\pi \sin \Delta \varphi_k)] + \text{Var}[h_k^I \sin(\pi \sin \Delta \varphi_k)]) \quad (A13)$$

In a similar way to (A13), the variance of h_k^I can be given by

$$\begin{aligned} \text{Var}[h^I] &= \sum_{k=1}^N \text{Var}[-h_k^R \sin(\pi \sin \Delta \varphi_k) + h_k^I \cos(\pi \sin \Delta \varphi_k)] \\ &= \sum_{k=1}^N (\text{Var}[h_k^R \sin(\pi \sin \Delta \varphi_k)] + \text{Var}[h_k^I \cos(\pi \sin \Delta \varphi_k)]) \end{aligned} \quad (A14)$$

Since that $\Delta \varphi_k$, $\Delta \theta_k$ and θ_k are independent and identically distributed, define the mean and variance of $\cos(\pi \sin \alpha_k)$ as μ_c and σ_c^2 , and the mean and variance of $\sin(\pi \sin \alpha_k)$ as μ_s and σ_s^2 , where $k \in \{1, 2, \dots, N\}$ and $\alpha_k \in \{\Delta \varphi_k, \Delta \theta_k, \theta_k\}$.

$$\begin{aligned} \text{Var}[h_k^R \cos(\pi \sin \Delta \varphi_k)] &= E[(h_k^R \cos(\pi \sin \Delta \varphi_k))^2] - (E[h_k^R \cos(\pi \sin \Delta \varphi_k)])^2 \\ &= E[(h_k^R)^2] E[(\cos(\pi \sin \Delta \varphi_k))^2] - (E[h_k^R] E[\cos(\pi \sin \Delta \varphi_k)])^2 \\ &= [E[h_k^R] + (E[h_k^R])^2] [E[\cos^2(\pi \sin \Delta \varphi_k)] + (E[\cos(\pi \sin \Delta \varphi_k)])^2] \\ &= \frac{1}{2} \sigma_h^2 (\sigma_c^2 + \mu_c^2) \end{aligned} \quad (A15)$$

In a similar way to (A15), it can be obtained that

$$\text{Var}[h_k^I \sin(\pi \sin \Delta \varphi_k)] = \text{Var}[h_k^R \sin(\pi \sin \Delta \varphi_k)] = \frac{1}{2} \sigma_h^2 (\sigma_s^2 + \mu_s^2) \quad (A16)$$

$$\text{Var}[h_k^I \cos(\pi \sin \Delta \varphi_k)] = \text{Var}[h_k^R \cos(\pi \sin \Delta \varphi_k)] = \frac{1}{2} \sigma_h^2 (\sigma_c^2 + \mu_c^2) \quad (\text{A17})$$

From (A13), (A14), (A16) and (A17), it can be obtained that

$$\begin{aligned} \text{Var}[h^R] &= N \left[\frac{1}{2} \sigma_h^2 (\sigma_c^2 + \mu_c^2) + \frac{1}{2} \sigma_h^2 (\sigma_s^2 + \mu_s^2) \right] \\ &= N \left[\frac{1}{2} \sigma_h^2 (\sigma_c^2 + \mu_c^2 + \sigma_s^2 + \mu_s^2) \right] \end{aligned} \quad (\text{A18})$$

$$\begin{aligned} \text{Var}[h^I] &= N \left[\frac{1}{2} \sigma_h^2 (\sigma_s^2 + \mu_s^2) + \frac{1}{2} \sigma_h^2 (\sigma_c^2 + \mu_c^2) \right] \\ &= N \left[\frac{1}{2} \sigma_h^2 (\sigma_c^2 + \mu_c^2 + \sigma_s^2 + \mu_s^2) \right] \end{aligned} \quad (\text{A19})$$

From (A9), (A18) and (A19), the variance of $\tilde{h}$ can be given by

$$\begin{aligned} \text{Var}[\tilde{h}] &= N \left[\frac{1}{2} \sigma_h^2 (\sigma_c^2 + \mu_c^2 + \sigma_s^2 + \mu_s^2) \right] + N \left[\frac{1}{2} \sigma_h^2 (\sigma_c^2 + \mu_c^2 + \sigma_s^2 + \mu_s^2) \right] + \frac{1}{\|x\|^2} \sigma_n^2 \\ &= N \left[\sigma_h^2 (\sigma_c^2 + \mu_c^2 + \sigma_s^2 + \mu_s^2) \right] + \frac{1}{\|x\|^2} \sigma_n^2 \end{aligned} \quad (\text{A20})$$

In a similar way to (A20), from (A10), the variance of $\tilde{g}$ can be given by

$$\text{Var}[\tilde{g}] = N \left[\sigma_g^2 (\sigma_c^2 + \mu_c^2 + \sigma_s^2 + \mu_s^2) \right] + \frac{1}{\|x\|^2} \sigma_n^2 \quad (\text{A21})$$

From (A7), the mean of $\tilde{h}$ can be given by

$$\begin{aligned} E[\tilde{h}] &= E[h^R + jh^I] + E \left[\frac{x^*}{\|x\|^2} n_b \right] \\ &= E[h^R] + jE[h^I] + \frac{x^*}{\|x\|^2} E[n_b] \end{aligned} \quad (\text{A22})$$

In a similar way to (A22), the mean of $\tilde{g}$ can be given by

$$E[\tilde{g}] = E[g^R] + jE[g^I] + \frac{x^*}{\|x\|^2} E[n_e] \quad (\text{A23})$$

From (A5), the mean of h^R in (A22) is

$$\begin{aligned} E[h^R] &= \sum_{k=1}^N E[h_k^R \cos(\pi \sin \Delta \varphi_k) + h_k^I \sin(\pi \sin \Delta \varphi_k)] \\ &= \sum_{k=1}^N (E[h_k^R \cos(\pi \sin \Delta \varphi_k)] + E[h_k^I \sin(\pi \sin \Delta \varphi_k)]) \\ &= \sum_{k=1}^N (E[h_k^R] E[\cos(\pi \sin \Delta \varphi_k)] + E[h_k^I] E[\sin(\pi \sin \Delta \varphi_k)]) \\ &= 0 \end{aligned} \quad (\text{A24})$$

In a similar way to (A24), from (A5), the mean of h^I in (A22) is

$$E[h^I] = \sum_{k=1}^N (-E[h_k^R] E[\sin(\pi \sin \Delta \varphi_k)] + E[h_k^I] E[\cos(\pi \sin \Delta \varphi_k)]) = 0 \quad (\text{A25})$$

From (A22), (A24) and (A25),

$$E[\tilde{h}] = E[h^R] + jE[h^I] + \frac{x^*}{\|x\|^2} E[n_b] = 0 \quad (\text{A26})$$

In a similar way to (A26),

$$E[\tilde{g}] = E[g^R] + jE[g^I] + \frac{x^*}{\|x\|^2} E[n_e] = 0 \quad (\text{A27})$$

From (A7), (A8), (A26) and (A27), the covariance of $\tilde{h}$ and $\tilde{g}$ can be given by

$$\begin{aligned}
\text{Cov}(\tilde{h}, \tilde{g}) &= E\left[\left(\tilde{h} - E[\tilde{h}]\right)\left(\tilde{g} - E[\tilde{g}]\right)^*\right] \\
&= E\left[\tilde{h}\tilde{g}^*\right] \\
&= E\left[\left((h^R + jh^I) + \frac{x^*}{\|x\|^2}n_b\right)\left((g^R - jg^I) + \frac{x}{\|x\|^2}n_e^*\right)\right] \\
&= E\left[\left((h^R + jh^I)(g^R - jg^I)\right) + (h^R + jh^I)\frac{x}{\|x\|^2}n_e^* + (g^R - jg^I)\frac{x^*}{\|x\|^2}n_b + \frac{1}{\|x\|^2}n_bn_e^*\right] \quad (\text{A28}) \\
&= E\left[(h^Rg^R + h^Ig^I) + j(-h^Rg^I + h^Rg^R) + \frac{x}{\|x\|^2}E[h^R + jh^I]E[n_e^*]\right. \\
&\quad \left.+ \frac{x^*}{\|x\|^2}E[g^R - jg^I]E[n_b] + \frac{1}{\|x\|^2}E[n_e^*]E[n_b]\right] \\
&= E[h^Rg^R + h^Ig^I] + jE[-h^Rg^I + h^Rg^R] \\
&= E[h^Rg^R] + E[h^Ig^I] + j(-E[h^Rg^I] + E[h^Ig^R])
\end{aligned}$$

From (A5) and (A6), the mean of h^Rg^R can be given by

$$E[h^Rg^R] = E\left[\left(\sum_{k=1}^N\left(h_k^R \cos(\pi \sin \Delta \varphi_k) + h_k^I \sin(\pi \sin \Delta \varphi_k)\right)\right)\left(\sum_{k=1}^N\left(g_k^R \cos(\pi \sin \Delta \theta_k) + g_k^I \sin(\pi \sin \Delta \theta_k)\right)\right)\right] \quad (\text{A29})$$

Since $\tilde{h}_i$ and $\tilde{g}_j$ are independent of each other when $i, j \in \{1, 2, \dots, N\}$ and $i \neq j$, so it can be obtained that

$$E[h_i^R \cos(\pi \sin \Delta \varphi_i) g_j^R \cos(\pi \sin \Delta \theta_j)] = E[h_i^R] E[\cos(\pi \sin \Delta \varphi_i) g_j^R \cos(\pi \sin \Delta \theta_j)] = 0 \quad (\text{A30})$$

where $i, j \in \{1, 2, \dots, N\}$ and $i \neq j$.

Obviously, remove the terms which equal to 0 in (A29), it can be obtained that

$$\begin{aligned}
E[h^Rg^R] &= E\left[\sum_{k=1}^N(h_k^R \cos(\pi \sin \Delta \varphi_k) g_k^R \cos(\pi \sin \Delta \theta_k) + h_k^R \cos(\pi \sin \Delta \varphi_k) g_k^I \sin(\pi \sin \Delta \theta_k)\right. \\
&\quad \left.+ h_k^I \sin(\pi \sin \Delta \varphi_k) g_k^R \cos(\pi \sin \Delta \theta_k) + h_k^I \sin(\pi \sin \Delta \varphi_k) g_k^I \sin(\pi \sin \Delta \theta_k))\right] \\
&= \sum_{k=1}^N(E[h_k^R g_k^R] E[\cos(\pi \sin \Delta \varphi_k)] E[\cos(\pi \sin \Delta \theta_k)] + E[h_k^R g_k^I] E[\cos(\pi \sin \Delta \varphi_k)] E[\sin(\pi \sin \Delta \theta_k)] \\
&\quad + E[h_k^I g_k^R] E[\sin(\pi \sin \Delta \varphi_k)] E[\cos(\pi \sin \Delta \theta_k)] + E[h_k^I g_k^I] E[\sin(\pi \sin \Delta \varphi_k)] E[\sin(\pi \sin \Delta \theta_k)]) \\
&= \sum_{k=1}^N(E[h_k^R g_k^R] \mu_c^2 + E[h_k^R g_k^I] \mu_c \mu_s + E[h_k^I g_k^R] \mu_s \mu_c + E[h_k^I g_k^I] \mu_s^2)
\end{aligned} \quad (\text{A31})$$

From (18),

$$\begin{aligned}
g_k &= (h_k^R + jh_k^I)[\cos(\pi \sin \theta_k) - j \sin(\pi \sin \theta_k)] \\
&= (h_k^R \cos(\pi \sin \theta_k) + h_k^I \sin(\pi \sin \theta_k)) + j[h_k^I \cos(\pi \sin \theta_k) - h_k^R \sin(\pi \sin \theta_k)] \\
&= g_k^R + jg_k^I
\end{aligned} \quad (\text{A32})$$

So,

$$\begin{aligned}
E[h_k^R g_k^R] &= E[h_k^R (h_k^R \cos(\pi \sin \theta_k) + h_k^I \sin(\pi \sin \theta_k))] \\
&= E\left[(h_k^R)^2 \cos(\pi \sin \theta_k) + h_k^R h_k^I \sin(\pi \sin \theta_k)\right] \\
&= E\left[(h_k^R)^2\right] E[\cos(\pi \sin \theta_k)] + E[h_k^R] E[h_k^I] E[\sin(\pi \sin \theta_k)] \\
&= \left[Var[h_k^R] + (E[h_k^R])^2\right] E[\cos(\pi \sin \theta_k)] \\
&= \frac{1}{2} \sigma_h^2 \mu_c
\end{aligned} \quad (\text{A33})$$

Form (A33), it can be obtained that

$$E[h_k^R g_k^R] \mu_c^2 = \frac{1}{2} \sigma_h^2 \mu_c^3 \quad (\text{A34})$$

In a similar way to (A34),

$$E[h_k^R g_k^I] \mu_c \mu_s = -\frac{1}{2} \sigma_h^2 \mu_c \mu_s^2 \quad (\text{A35})$$

$$E[h_k^I g_k^R] \mu_s \mu_c = \frac{1}{2} \sigma_h^2 \mu_c \mu_s^2 \quad (\text{A36})$$

$$E[h_k^I g_k^I] \mu_s^2 = \frac{1}{2} \sigma_h^2 \mu_c \mu_s^2 \quad (\text{A37})$$

From (A31), (A34)–(A37), it can be obtained that

$$\begin{aligned} E[h^R g^R] &= N \left(\frac{1}{2} \sigma_h^2 \mu_c^3 - \frac{1}{2} \sigma_h^2 \mu_c \mu_s^2 + \frac{1}{2} \sigma_h^2 \mu_c \mu_s^2 + \frac{1}{2} \sigma_h^2 \mu_c \mu_s^2 \right) \\ &= \frac{N}{2} \sigma_h^2 (\mu_c^3 + \mu_c \mu_s^2) \end{aligned} \quad (\text{A38})$$

In a similar way to (A38),

$$E[h^I g^I] = \frac{N}{2} \sigma_h^2 (\mu_c^3 + \mu_c \mu_s^2) \quad (\text{A39})$$

$$E[h^R g^I] = \frac{N}{2} \sigma_h^2 (-\mu_c^2 \mu_s - \mu_s^3) \quad (\text{A40})$$

$$E[h^I g^R] = \frac{N}{2} \sigma_h^2 (\mu_s^3 + \mu_c^2 \mu_s) \quad (\text{A41})$$

So, from (A28), (A38)–(A40), it can be obtained that

$$\begin{aligned} \text{Cov}(\tilde{h}, \tilde{g}) &= E[h^R g^R] + E[h^I g^I] + j(-E[h^R g^I] + E[h^I g^R]) \\ &= \frac{N}{2} \sigma_h^2 [(\mu_c^3 + \mu_c \mu_s^2) + (\mu_c^3 + \mu_c \mu_s^2)] + j \left[\frac{N}{2} \sigma_h^2 (-(-\mu_c^2 \mu_s - \mu_s^3) + (\mu_s^3 + \mu_c^2 \mu_s)) \right] \\ &= N \sigma_h^2 [(\mu_c^3 + \mu_c \mu_s^2) + j(\mu_s^3 + \mu_c^2 \mu_s)] \end{aligned} \quad (\text{A42})$$

From (A20), (A21) and (A42), the correlation coefficient between $\tilde{h}$ and $\tilde{g}$ can be given by

$$\begin{aligned} \rho(\tilde{h}, \tilde{g}) &= \frac{\text{Cov}(\tilde{h}, \tilde{g})}{\sqrt{\text{Var}[\tilde{h}] \sqrt{\text{Var}[\tilde{g}]}} \\ &= \frac{N \sigma_h^2 [(\mu_c^3 + \mu_c \mu_s^2) + j(\mu_s^3 + \mu_c^2 \mu_s)]}{\sqrt{N [\sigma_h^2 (\sigma_c^2 + \mu_c^2 + \sigma_s^2 + \mu_s^2)] + \frac{1}{\|x\|^2} \sigma_h^2} \sqrt{N [\sigma_g^2 (\sigma_c^2 + \mu_c^2 + \sigma_s^2 + \mu_s^2)] + \frac{1}{\|x\|^2} \sigma_g^2}} \end{aligned} \quad (\text{A43})$$

Appendix B

From (22), it can be obtained that

$$\begin{aligned} h' &= \sum_{k=1}^N (h_k^R + j h_k^I) \\ &= \sum_{k=1}^N h_k^R + j \sum_{k=1}^N h_k^I \\ &= h'^R + j h'^I \end{aligned} \quad (\text{A44})$$

The mean and variance of h' can be given by

$$E[h'] = E \left[\sum_{k=1}^N h_k^R \right] + j E \left[\sum_{k=1}^N h_k^I \right] = 0 \quad (\text{A45})$$

$$\begin{aligned} \text{Var}[h'] &= \text{Var} \left[\sum_{k=1}^N h_k^R \right] + \text{Var} \left[\sum_{k=1}^N h_k^I \right] \\ &= \frac{N}{2} \sigma_h^2 + \frac{N}{2} \sigma_h^2 \\ &= N \sigma_h^2 \end{aligned} \quad (\text{A46})$$

In a similar way to (A28), from (A7), (A26), (A43) and (A45), the covariance of $\tilde{h}$ and h' can

be given by

$$\begin{aligned}
 \text{Cov}(\tilde{h}, h') &= E\left[\left(\tilde{h} - E[\tilde{h}]\right)(h' - E[h'])^*\right] \\
 &= E\left[\tilde{h}h'^*\right] \\
 &= E\left[\left(h^R + jh^I\right) + \frac{x^*}{\|x\|^2}n_b\right]\left(h'^R - jh'^I\right) \\
 &= E\left[h^R h'^R\right] + E\left[h^I h'^I\right] + j\left(-E\left[h^R h'^I\right] + E\left[h^I h'^R\right]\right)
 \end{aligned} \tag{A47}$$

In a similar way to (A29) and (A33), from (A5) and (A44), it can be obtained that

$$\begin{aligned}
 E\left[h^R h'^R\right] &= E\left[\left(\sum_{k=1}^N \left(h_k^R \cos(\pi \sin \Delta \varphi_k) + h_k^I \sin(\pi \sin \Delta \varphi_k)\right)\right)\left(\sum_{k=1}^N h_k^R\right)\right] \\
 &= E\left[\sum_{k=1}^N \left(\left(h_k^R\right)^2 \cos(\pi \sin \Delta \varphi_k) + h_k^R h_k^I \sin(\pi \sin \Delta \varphi_k)\right)\right] \\
 &= \sum_{k=1}^N E\left[\left(h_k^R\right)^2\right] E[\cos(\pi \sin \Delta \varphi_k)] \\
 &= \frac{N}{2} \sigma_h^2 \mu_c
 \end{aligned} \tag{A48}$$

In a similar way to (A48),

$$E\left[h^I h'^I\right] = \sum_{k=1}^N E\left[\left(h_k^I\right)^2\right] E[\cos(\pi \sin \Delta \varphi_k)] = \frac{N}{2} \sigma_h^2 \mu_c \tag{A49}$$

$$E\left[h^R h'^I\right] = \sum_{k=1}^N E\left[\left(h_k^I\right)^2\right] E[\sin(\pi \sin \Delta \varphi_k)] = \frac{N}{2} \sigma_h^2 \mu_s \tag{A50}$$

$$E\left[h^I h'^R\right] = -\sum_{k=1}^N E\left[\left(h_k^R\right)^2\right] E[\sin(\pi \sin \Delta \varphi_k)] = -\frac{N}{2} \sigma_h^2 \mu_s \tag{A51}$$

From (A47)–(A51),

$$\begin{aligned}
 \text{Cov}(\tilde{h}, h') &= E\left[h^R h'^R\right] + E\left[h^I h'^I\right] + j\left(-E\left[h^R h'^I\right] + E\left[h^I h'^R\right]\right) \\
 &= \frac{N}{2} \sigma_h^2 \mu_c + \frac{N}{2} \sigma_h^2 \mu_c + j\left(-\frac{N}{2} \sigma_h^2 \mu_s - \frac{N}{2} \sigma_h^2 \mu_s\right) \\
 &= N \sigma_h^2 \mu_c - j(N \sigma_h^2 \mu_s)
 \end{aligned} \tag{A52}$$

From (A20), (A46) and (A52),

$$\begin{aligned}
 \rho(\tilde{h}, h') &= \frac{\text{Cov}(\tilde{h}, h')}{\sqrt{\text{Var}[\tilde{h}]}\sqrt{\text{Var}[h']}} \\
 &= \frac{N \sigma_h^2 (\mu_c - j \mu_s)}{\sqrt{N[\sigma_h^2 (\sigma_c^2 + \mu_c^2 + \sigma_s^2 + \mu_s^2)] + \frac{1}{\|x\|^2} \sigma_h^2} \sqrt{N \sigma_h^2}}
 \end{aligned} \tag{A53}$$

References

1. Qu, Z.; Zhang, G.; Cao, H.; Xie, J. LEO Satellite Constellation for Internet of Things. *IEEE Access* **2017**, *5*, 18391–18401. [\[CrossRef\]](#)
2. Liu, C.; Kirchengast, G.; Sun, Y.; Du, Q.; Bai, W.; Proschek, V.; Wang, X.; Xia, J.; Meng, X.; Wang, D.; et al. Study on LEO-LEO microwave occultation. In Proceedings of the 2017 IEEE International Geoscience and Remote Sensing Symposium (IGARSS), Fort Worth, TX, USA, 23–28 July 2017; pp. 538–541. [\[CrossRef\]](#)
3. Deng, R.; Di, B.; Zhang, H.; Song, L. Ultra-Dense LEO Satellite Constellation Design for Global Coverage in Terrestrial-Satellite Networks. In Proceedings of the GLOBECOM 2020—2020 IEEE Global Communications Conference, Taipei, China, 7–11 December 2020; pp. 1–6. [\[CrossRef\]](#)
4. Wu, C.; Sun, Y.; Wang, X.; Liu, C.; Du, Q.; Bai, W.; Wang, D.; Meng, X.; Cai, Y.; Liu, C.; et al. A Leo-Leo Occultation System Using Microwave Signals. In Proceedings of the IGARSS 2018—2018 IEEE International Geoscience and Remote Sensing Symposium, Valencia, Spain, 22–27 July 2018; pp. 3147–3148. [\[CrossRef\]](#)

5. Liang, H.; Chen, F.; Ji, X.; Lu, P.; Gao, Y. The development of world-earth integrated information network and the application of mimicry technology. *Sci. China Inf. Sci.* **2019**, *49*, 799–818.
6. Ji, X.; Tao, X.; Huang, K.; Wu, H. Introduction to the topic of B5G network security. *Sci. China Inf. Sci.* **2021**, *51*, 171–172.
7. Wang, Y.; Gu, L.; Liu, H. Status and future development of low-orbit satellite mobile communications. *Commun. Technol.* **2020**, *53*, 103–109.
8. Ji, X.; Liang, H.; Hu, H. Thoughts on the Security Protection Technology of World-Ground Integration Information Network. *Tele-Commun. Sci.* **2017**, *33*, 24–35.
9. Li, B.; Fei, Z.; Zhou, C.; Zhang, Y. Physical-Layer Security in Space Information Networks: A Survey. *IEEE Internet Things J.* **2019**, *7*, 33–52. [[CrossRef](#)]
10. Jin, L.; Hu, X.; Sun, X.; Lou, Y.; Huang, K.; Zhong, Z.; Xu, X. Native Security Scheme Based on Physical Layer Chain Key for Encryption and Authentication. In Proceedings of the 2021 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Nanjing, China, 29 March 2021; pp. 1–7. [[CrossRef](#)]
11. Jin, L.; Wang, X.; Lou, Y.; Xu, X. Achieving one-time pad via endogenous secret keys in wireless communication. In Proceedings of the 2020 IEEE/CIC International Conference on Communications in China (ICCC), Chongqing, China, 9–11 August 2020; pp. 1092–1097. [[CrossRef](#)]
12. Guo, K.; Zhang, B.; Huang, Y.; Guo, D. Secure performance analysis of satellite communication networks in Shadowed Rician Channel. In Proceedings of the 2016 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), Limassol, Cyprus, 12–14 December 2016; pp. 156–159. [[CrossRef](#)]
13. Gao, Y.; Ao, H.; Zhou, Q.; Feng, Z.; Zhou, W.; Li, Y.; Li, X. Modeling of satellite communication systems design with physical layer security. In Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 22–24 March 2017; pp. 1680–1683. [[CrossRef](#)]
14. Kalantari, A.; Zheng, G.; Gao, Z.; Han, Z.; Ottersten, B. Secrecy Analysis on Network Coding in Bidirectional Multibeam Satellite Communications. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1862–1874. [[CrossRef](#)]
15. Fu, Q.-Y.; Feng, Y.-H.; Wang, H.-M.; Liu, P. Initial Satellite Access Authentication Based on Doppler Frequency Shift. *IEEE Wirel. Commun. Lett.* **2020**, *10*, 498–502. [[CrossRef](#)]
16. Jin, L.; Lou, Y.; Xu, X.; Zhong, Z.; Wang, H. Separating Multi-Stream Signals Based on Space-Time Isomerism. In Proceedings of the 2020 International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, China, 21–23 October 2020; pp. 418–423. [[CrossRef](#)]
17. Nie, X.; Mi, H.; Wu, X. Research on satellite-to-ground channel performance based on integrated channel model. *Spacecr. Eng.* **2012**, *21*, 48–52. [[CrossRef](#)]
18. Huang, K.; Jin, L.; Chen, Y.; Lou, Y.; Zhou, Y.; Ma, K.; Xu, X.; Zhong, Z.; Zhang, S. Development and new challenges of wireless physical layer key generation technology. *J. Electron. Inf.* **2020**, *42*, 2330–2341.
19. Li, X.; Jin, L.; Zhong, Z.; Lou, Y. A Physical-Layer Message Encryption and Authentication Scheme. In Proceedings of the 2018 IEEE 4th International Conference on Computer and Communications (ICCC), Chengdu, China, 7–10 December 2018; pp. 1893–1898. [[CrossRef](#)]
20. Jin, L.; Cai, A.; Huang, K.; Zhong, Z.; Lou, Y. Key generation scheme based on multiple random signal streams. *J. Electron. Inf. Technol.* **2019**, *41*, 1405–1412.
21. Wang, H.-M.; Bai, J.; Dong, L. Intelligent Reflecting Surfaces Assisted Secure Transmission without Eavesdropper's CSI. *IEEE Signal Process. Lett.* **2020**, *27*, 1300–1304. [[CrossRef](#)]
22. Li, Z.; Wang, S.; Mu, P.; Wu, Y.-C. Sum Rate Maximization of Secure NOMA Transmission with Imperfect CSI. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6. [[CrossRef](#)]
23. Wang, H.-M.; Jiang, J.-C.; Wang, Y.-N. Model Refinement Learning and an Example on Channel Estimation with Universal Noise Model. *IEEE J. Sel. Areas Commun.* **2020**, *39*, 31–46. [[CrossRef](#)]
24. Zhan, F.; Yao, N.; Gao, Z.; Yu, H. Efficient key generation leveraging wireless channel reciprocity for MANETs. *J. Netw. Comput. Appl.* **2018**, *104*, 18–28. [[CrossRef](#)]
25. Bennett, C.H.; Brassard, G.; Crepeau, C.; Maurer, U.M. Generalized privacy amplification. *IEEE Trans. Inf. Theory* **1995**, *41*, 1915–1923. [[CrossRef](#)]
26. Yan, S.; Li, Q. Optimizing Array Signal Processing (Volumes 1 and 2). *Acta Acoust.* **2018**, *43*, 728.
27. Hu, X. Research on Physical Layer Key Generation Technology under the Conditions of Eavesdropping Channel. Master's Thesis, Information Engineering University, Zhengzhou, China, 2018.
28. Jin, H.; Huang, K.; Jin, L.; Zhong, Z.; Chen, Y. Physical-Layer Secret Key Generation with Correlated Eavesdropping Channel. In Proceedings of the 2018 IEEE 4th International Conference on Computer and Communications (ICCC), Chengdu, China, 7–10 December 2018; pp. 226–231. [[CrossRef](#)]
29. Zhang, J.; Marshall, A.; Woods, R.; Duong, T.Q. Secure key generation from OFDM subcarriers' channel responses. In Proceedings of the 2014 IEEE Globecom Workshops (GC Wkshps), Austin, TX, USA, 8–12 December 2014; pp. 1302–1307. [[CrossRef](#)]
30. Bassham, L.; Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Leigh, S.; Levenson, M.; Vangel, M.; Heckert, N.; Banks, D. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications; Special Publication (NIST SP); National Institute of Standards and Technology; Gaithersburg, MD, USA. 2010. Available online: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762 (accessed on 4 December 2021).

-
31. Xiao, S.; Guo, Y.; Huang, K.; Jin, L. Cooperative Group Secret Key Generation Based on Secure Network Coding. *IEEE Commun. Lett.* **2018**, *22*, 1466–1469. [[CrossRef](#)]
 32. Xu, Q.; Ren, P. Channel-Aware Key Generation under Wireless Fading Environment. *IEEE Commun. Lett.* **2020**, *24*, 1636–1640. [[CrossRef](#)]
 33. Hu, X.; Jin, L.; Huang, K.; Sun, X.; Zhou, Y. Secret Key Generation Assisted by Intelligent Reflecting Surface with Discrete Phase Shift in Static Environment. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 1867–1870. [[CrossRef](#)]