Aerial Bridge: A Secure Tunnel Against Eavesdropping in Terrestrial-Satellite Networks

Qubeijian Wang, *Member, IEEE*, Hao Wang, Wen Sun, *Senior Member, IEEE*, Nan Zhao, *Senior Member, IEEE*, Hong-Ning Dai, *Senior Member, IEEE*, and Wei Zhang, *Fellow, IEEE*

***Abstract*— Terrestrial-satellite networks (TSNs) can provide worldwide users with ubiquitous and seamless network services. Meanwhile, malicious eavesdropping is posing tremendous challenges on secure transmissions of TSNs due to their widescale wireless coverage. In this paper, we propose an aerial bridge scheme to establish secure tunnels for legitimate transmissions in TSNs. With the assistance of unmanned aerial vehicles (UAVs), massive transmission links in TSNs can be secured without impacts on legitimate communications. Owing to the stereo position of UAVs and the directivity of directional antennas, the constructed secure tunnel can significantly relieve confidential information leakage, resulting in the precaution of wiretapping. Moreover, we establish a theoretical model to evaluate the effectiveness of the aerial bridge scheme compared with the ground relay, non-protection, and UAV jammer schemes. Furthermore, we conduct extensive simulations to verify the accuracy of theoretical analysis and present useful insights into the practical deployment by revealing the relationship between the performance and other parameters, such as the antenna beamwidth, flight height and density of UAVs.**

***Index Terms*— Eavesdropping probability, legitimate connectivity, stochastic geometry, terrestrial-satellite network (TSNs), unmanned aerial vehicles (UAVs).**

Manuscript received 24 January 2022; revised 3 September 2022 and 11 January 2023; accepted 13 March 2023. Date of publication 23 March 2023; date of current version 13 November 2023. This work was supported in part by the Shanghai Sailing Program under Grant 21YF1451100, in part by the Natural Science Basic Research Program of Shaanxi under Grant 2022JQ-625, in part by the Fundamental Research Funds for the Central Universities under Grant D5000210591, in part by the National Natural Science Foundation of China under Grant 62272391 and Grant 62271099, and in part by the Key Industry Innovation Chain of Shaanxi under Grant 2021ZDLGY05-08. The associate editor coordinating the review of this article and approving it for publication was P. Li. *(Corresponding author: Wen Sun.)*

Qubeijian Wang is with the School of Cybersecurity, Northwestern Polytechnical University, Xi'an 710072, China, and also with the Collaborative Innovation Center, Northwestern Polytechnical University, Shanghai 215400, China (e-mail: qubeijian.wang@nwpu.edu.cn).

Hao Wang and Wen Sun are with the School of Cybersecurity, Northwestern Polytechnical University, Xi'an 710072, China (e-mail: wanghao_@mail.nwpu.edu.cn; sunwen@nwpu.edu.cn).

Nan Zhao is with the School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, China (e-mail: zhaonan@dlut.edu.cn).

Hong-Ning Dai is with the Department of Computer Science, Hong Kong Baptist University, Hong Kong (e-mail: hndai@ieee.org).

Wei Zhang is with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW 2052, Australia (e-mail: w.zhang@unsw.edu.au).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TWC.2023.3258599.

Digital Object Identifier 10.1109/TWC.2023.3258599

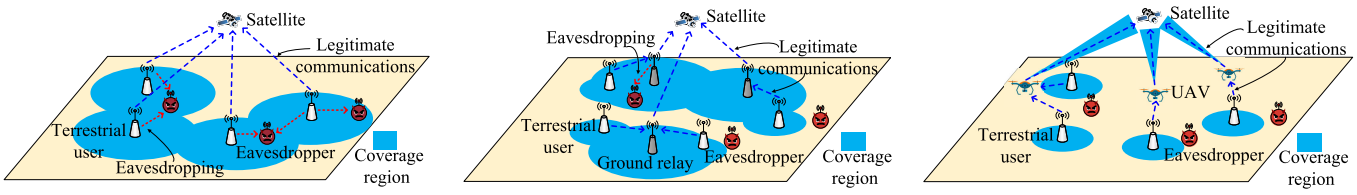
I. Introduction

As an emerging enabler, terrestrial-satellite networks (TSNs), are prospective to assist 6G wireless networks in constructing comprehensive and seamless network services. TSNs can effectively complement traditional wireless services in remote or rural areas. Owing to their ubiquitous service footprint and robust multi-link transmission, TSNs can provide flexible access, high-speed and wide-coverage connectivity to worldwide terminals, in fields including intelligent transportation, remote area monitoring, disaster rescue and tactical surveillance [1].

In fact, TSNs face a vital menace in information leakage, resulting in serious adversary wiretapping. Both the openness and the broadcasting nature of wireless channels in TSNs may cause confidential information leakage to eavesdroppers. Meanwhile, radio signals in TSNs are emitted by an extremely large transmit power to resist high attenuation caused by a long transmission distance and masking effect [2]. By contrast, the increase of transmit power obliges TSNs to face a tremendous surge in eavesdropping risks [3], [4]. Taking Fig. 1(a) as an example, all the eavesdroppers fall into the coverage regions of terrestrial users, where the coverage region (in blue shade) refers to the transmission region of a terrestrial user who directly transmits information to the satellite. Consequently, eavesdroppers can easily wiretap confidential information. However, traditional cryptographic encryption schemes cannot be fully adopted for TSNs due to inherent limitations and vulnerabilities. First, there are unpredictable difficulties in secret key distribution and management for TSNs [5]. Second, encryption typically has an explicit computational capability requirement, which may nevertheless be satisfied by resource-constrained devices like the Internet of Things (IoT) devices. In TSNs, the prevalent encryption, such as Advanced Encryption Standard (AES), usually assumes that the computational capability of adversaries is restricted, i.e., less than that of legitimate nodes [6], [7] while it cannot be ruled out that the encrypted information can be decoded by practical adversaries who may have sufficient computing capability.

A. Related Work and Motivation

As a complement to cryptographic encryption, physical layer security (PLS) has been proposed to provide TSNs



(a) Direct link in TSNs. (b) Ground relay scheme. (c) Aerial bridge scheme.

Fig. 1. Aerial bridge scheme versus direct link in TSNs and the ground relay scheme.

with promising security solutions. Generally, PLS can protect confidential information without a strong constraint on computational capability of devices [8]. The popular PLS methods in TSNs are cataloged as beamforming and friendly jamming schemes. In [9], secure TSNs were first realized with consideration of beamforming, in which a joint beamforming scheme was proposed to minimize the transmit power under the required secrecy rate constraints. Moreover, Lin et al. introduced robust secure beamforming to serve multi-beam satellite communications [10]. However, for unknown eavesdroppers, obtaining the accurate channel state information (CSI) is still a challenge. The presence of unknown eavesdroppers still poses challenges on the network security. By contrast, friendly jamming does not need to know the CSI of the eavesdropping channel. In [11], [12], and [13], they considered friendly jamming methods, in which jamming signals emitted by multiple antennas of the transmitter are utilized to prevent wiretapping. In fact, the impact of jamming signals on legitimate communications can be relieved, only if the jamming signals are known to the legitimate receiver. Thus, sharing pseudo-random sequences and establishing secure wired links are chosen to cancel the jamming signals received by legitimate users. Friendly jamming may be inappropriate for TSNs, since a satellite usually serves massive terrestrial users [9] and it will be quite expensive to deploy many satellites as jammers. Moreover, the effective jamming-cancellation is also difficult to be deployed.

Recently, a relay network has drawn an increasing attention, due to its merits on the coverage extension for TSNs. Meanwhile, some studies also focused on the relay-based PLS to improve the security of TSNs. In [14], Bankey and Upadhyay investigated the secrecy performance of a multi-relay hybrid satellite-terrestrial relay network with multiple eavesdroppers, and the relay selection was optimized to minimize the secrecy outage probability. Yan et al. [15] proposed an interference relay model to decrease the eavesdropping risk. Moreover, Guo et al. [16] introduced a relay selection scheme to enhance the quality of legitimate transmission in TSNs. The aforementioned studies only considered static relays (i.e., ground relays), which nevertheless limit the network flexibility and extensibility. As illustrated in Fig. 1(b), the introduction of ground relays can avoid some eavesdropping activities (at some specific regions) in contrast to the non-relay scheme as shown in Fig. 1(a). However, this decrement is not significant since the introduction of ground relays also increases the area of the coverage regions, consequently increasing the eavesdropping risks.

As an emerging technology, UAVs play roles of assistance to support traditional terrestrial networks. With the growing number of deployed UAVs, they have been increasingly introduced in TSNs to enhance the security and reliability of transmissions. For example, Li et al. [17] studied an artificial noise-aided method where UAV relays generated artificial noise to disturb a single eavesdropper around a legitimate user. Yin et al. [18] investigated a jamming relay scheme where UAVs act as relays to participate in legitimate transmissions while confusing the eavesdropper by sending jamming signals. Similarly, Pang et al. proposed a cooperative jamming scheme, when a UAV relay connected with the destination through a legitimate link, another UAV can work as a jammer to disturb the eavesdropping through jamming signals [19]. In [20], Liao et al. considered a UAV cooperative communication scheme to resist both eavesdropping and jamming attacks, where an incentive mechanism is designed to encourage UAVs to defend an illegal node with the perfect CSI jointly. Accordingly, most of the existing studies have the following restrictions: 1) The network security is improved at the expense of degrading legitimate data transmission. When deploying artificial noises or jamming signals to destroy the wiretapping link of the eavesdropper, these signals cannot avoid the impacts on the quality of legitimate data transmissions, since it is difficult to obtain the accurate CSI of secret eavesdroppers. 2) Effective protection is only suitable for an individual transmission. In TSNs, a satellite usually serves numerous users, and the individual transmission protection is unsuitable and ineffective for practical TSNs.

B. Contribution

To fill the above gaps, in this paper, we present an aerial bridge scheme for TSNs with the help of multiple UAVs, to provide secure communication service for massive terrestrial users. In our scheme, the confidential information is transmitted through a UAV *bridge* to the satellite rather than being directly transmitted to the satellite so as to weaken the eavesdropping risks. Considering Fig. 1(c) as an example, eavesdroppers can barely wiretap confidential information when we properly configure the stereo position of UAVs and the directivity of directional antennas. Comparing with the direct link in TSNs and the ground relay scheme (as shown in Fig. 1(a) and Fig. 1(b), respectively), our aerial bridge scheme can significantly reduce the eavesdropping risk (i.e., the decreased coverage region). In particular, our proposed aerial bridge scheme has the following merits: 1) it can significantly

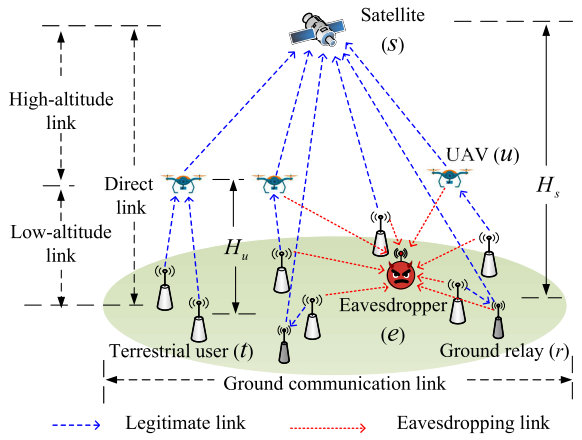


Fig. 2. Aerial bridge-assisted TSNs.

reduce the eavesdropping risk, resulting in the reduced information leakage; 2) it can improve the legitimate connectivity by reducing the interference from other terrestrial users; 3) the aerial bridges can be flexibly deployed in TSNs to serve for terrestrial users; 4) the deployment number of aerial bridges can be dynamically adjusted according to the requirement of terrestrial users, thereby reducing construction costs. Based on the theoretical analysis and extensive simulations, we further verify the effectiveness of the proposed scheme. The major contributions of this work can be summarized as follows:

- Firstly, we propose an aerial bridge scheme to secure the massive data transmissions in TSNs with the presence of eavesdroppers. Multiple UAVs serving as bridges assist the legitimate transmissions between terrestrial users and the satellite to degrade the eavesdropping risk.
- We establish a theoretical model to analyze the eavesdropping probability and the link connectivity, thereby measuring the legitimate transmissions and eavesdropping risks in wiretapped TSNs. In particular, we derive the closed-form expressions of both metrics.
- To evaluate the performance of the aerial bridge scheme, we compare it with the ground relay scheme, non-protection scheme, and UAV jammer scheme. Extensive simulation results validate the accuracy of our theoretical model. Meanwhile the simulation results also reveal that our scheme outperforms the others. Furthermore, we investigate the performance of our scheme under different parameter settings.

The remainder of this paper is organized as follows. Section II presents the system model of the proposed scheme. Section III and Section IV analyze the eavesdropping probability and the link connectivity, respectively. In Section V, we present simulation results. Finally, we conclude the work in Section VI.

II. System Model

A. Network Model

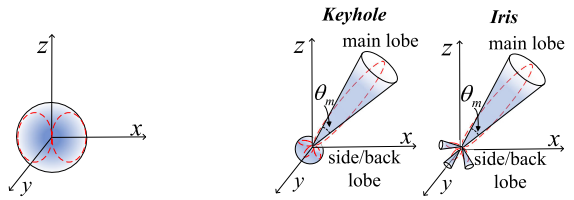
In this paper, we mainly consider a wiretapped TSN model, as depicted in Fig. 2, where multiple terrestrial users (denoted by t) transmit confidential information through legitimate links to a satellite (denoted by s), in the presence of eavesdroppers (denoted by e). We denote the deployment height of the satellite as H_s. To make the distribution of terrestrial users traceable in theoretic analysis, we assume that terrestrial users are randomly distributed on the ground according to the homogeneous Poisson point process (HPPP) with density λ_t [21]. It is worth mentioning that the location of each user is independent, so that, such distribution is deemed as a close-to-accuracy model to describe the practical locations of users [22]. Especially for TSNs, the different distance among the terrestrial users caused by diverse distributions, e.g., PPP and Poisson cluster process (PCP), is much smaller than the communication distance between the terrestrial user and the satellite [23]. Herein, we adopt HPPP as the user distribution model for theoretical analysis.

To prevent wiretapping from passive eavesdroppers in TSNs, we propose an aerial bridge scheme, as shown in Fig. 2. Multiple UAVs (denoted by u) are uniformly deployed on the aerial platform with height H_u, serving as aerial bridges between terrestrial users and the satellite. Specifically, the legitimate terrestrial user can transmit confidential information to a UAV with relatively low power, thereby reducing the information leakage risks at the terrestrial user. Then, the UAV bridge forwards the received signal to the satellite by a directional antenna towards the satellite. Thanks to the directivity of directional antennas introduced in Section II-C, the information leakage can be significantly reduced in the direction towards eavesdroppers. Herein, we model the distribution of UAVs according to the 3D-HPPP with density λ_u. The serving height of UAVs H_u is uniformly distributed in the space enclosed by the minimum UAV height $H_{u,\min}$ and the maximum UAV height $H_{u,\max}$.

For comparison purposes, in this paper, we introduce a ground relay scheme, where relays (denoted by r) are placed on the ground. Like the secure transmission process of the aerial bridge scheme, confidential information is transmitted from the target user to the satellite with the assistance of the closest ground relay. Similarly, we also choose HPPP with density λ_r to represent the distribution of ground relays for performance comparison.

B. Threat Model

In TSNs, passive eavesdroppers are randomly distributed among terrestrial users. Each eavesdropper independently wiretaps confidential information from possible terrestrial users and UAVs in the aerial bridge scheme. Specifically, eavesdroppers are deployed with the omni-directional antenna to acquire potential confidential information from all directions. When eavesdroppers appear within the communication range of any legitimate node (i.e., terrestrial users and UAVs), an eavesdropping link can be established with that node, then successfully receiving and decoding the target signals. It is worth mentioning that both CSI and the precise locations of the eavesdroppers are always unknown to legitimate users.



(a) Omni-directional antenna. (b) Directional antenna.

Fig. 3. Antenna models.

In this case, eavesdropping activities are hard to be detected and defend, since eavesdroppers are perfectly hidden.

C. Antenna Model

In the considered scenario, there are two types of antennas, i.e., omni-directional antennas and directional antennas. Omni-directional antennas are deployed at all ground nodes to transmit/receive signals uniformly in all directions. Hence, ground nodes can conquer the coverage deficiency in horizontal and vertical planes [24], to achieve maximum coverage. Likewise, for eavesdroppers, omni-directional antennas can make them to wiretap confidential information from legitimate users in all directions. On the contrary, UAVs and satellites are equipped with directional antennas to intensively transmit/receive signals in the desired direction. Since UAVs and satellites are all deployed in the air, signals usually need to transmit towards a specific direction, i.e., the target node on the ground. Moreover, these signals suffer from a large path loss caused by the long transmission distance. Adopting directional antennas can ensure a high transmission quality for communications of UAVs and satellites [25]. As shown in Fig. 3, the radiation of the realistic antenna model varies in diverse directions (i.e., red dotted line), so that, it is not tractable in the theoretic analysis, especially for directional antennas [26], [27]. In this context, we adopt the approximated antenna models [28]. We then introduce the antenna gain to further measure the directivity of an antenna.

1) Omni-Directional Antenna: As shown in Fig. 3(a), the realistic radiation model of the omni-directional antenna varies with directions. Referring to 3GPP, the antenna has the normalized gain in both horizontal and vertical directions, while the gain for all horizontal directions are equal to 1 [29]. Hence, the antenna gain of the omni-directional antenna G^o for realistic model can be expressed as $G^o = 10^{\left(-1.2\phi_o^2/\phi_{3\text{dB}}^2\right)}$, where $\phi_o \in [0, \pi/2]$ is the elevation angle of the antenna element, $\phi_{3\text{dB}} = 65^\circ$ is 3dB antenna beamwidth. Furthermore, we also adopt the isotropic antenna model (i.e., blue radiation in Fig. 3(a)) which radiates equal radio power in all directions to track reasonable analysis. In this model, the antenna gain of an omni-directional antenna is denoted by G^o, where $G^o = 1$.

2) Directional Antenna: A realistic directional antenna is usually composed of one main lobe and several side/back lobes, i.e., red dotted line in Fig. 3(b), which can transmit the signals in multiple specific directions with different antenna gains. Nevertheless, it also makes the theoretical analysis more complicated. In this paper, we adopt the keyhole model and iris model, i.e., blue radiation and yellow radiation, respectively, in Fig. 3(b). The keyhole model is composed of one main lobe with beamwidth θ_m and a joint side/back lobe with beamwidth $2\pi - \theta_m$ [30]. Then, the antenna gains of the main lobe and the joint side/back lobe are denoted by G^m and G^b, respectively, with the following relationship

$$G^m = \frac{2 - G^b\left(1 + \cos\frac{\theta_m}{2}\right)}{1 - \cos\frac{\theta_m}{2}}. \tag{1}$$

To precisely track the radiation pattern of realistic directional antennas, we also adopt the iris model which consists of a single main lobe with beamwidth θ_m and several side/back lobes with beamwidth θ_b. Note that, for simplicity, we assume that $\theta_m = \theta_b$. Then, the antenna gain of the main lobe and the side/back lobes can be given by the following expressions [31], [32], respectively,

$$\begin{cases} G^m = \dfrac{3}{\theta_m^2}, \\ G^b = \dfrac{1 - \frac{3}{2\pi\theta_m}\sin\left(\frac{\theta_m}{2}\right)}{1 - \frac{\theta_m}{2\pi}\sin\left(\frac{\theta_m}{2}\right)}. \end{cases} \tag{2}$$

The main lobe and N side/back lobes of the antenna are uniformly distributed in the space. Herein, the solid angle between any two neighbor lobes denoted by ψ can be calculated by $\psi = 4\pi/(N+1) - 2\pi\left(1 - \cos\left(\theta_m/2\right)\right)$.

D. Channel Model

In this paper, we summarize four channel models as shown in Fig. 2, including the ground communication link, low-altitude link, high-altitude link and direct link, which are introduced as follows.

1) Ground Link/Low-Altitude Link: The transmission links among ground nodes (i.e., eavesdroppers, terrestrial users and relays) are modeled as ground links. Particularly, ground links are denoted by $\mathrm{g} = \{te, tr, re\}$, where te, tr and re represent the links from a terrestrial user to an eavesdropper, from a terrestrial user to a ground relay and from a ground relay to an eavesdropper, respectively. Moreover, we define the transmission links between a terrestrial user or an eavesdropper and a UAV as low-altitude links, which are denoted by $\mathrm{l} = \{tu, ue\}$. Because both ground links and low-altitude links mainly suffer from multi-path effect and large-scale path-loss effect, we assume that they experience path loss and Rayleigh fading [33]. Then, the received power of ground links or low-attitude links can be expressed as

$$R_{\mathrm{g,l}} = P_{\mathrm{g,l}} G_{\{t,r,u\}} G_{\{e,r,u\}} h_{\mathrm{g,l}} {l_{\mathrm{g,l}}}^{-\alpha_{\mathrm{g,l}}}, \tag{3}$$

where $P_{\mathrm{g,l}}$ is the transmit power of ground links or low-attitude links, $G_{\{t,r,u\}}$ is the transmitted antenna gain, and $G_{\{e,r,u\}}$ is the received antenna gain. Since all ground nodes are equipped with omni-directional antennas, we have $G_{\{t,r\}} = G_{\{e,r\}} = 1$. For UAVs, the antenna gain G_u in the low-altitude link can be expressed as G_u^m (received/transmitted by the main lobe) and G_u^b (received/transmitted by the side/back lobe). The straight-line transmission distance between two target nodes is denoted by $l_{\mathrm{g,l}}$, $h_{\mathrm{g,l}}$ is the channel coefficient following an exponential distribution with mean $1/\mu_{\mathrm{g,l}}$, and $\alpha_{\mathrm{g,l}}$ is the path loss factor.

2) High-Altitude Link: The transmission link from a UAV to the satellite is defined as a high-altitude link. Since it is barely to be affected by obstacles, the high-altitude link has a limited multi-path effect. Therefore, the signal experiences unbound path loss in the high-altitude link [34]. Then, the received power at the satellite can be given as

$$R_{us} = P_{us} G_u G_s l_{us}^{-\alpha_{us}}, \tag{4}$$

where P_{us} is the transmit power of UAVs, G_u is the transmitted antenna gain of UAVs, and G_s is the received antenna gain of the satellite. Moreover, l_{us} denotes the distance between the UAV and the satellite, and α_{us} is the path loss factor.

3) Direct Link: We depict the transmission link between a legitimate ground node (i.e., a terrestrial user or a ground relay) and the satellite as a direct link, which is subject to shadowing and obstacles. As a widely used model in TSNs, the Shadowed-Rician fading model can represent a realistic channel by adjusting the fading parameters. Thus, we use the independent and identically distributed (i.i.d) Shadowed-Rician fading to depict the channel of the direct link [35]. In this paper, direct links are denoted by $\mathrm{d} = \{ts, rs\}$, where ts and rs represent the links from a terrestrial user or a ground relay to the satellite, respectively. Therefore, the received power at the satellite can be expressed as

$$R_{\mathrm{d}} = P_{\mathrm{d}} G_{\{t,r\}} G_s h_{\mathrm{d}} l_{\mathrm{d}}^{-\alpha_{\mathrm{d}}}, \tag{5}$$

where l_{d} is the distance of the direct link, and α_{d} is the path loss factor. In addition, h_{d} is the channel coefficient. Since the fading severity parameter m is an arbitrary integer with the range of $[0, \infty)$, the probability density function (PDF) of h_{d} is given by [36]

$$f_{h_{\mathrm{d}}}(x) = \frac{1}{2\rho}\left(\frac{2\rho m}{2\rho m + \Omega}\right)^m \exp\left(-\frac{x}{2\rho}\right) {}_1\mathrm{F}_1 \times \left(m, 1, \frac{\Omega x}{2\rho\left(2\rho m + \Omega\right)}\right), \tag{6}$$

where Ω and 2ρ denote the average powers of the line-of-sight (LOS) and multipath components, respectively. It is worth noting that when the fading severity parameter $m = \infty$, the envelope of h_{d} follows the Rician distribution. Moreover, ${}_1\mathrm{F}_1(\mathfrak{a}, \mathfrak{b}, \mathfrak{c})$ is a confluent hypergeometric function, which can be further rewritten as [37] and [38]

$${}_1\mathrm{F}_1\left(m, 1, \frac{\Omega x}{2\rho\left(2\rho m + \Omega\right)}\right) = \sum_{n=0}^{m-1} \frac{(1-m)_n}{(n!)^2}\left(-\frac{\Omega x}{2\rho\left(2\rho m + \Omega\right)}\right)^n \times \exp\left(\frac{\Omega x}{2\rho\left(2\rho m + \Omega\right)}\right). \tag{7}$$

III. Eavesdropping Probability Analysis

In this section, we aim at investigating the eavesdropping risks of TSNs under the aerial bridge scheme, the ground relay scheme and the direct link. Since eavesdroppers are secret, they may appear at any locations to wiretap confidential information from legitimate nodes in TSNs. Hence, we need to accurately evaluate the eavesdropping risks from any eavesdroppers in TSNs. Herein, we exploit the eavesdropping probability as a metric, which is defined as follows.

Definition 1: Eavesdropping probability is the probability that the confidential information from no less than one legitimate user is successfully wiretapped by the eavesdropper.

In fact, if there is one user in TSNs can be wiretapped by the eavesdropper, the network security will be challenged. Hence, the eavesdropping probability given in Definition 1 can accurately evaluate the eavesdropping risks in TSNs. Next, we analyze the eavesdropping probability of the aerial bridge scheme in Section III-A and the eavesdropping probability of the ground relay scheme and the direct link in TSNs in Section III-B.

A. Eavesdropping Probability of Aerial Bridge Scheme

We present the eavesdropping probability of the aerial bridge scheme in this subsection. For the aerial bridge scheme, the data transmission is processed in two steps through the low-attitude link (i.e., the link from the terrestrial user to the UAV bridge) and the high-attitude link (i.e., the link from the UAV bridge to the satellite). Unfortunately, confidential information is possibly leaked in both links. To evaluate the eavesdropping risks for the aerial bridge scheme, we should comprehensively consider the eavesdropping probability of both eavesdropping links. Firstly, we derive the eavesdropping probability of a ground eavesdropping link denoted by $\mathcal{P}_{\mathrm{k}}$. The expression is present in Lemma 1 as follows.

Lemma 1: The eavesdropping probability of a ground eavesdropping link $\mathcal{P}_{\mathrm{k}}$ can be expressed as

$$\mathcal{P}_{\mathrm{k}} = \int_0^{\left(\frac{P_{\mathrm{k}} h_{\mathrm{k}} G_e G_{\{t,r\}}}{\eta_e}\right)^{\frac{1}{\alpha_{\mathrm{k}}}}} l_{\mathrm{k}} \exp\left(-\lambda_{\{t,r\}} \pi {l_{\mathrm{k}}}^2 - \mu_{\mathrm{k}} \gamma_e {l_{\mathrm{k}}}^{\alpha_{\mathrm{k}}} \sigma^2\right) \mathbf{d} l_{\mathrm{k}} \times 2\pi\lambda_{\{t,r\}} \exp\left(-2\pi\lambda_{\{t,r\}} \int_0^{l_{\max}} \frac{\gamma_e}{1+\gamma_e} l_{\mathrm{k}} \mathrm{d} l_{\mathrm{k}}\right), \tag{8}$$

where $\mathrm{k} = \{te, re\}$ denote the ground eavesdropping links, γ_e is signal-to-interference-plus-noise ratio (SINR) threshold at the eavesdropper, $\lambda_{\{t,r\}}$ is the density of legitimate ground transmitters, and σ^2 is Gaussian white noise. The straight-line distance from a legitimate ground transmitter to the eavesdropper is represented by l_{k}.

Proof: Considering the component sensitivity of the antenna, the signal cannot be availably received when its power is extremely low. We specify the threshold of received power at the eavesdropper as η_e. Thus, the maximum eavesdropping range for ground eavesdropping links denoted by $l_{\max}$ can be calculated as

$$l_{\max} = \left(\frac{P_{\mathrm{k}} h_{\mathrm{k}} G_e G_{\{t,r\}}}{\eta_e}\right)^{\frac{1}{\alpha_{\mathrm{k}}}}. \tag{9}$$

The legitimate users or ground relay are horizontal to the eavesdroppers, thus, the elevation angle ϕ_o at both transmitter and receiver are equal to 0, resulting in $G_e = G_{\{t,r\}} = 1$. Note that only when the legitimate users appear at the region within the maximum eavesdropping range $l_{\max}$, the eavesdropper can acquire the legitimate signal. Referring to [39], the cumulative distribution function (CDF) of the distance between the

eavesdropper and the legitimate node $l_{\rm k}$ can be expressed as

$$F_{l_{\rm k}}(l_{\max}) = \mathbb{P}\left[l_{\rm k} \le l_{\max}\right] = 1 - \exp\left(-\lambda_{\{t,r\}}\pi l_{\max}^2\right). \quad (10)$$

Then, we can derive the PDF of $l_{\rm k}$ as

$$f_{l_{\rm k}}(x) = \frac{\mathbf{d}F_{l_{\rm k}}(x)}{\mathbf{d}x} = 2\pi\lambda_{\{t,r\}} x \exp\left(-\lambda_{\{t,r\}}\pi x^2\right). \quad (11)$$

An eavesdropper can successfully decode the confidential information from a legitimate node only if its received SINR is larger than the threshold γ_e. To evaluate the eavesdropping risks for the whole legitimate ground transmitters in TSNs, the eavesdropping probability $\mathcal{P}_{\rm k}$ can be expressed as [40]

$$\mathcal{P}_{\rm k} = \mathbb{E}\left[\mathbb{P}\left[\frac{P_{\rm k}G_eG_{\{t,r\}}h_{\rm k}l_{\rm k}^{-\alpha_{\rm k}}}{I_{\rm k}+\sigma^2} > \gamma_e \mid l_{\rm k}\right]\right], \quad (12)$$

where $I_{\rm k}$ denotes the interference from other users, $\mathbb{E}[\cdot]$ represents the expected value. Then, (12) can be further derived as

$$\begin{aligned}
\mathcal{P}_{\rm k} &= \int_0^{l_{\max}} \mathbb{P}\left[\frac{P_{\rm k}G_eG_{\{t,r\}}h_{\rm k}l_{\rm k}^{-\alpha_{\rm k}}}{I_{\rm k}+\sigma^2} > \gamma_e \mid l_{\rm k}\right] f_{l_{\rm k}}(l_{\rm k})\mathbf{d}l_{\rm k} \\
&= \int_0^{l_{\max}} \mathbb{P}\left[h_{\rm k} > \frac{\gamma_e {l_{\rm k}}^{\alpha_{\rm k}}}{P_{\rm k}G_eG_{\{t,r\}}}\left(I_{\rm k}+\sigma^2\right) \mid l_{\rm k}\right] f_{l_{\rm k}}(l_{\rm k})\mathbf{d}l_{\rm k} \\
&= \int_0^{l_{\max}} \mathbb{E}_{I_{\rm k}}\left[\exp\left(-\frac{\mu_{\rm k}\gamma_e {l_{\rm k}}^{\alpha_{\rm k}}}{P_{\rm k}G_eG_{\{t,r\}}}\left(I_{\rm k}+\sigma^2\right)\right) \mid l_{\rm k}\right] f_{l_{\rm k}}(l_{\rm k})\mathbf{d}l_{\rm k} \\
&= \int_0^{l_{\max}} \exp\left(-\mu_{\rm k}\gamma_e l_{\rm k}^{\alpha_{\rm k}}\sigma^2\right)\mathcal{L}_{I_{\rm k}}\left(\frac{\mu_{\rm k}\gamma_e l_{\rm k}^{\alpha_{\rm k}}}{P_{\rm k}G_eG_{\{t,r\}}}\right) f_{l_{\rm k}}(l_{\rm k})\mathbf{d}l_{\rm k} \\
&= \int_0^{\left(\frac{P_{\rm k}h_{\rm k}G_eG_{\{t,r\}}}{\eta_e}\right)^{\frac{1}{\alpha_{\rm k}}}} \exp\left(-\mu_{\rm k}\gamma_e l_{\rm k}^{\alpha_{\rm k}}\sigma^2\right)\mathcal{L}_{I_{\rm k}}\left(\frac{b_e}{P_{\rm k}}\right) f_{l_{\rm k}}(l_{\rm k})\mathbf{d}l_{\rm k},
\end{aligned} \quad (13)$$

where $b_e = \frac{\mu_e\gamma_e l_{\rm k}^{\alpha_{\rm k}}}{G_eG_{\{t,r\}}}$ and $\mathcal{L}_{I_{\rm k}}\left(\frac{b_e}{P_{\rm k}}\right)$ is the Laplace transform of the cumulative interference from the other terrestrial users, which can be calculated as

$$\begin{aligned}
\mathcal{L}_{I_{\rm k}}\left(\frac{b_e}{P_{\rm k}}\right) &= \mathbb{E}_{\Phi_{A_e}}\exp\left(\sum -\frac{b_e}{P_{\rm k}}P_{\rm k}G_eG_{\{t,r\}}h_{\rm k}{l_{\rm k}}^{-\alpha_{\rm k}}\right) \\
&= \mathbb{E}_{\Phi_{A_e}}\left[\prod \exp(-b_eG_eG_{\{t,r\}}h_{\rm k}{l_{\rm k}}^{-\alpha_{\rm k}})\right] \\
&= \mathbb{E}_{\Phi_{A_e}}\left[\prod \frac{1}{1+\gamma_e}\right].
\end{aligned} \quad (14)$$

Herein, Φ_{A_e} is the set of the other interfering users. The probability generation function (PGF) of the HPPP has the following property: for a function $f(x)$, $\mathbb{E}_{\Phi_{A_e}}\left[\prod f(x)\right] = \exp\left(-\lambda\int_{\pi l_{\max}^2}(1-f(x))\mathrm{d}x\right)$. Therefore, (14) can be further transformed as

$$\begin{aligned}
\mathcal{L}_{I_{\rm k}}\left(\frac{b_e}{P_{\rm k}}\right) &= \exp\left(\lambda_{\{t,r\}}\int_{\pi l_{\max}^2}\left(1-\frac{1}{1+\gamma_e}\right)l_{\rm k}\mathbf{d}l_{\rm k}\right) \\
&= \exp\left(-\lambda_{\{t,r\}}\int_{\pi l_{\max}^2}\frac{\gamma_e}{1+\gamma_e}l_{\rm k}\mathbf{d}l_{\rm k}\right) \\
&= \exp\left(-2\pi\lambda_{\{t,r\}}\int_0^{l_{\max}}\frac{\gamma_e}{1+\gamma_e}l_{\rm k}\mathbf{d}l_{\rm k}\right).
\end{aligned} \quad (15)$$

Consequently, inserting (11) and (15) into (13), we have the final expression of $\mathcal{P}_{\rm k}$, as given in (8). ■

Next, we derive the eavesdropping probability of a low-altitude eavesdropping link denoted by $\mathcal{P}_{ue}$. It is worth mentioning that the low-altitude eavesdropping link only includes the link from the UAV bridge to the eavesdropper. The expression of $\mathcal{P}_{ue}$ is given in Lemma 2 as follows.

Lemma 2: The eavesdropping probability of a low-altitude eavesdropping link $\mathcal{P}_{ue}$ is given by

$$\begin{aligned}
&\mathcal{P}_{ue} \\
&= \pi\lambda_u \times \frac{\tan(\frac{\pi-\theta_u}{2}-\psi_u)-\tan(\frac{\pi-3\theta_u}{2}-\psi_u)}{\sqrt{\lambda_u}\left(H_{u,\max}-H_{u,\min}\right)} \\
&\quad\times \exp\left(-2\pi\lambda_u\int_{H_{u,min}}^{H_{u,max}}\int_{h_u}^{l_{\max'}}\frac{\gamma_e f_{H_u}(h_u)}{1+\gamma_e}l_{ue}\mathbf{d}l_{ue}\mathbf{d}h_u\right) \\
&\quad\times \int_{H_{u,min}}^{H_{u,max}}\int_{h_u}^{l_{\max'}}\exp\left(-\lambda_u\pi\left({l_{ue}}^2-h_u^2\right)-\mu_u\gamma_e {l_{ue}}^{\alpha_{ue}}\sigma^2\right) \\
&\quad\times l_{ue}f_{H_u}(h_u)\mathbf{d}l_{ue}\mathbf{d}h_u,
\end{aligned} \quad (16)$$

where $f_{H_u}(h_u) = (H_{u,\max}-H_{u,\min})$ denotes the PDF of UAV deployment height H_u, while l_{ue} is the straight-line distance of the low-attitude eavesdropping link within the range of $[H_u, l_{\max'}]$. Note that $l_{\max'}=\max\{\left(P_{ue}h_{ue}G_eG_u^b/\eta_e\right)^{1/\alpha_{ue}}, H_u\}$ is the maximum eavesdropping range for the low-attitude eavesdropping link. Herein, G_e depends on the vertical angle between the eavesdropper and the UAV, $G_u^b = \left(1-\frac{3}{2\pi\theta_u}\sin\left(\frac{\theta_u}{2}\right)\right)/\left(1-\frac{\theta_u}{2\pi}\sin\left(\frac{\theta_u}{2}\right)\right)$ denotes the antenna gain of the side/back lobe at UAV under the iris model, where θ_u is the main lobe beamwidth of UAV.

Proof: The antenna gains of the UAV and the eavesdropper are related to the angle between the UAV and the eavesdropper. Note that the elevation angle of the omni-directional antenna at the eavesdropper is equal to the depression angle of the directional antenna at the UAV, i.e., $\phi_o = \phi_d$. Herein, ϕ_d can be calculated by $\phi_d = \arctan\left(H_u/d_{ue}\right)$, where d_{ue} is the distance between an eavesdropper and the UAV projection. Following the similar procedure of (10) (11), the PDF of d_{ue} can be expressed as $f_{d_{ue}}(x) = 2\pi\lambda_u x\exp\left(-\lambda_u\pi x^2\right)$. Then, according to $f_{d_{ue}}(x)$ and $f_{H_u}(h_u)$, the PDF of ϕ_d is derived as

$$f_{\phi_d}(\phi) = \frac{1}{2\sqrt{\lambda_u}\left(H_{u,\max}-H_{u,\min}\right)}\times\frac{1}{\cos^2\phi}. \quad (17)$$

The eavesdropper can only wiretap the confidential information leaked by the side/back lobes of UAV antennas. It means only when the eavesdropper appears in the coverage region of side/back lobes of UAV antennas, i.e., $\phi_d \in [\frac{\pi-\theta_u}{2}-(\psi_u+\theta_u), \frac{\pi-\theta_u}{2}-\psi_u]$, confidential information can be wiretapped. The solid angle ψ_u can be calculated by $\psi_u = 4\pi/(N+1) - 2\pi\left(1-\cos\left(\theta_u/2\right)\right)$. Then, we further derive the probability that the eavesdropper is inside the coverage region of side/back lobes of the UAV as

$$\begin{aligned}
\mathcal{P}_{in,e} &= \mathbb{P}\left[\frac{\pi-\theta_u}{2}-(\psi_u+\theta_u) \le \phi \le \frac{\pi-\theta_u}{2}-\psi_u\right] \\
&= F_{\phi_d}(\frac{\pi-\theta_u}{2}-\psi_u) - F_{\phi_d}(\frac{\pi-\theta_u}{2}-(\psi_u+\theta_u)) \\
&= \frac{\tan(\frac{\pi-\theta_u}{2}-\psi_u)-\tan(\frac{\pi-3\theta_u}{2}-\psi_u)}{2\sqrt{\lambda_u}\left(H_{u,\max}-H_{u,\min}\right)}.
\end{aligned} \quad (18)$$

For keyhole model, $\mathcal{P}_{in,e}=1$. In addition, according to (17), the antenna gain of the eavesdropper G_e can be calculated by $G_e=\int_0^{\pi/2}10^{-1.2\phi_o^2/\phi_{3\text{dB}}^2}f_{\phi_d}(\phi_o)\mathbf{d}\phi_o$. Following the similar derivation procedure in the proof of Lemma 1, the eavesdropping probability of the low-altitude eavesdropping link $\mathcal{P}_{ue}$ given in (16) can be obtained. ■

After we obtain the aforementioned preliminary results of the eavesdropping probability. We can have the following results for the eavesdropping probability of the aerial bridge scheme.

Theorem 1: The eavesdropping probability of the aerial bridge scheme is expressed as

$$\begin{aligned}\mathcal{P}_{\text{eave}}^{\text{uav}}&=1-\Big[1-2\pi\lambda_t\exp\left(-\frac{\lambda_t\gamma_e\pi l_{\max}^2}{1+\gamma_e}\right)\\&\times\int_0^{l_{\max}}l_{te}\exp\left(-\lambda_t\pi {l_{te}}^2-\mu_{te}\gamma_e {l_{te}}^{\alpha_{te}}\sigma^2\right)\mathbf{d}l_{te}\Big]\\&\times\Big[1-2\pi\lambda_u\exp\left(-\int_{H_{u,min}}^{H_{u,max}}\frac{\lambda_u\gamma_e\pi\left({l_{\max'}}^2-h_u^2\right)}{1+\gamma_e}f_{H_u}(h_u)\mathbf{d}h_u\right)\\&\times\int_{H_{u,min}}^{H_{u,max}}\int_{h_u}^{l_{\max'}}\exp\left(-\lambda_u\pi\left({l_{ue}}^2-h_u^2\right)-\mu_{ue}\gamma_e {l_{ue}}^{\alpha_{ue}}\sigma^2\right)\\&\times f_{H_u}(h_u)l_{ue}\mathbf{d}l_{ue}\mathbf{d}h_u\times\mathcal{P}_{in,e}\Big].\end{aligned}\tag{19}$$

Proof: According to Definition 1, the preliminary expression of the eavesdropping probability of the aerial bridge scheme can be expressed as

$$\mathcal{P}_{\text{eave}}^{\text{uav}}=1-\left(1-\mathcal{P}_{te}\right)\times\left(1-\mathcal{P}_{ue}\right),\tag{20}$$

where $\mathcal{P}_{te}$ denotes the eavesdropping probability of the ground eavesdropping link between the user and the eavesdropper, while $\mathcal{P}_{ue}$ is the eavesdropping probability of the low-altitude eavesdropping link. According to the results given in Lemma 1 and Lemma 2, we can obtain the expressions of $\mathcal{P}_{te}$ and $\mathcal{P}_{ue}$. Then, inserting (8) and (16) into (20), we have the eavesdropping probability $\mathcal{P}_{\text{eave}}^{\text{uav}}$ for the aerial bridge scheme.■

The eavesdropping probability $\mathcal{P}_{\text{eave}}^{\text{uav}}$ depends on the connectivity of the ground eavesdropping link and the low-altitude eavesdropping link. Thus, the information leakage occurring in any link endangers the transmission of confidential information. Referring to Theorem 1, $\mathcal{P}_{\text{eave}}^{\text{uav}}$ is determined by comprehensive system parameters, including the density of terrestrial users λ_t and the density of UAVs λ_u, the UAV deployment height H_u, as well as the eavesdropping range in terms of the transmits power of the terrestrial user P_{te} and the transmits power of the UAV P_{ue}. More insights are presented in Section V-B.

B. Eavesdropping Probability of Ground Relay Scheme and Direct Link in TSNs

For comparison purposes, we also consider the ground relay scheme and direct link in TSNs without protection (i.e., non-protection scheme) in this paper. Specifically, in the ground relay scheme, the eavesdropper still wiretaps the confidential information leaked from two links, including the link from the user to the ground relay and the link from the ground relay to the satellite. When the user communicates with the satellite directly without any protection, the eavesdropper can only wiretap the information transmitted by the legitimate user. Next, we conduct the analysis on the eavesdropping probability of the ground relay scheme and the non-protection scheme, respectively.

Firstly, we present the the result about the eavesdropping probability of the ground relay scheme denoted by $\mathcal{P}_{\text{eave}}^{\text{gro}}$ in Theorem 2.

Theorem 2: The eavesdropping probability of the ground relay scheme $\mathcal{P}_{\text{eave}}^{\text{gro}}$ is expressed as

$$\begin{aligned}\mathcal{P}_{\text{eave}}^{\text{gro}}&=1-\Big[1-2\pi\lambda_t\exp\left(-\frac{\lambda_t\gamma_e\pi l_{\max}^2}{1+\gamma_e}\right)\\&\times\int_0^{l_{\max}}l_{te}\exp\left(-\lambda_t\pi {l_{te}}^2-\mu_{te}\gamma_e {l_{te}}^{\alpha_{te}}\sigma^2\right)\mathbf{d}l_{te}\Big]\\&\times\Big[1-2\pi\lambda_r\exp\left(-\frac{\lambda_r\gamma_e\pi l_{\max}^2}{1+\gamma_e}\right)\\&\times\int_0^{l_{\max}}l_{re}\exp\left(-\lambda_r\pi {l_{re}}^2-\mu_{re}\gamma_e {l_{re}}^{\alpha_{re}}\sigma^2\right)\mathbf{d}l_{re}\Big].\end{aligned}\tag{21}$$

Proof: According to Definition 1, the eavesdropping probability of the ground relay scheme can be given as

$$\mathcal{P}_{\text{eave}}^{\text{gro}}=1-\left(1-\mathcal{P}_{te}\right)\times\left(1-\mathcal{P}_{re}\right),\tag{22}$$

where $\mathcal{P}_{re}$ denotes the eavesdropping probability of the ground eavesdropping link between the ground relay and the eavesdropper. Both $\mathcal{P}_{te}$ and $\mathcal{P}_{re}$ are expressed in Lemma 1. Consequently, we can obtain the eavesdropping probability $\mathcal{P}_{\text{eave}}^{\text{gro}}$ of the ground relay scheme by inserting expressions of $\mathcal{P}_{te}$ and $\mathcal{P}_{re}$ into (22). ■

Similar to Theorem 1, the eavesdropping probability $\mathcal{P}_{\text{eave}}^{\text{gro}}$ in Theorem 2 is determined by the connectivity of two types of ground eavesdropping links. Thus, the density λ_t and λ_r as well as the transmit power P_{te} and P_{re} can affect $\mathcal{P}_{\text{eave}}^{\text{gro}}$.

Then, we obtain the result about the eavesdropping probability of the non-protection scheme denoted by $\mathcal{P}_{\text{eave}}^{\text{non}}$ as follows.

Theorem 3: The eavesdropping probability of the non-protection scheme $\mathcal{P}_{\text{eave}}^{\text{non}}$ can be expressed as

$$\begin{aligned}\mathcal{P}_{\text{eave}}^{\text{non}}=&\int_0^{\left(\frac{P_{te}G_tG_eh_{te}}{\eta_e}\right)^{\frac{1}{\alpha_{te}}}}l_{te}\exp\left(-\lambda_t\pi {l_{te}}^2-\mu_{te}\gamma_e {l_{te}}^{\alpha_{te}}\sigma^2\right)\mathbf{d}l_{te}\\&\times 2\pi\lambda_t\exp\left(-2\pi\lambda_t\int_0^{l_{\max}}\frac{\gamma_e}{1+\gamma_e}l_{te}\mathbf{d}l_{te}\right).\end{aligned}\tag{23}$$

Proof: Since the legitimate user communicates with the satellite directly without protection, the eavesdropper can only wiretap the confidential information transmitted by the user. Therefore, the eavesdropping probability of the non-protection scheme is expressed as $\mathcal{P}_{\text{eave}}^{\text{non}}=\mathcal{P}_{te}$. Then, we can obtain the eavesdropping probability $\mathcal{P}_{\text{eave}}^{\text{non}}$ according to (8). ■

According to Theorem 3, it can ben seen that the eavesdropping probability $\mathcal{P}_{\text{eave}}^{\text{non}}$ only relies on a ground eavesdropping link. Thus, the density λ_t, the transmit power P_{te} and the antenna gain G_t are dominate parameters for $\mathcal{P}_{\text{eave}}^{\text{non}}$.

IV. Link Connectivity Analysis

In this section, we evaluate the performance of legitimate transmission for TSNs under the aerial bridge scheme, the ground relay scheme and non-protection scheme. In TSNs, a satellite serves massive legitimate nodes in a wide coverage region. The topological connection is the basic guarantee of communications. Thus, we need to analysis the topological connection of each legitimate node in TSNs to evaluate the quality of legitimate transmission. Herein, we introduce link connectivity as a metric. The definition is given as follows.

Definition 2: Link connectivity is the probability that the confidential information transmitted from the legitimate source can be successfully decoded at the legitimate destination.

Next, we conduct the analysis on the link connectivity of the aerial bridge scheme in Section IV-A and the link connectivity of the ground relay scheme and the direct link in TSNs in Section IV-B.

A. Link Connectivity of Aerial Bridge Scheme

We first analyze the link connectivity of the aerial bridge scheme, in which UAVs play the roles of aerial bridges to support data transmissions between terrestrial users and the satellite while countering wiretapping from eavesdroppers. To analyze the link connectivity of the aerial bridge scheme, we need to obtain the expectations of the received cumulative interference of the satellite from UAVs and terrestrial users, respectively. We first derive the expectations of the received cumulative interference from UAVs denoted by I_{us}, which is presented in the following result.

Lemma 3: The received cumulative interference of the satellite from UAVs can be expressed as

$$\begin{aligned} I_{us} &= 2\left(\lambda_u \pi D_I\right)^2 \times \mathcal{P}_{in,u} P_{us} G_u^m G_s^m \\ &\times \int_0^{D_I} \left((H_s - H_u)^2 + d_{js}^2\right)^{-\frac{\alpha_{us}}{2}} \mathrm{e}^{-\lambda_u \pi d_{js}^2} d_{js} \mathbf{d} d_{js} \\ &+ \upsilon \times 2\pi \lambda_u^2 A_{s'} \times \mathcal{P}_{in,u'} P_{us} G_u^m G_s^b \\ &\times \int_{(H_s - H_u)\tan\frac{\theta_s}{2}}^{\left(\frac{P_{us} G_u^m G_s^b}{\eta_s}\right)^{\frac{1}{\alpha_{us}}}} \left((H_s - H_u)^2 + d_{js}^2\right)^{-\frac{\alpha_s}{2}} \\ &\times \mathrm{e}^{-\lambda_u \pi d_{js}^2} d_{js} \mathbf{d} d_{js}, \end{aligned} \tag{24}$$

where $D_I = \min\left\{\left(P_{us} G_u^m G_s^m / \eta_s\right)^{1/\alpha_{us}}, (H_s - H_u)\tan\theta_s/2\right\}$ denotes the effective distance of main lobe interference, η_s is the threshold of received power at the satellite, d_{js} denotes the projection distance between the j-th UAV and the satellite, and $\upsilon = \{0, 1\}$. Moreover, $\mathcal{P}_{in,u}$ and $\mathcal{P}_{in,u'}$ are the probability that interfering UAVs appear in the coverage region of the main lobe and side/back lobe at the satellite, respectively.

Proof: Please refer to the Appendix A. ∎

Then, we derive the expectations of the received cumulative interference from terrestrial users denoted by I_{ts}. The expression is given in Lemma 4.

Lemma 4: The received cumulative interference of the satellite from terrestrial users can be expressed as

$$\begin{aligned} I_{ts} &= \lambda_t \pi \min\left\{\left(\frac{P_{ts} G_s^m G_t h_{ts}}{\eta_s}\right)^{\frac{2}{\alpha_{ts}}} - H_s^2, \left(H_s \tan\left(\frac{\theta_s}{2}\right)\right)^2\right\} \\ &\times P_{ts} \overline{L_{ts}} G_s^m G_t \times (2\rho)^{m-1} \left(m\left(2\rho m + \Omega\right)\right)^{m-2} \\ &\times \sum_{n=0}^{m-1} \frac{(1-m)_n}{(n!)^2} \left(-\frac{\Omega}{2\rho P_{ts} \overline{L_{ts}} G_s^m G_t}\right)^n \Gamma(n+2) m^{-n} \\ &\times \left(1 + \int_0^{\frac{\pi-\theta_s}{2}} \frac{2\pi\lambda_t H_s^2 \cos\phi}{\sin^3\phi} \exp\left(-\frac{\pi\lambda_t H_s^2}{\sin^3\phi}\right) \mathrm{d}\phi\right), \end{aligned} \tag{25}$$

It is worth mentioning that G_t and G_s^m are related to the elevation angle between the terrestrial user and the satellite according to the selected antenna model.

Proof: Please refer to the Appendix B. ∎

Based on the aforementioned results from Lemmas 3 and 4, we can have the following result about the link connectivity of the aerial bridge scheme denoted by $\mathcal{P}_{\text{con}}^{\text{uav}}$.

Theorem 4: The link connectivity of the aerial bridge scheme $\mathcal{P}_{\text{con}}^{\text{uav}}$ is expressed as

$$\begin{aligned} \mathcal{P}_{\text{con}}^{\text{uav}} &= \int_{H_{u,\min}}^{H_{u,\max}} \left[1 - \exp\left(-\lambda_u \pi \left(\left(\frac{P_{us} G_u^m G_s^m}{\gamma_s (I_{ts} + I_{us} + \sigma^2)}\right)^{\frac{2}{\alpha_{us}}} - (H_s - H_u)^2\right)\right)\right] \\ &\times 2\pi\lambda_t \left(1 - \exp\left(-\lambda_t \pi \left(H_u \tan\frac{\theta_u}{2}\right)^2\right)\right) \int_{H_u}^{\frac{H_u}{\cos(\theta_u/2)}} \\ &\times \exp\left(-\pi\lambda_t \int_{l_{min}^{-\alpha_{tu}}}^{\frac{\eta_u}{P_{tu} G_t G_u^b h_{tu}}} \frac{b_u G_u^b w}{\mu_{tu} + b_u G_u^b w} \left(-\frac{2}{\alpha_{tu}}\right) w^{\frac{-\alpha_{tu}-2}{\alpha_{tu}}} \mathbf{d} w\right) \\ &\times \exp\left(-\pi\lambda_t \frac{2 b_u G_u^m \left(H_u \sqrt{\tan^2\frac{\theta_u}{2} + 1}\right)^{2-\alpha_{tu}}}{(\alpha_{tu} - 2)\mu_{tu}}\right. \\ &\left. \times {}_2\mathrm{F}_1\left(1, \frac{\alpha_{tu}-2}{\alpha_{tu}}; 2 - \frac{2}{\alpha_{tu}}; -\frac{b_u G_u^m \left(H_u \sqrt{\tan^2\frac{\theta_u}{2} + 1}\right)^{-\alpha_{tu}}}{\mu_{tu}}\right)\right) \\ &\times l_{tu} \\ &\times \exp\left(-\lambda_t \pi \left(l_{tu}^2 - H_u^2\right) - \mu_{tu}\gamma_u l_{tu}^{\alpha_{tu}} \sigma^2\right) \mathbf{d} l_{tu} f_{H_u}(H_u) \mathbf{d} H_u, \end{aligned} \tag{26}$$

where $l_{min} = H_u\left(\tan^2(\theta_u/2) + 1\right)^{1/2}$ denotes the minimum interfering distance for the side/back lobe at the UAV, γ_u and γ_s are the SINR thresholds of the UAV and the satellite, respectively.

Proof: In the aerial bridge scheme, there are two types of transmission links based on different channel models, including the low-altitude link (i.e., the transmission from the target user to the UAV) and the high-altitude link (i.e., the transmission from the UAV to the satellite). Specifically, the terrestrial user transmits confidential information to the UAV. After the

information is successfully detected and decoded at the UAV, it is forwarded from the UAV to the satellite. According to Definition 2, in the aerial bridge scheme, the confidential information transmitted from the legitimate user can be successfully decoded by the satellite, and the following conditions should be satisfied: 1) the information transferred from the user can be successfully decoded by the UAV (defined as the link connectivity of the low-altitude link); 2) the information forwarded by the UAV can be successfully received and decoded by the satellite (defined as the link connectivity of the high-altitude link). Then, we obtain the link connectivity of the aerial bridge scheme, which can be expressed as

$$\mathcal{P}_{\text{con}}^{\text{uav}} = \mathcal{P}_{tu} \times \mathcal{P}_{us}, \tag{27}$$

where $\mathcal{P}_{tu}$ is the link connectivity of the low-altitude link, while $\mathcal{P}_{us}$ is the link connectivity of the high-altitude link. Next, we present the derivations of $\mathcal{P}_{tu}$ and $\mathcal{P}_{us}$, respectively.

In the target scenario, we assume that the main lobe of the UAV antenna is perpendicularly projected on the ground. Therefore, the coverage area on the ground is deemed as a circle with the center of the UAV projection. According to the Pythagorean theorem, the distance between the target user and the UAV denoted by l_{tu} can be calculated by $(H_u^2 + d_{tu}^2)^{1/2}$, where d_{tu} represents the distance between the user and the UAV projection. Similar to the derivation of PDF of l_{k} given in (11), the PDF of l_{tu} can be further expressed as

$$f_{l_{tu}}(x) = \exp\left(-\lambda_t \pi \left(x^2 - H_u^2\right)\right) 2\pi\lambda_t x. \tag{28}$$

Additionally, when a UAV bridge can successfully decode the confidential information from the target legitimate user, the following conditions needs to be satisfied [41]: 1) at least one UAV can connect with the target user; 2) the received SINR at UAV is larger than the threshold γ_u. Hence, the link connectivity $\mathcal{P}_{tu}$ can be expressed as

$$\begin{aligned}
&\mathcal{P}_{tu} \\
&= \mathbb{P}\left[l_{tu} < H_u \tan\frac{\theta_u}{2}\right] \times \mathbb{P}\left[\text{SINR}_u > \gamma_u\right] \\
&= \int_{H_{u,\min}}^{H_{u,\max}} \left(1 - \exp\left(-\lambda_t \pi \left(h_u \tan\frac{\theta_u}{2}\right)^2\right)\right) f_{H_u}(h_u) \mathbf{d}h_u \\
&\quad \times \mathbb{E}_{l_{tu}}\left[\mathbb{P}\left[\frac{P_{tu} G_t G_u^m h_{tu} l_{tu}^{-\alpha_{tu}}}{I_{tu} + \sigma^2} > \gamma_u \mid l_{tu}\right]\right],
\end{aligned} \tag{29}$$

where I_{tu} is the cumulative interference from other users received by the UAV. Especially, I_{tu} comprises two parts, including the interference received by the main lobe I_{tu}^m and the interference received by side/back lobe I_{tu}^b. Then, the last term of the right hand side in (29) can be further derived as

$$\begin{aligned}
&\mathbb{E}_{l_{tu}}\left[\mathbb{P}\left[\frac{P_{tu} G_t G_u^m h_{tu} l_{tu}^{-\alpha_{tu}}}{I_{tu} + \sigma^2} > \gamma_u \mid l_{tu}\right]\right] \\
&= \int_{H_{u,\min}}^{H_{u,\max}} \int_{H_u}^{\frac{H_u}{\cos(\theta_u/2)}} f_{H_u}(H_u)\, f_{l_{tu}}(l_{tu}) \\
&\quad \times \exp\left(-\mu_{tu}\gamma_u l_{tu}^{\alpha_{tu}} \sigma^2\right) \mathcal{L}_{I_{tu}^m}\left(\frac{b_u}{P_{tu}}\right) \mathcal{L}_{I_{tu}^b}\left(\frac{b_u}{P_{tu}}\right) \mathbf{d}l_{tu} \mathbf{d}H_u,
\end{aligned} \tag{30}$$

where $b_u = \frac{\mu_{tu}\gamma_u l_{tu}^{\alpha_{tu}}}{G_t G_u^m}$. $\mathcal{L}_{I_{tu}^m}\left(\frac{b_u}{P_{tu}}\right)$ and $\mathcal{L}_{I_{tu}^b}\left(\frac{b_u}{P_{tu}}\right)$ denote the Laplace transform of I_{tu}^m and I_{tu}^b, respectively. Note that the cumulative interference of the UAV can be calculated by $I_{tu}^m = \sum_{i \in \Phi_{A_u}} P_{tu} G_u^m h_{tu} l_{iu}^{-\alpha_{tu}}$ and $I_{tu}^b = \sum_{i \in \Phi_t \setminus \Phi_{A_u}} P_{tu} G_u^b h_{tu} l_{iu}^{-\alpha_{tu}}$, respectively, where l_{iu} denotes the distance between the i-th user and the UAV. Moreover, Φ_t is the set of all users in the network, Φ_{A_u} is the set of users who are distributed in the coverage area of the main lobe at the UAV. Similar to the derivations of (14) and (15), the Laplace transform of I_{tu}^m and I_{tu}^b are given as

$$\begin{aligned}
\mathcal{L}_{I_{tu}^m}\left(\frac{b_u}{P_{tu}}\right) = \exp\Bigg(&-\pi\lambda_t \frac{2 b_u G_u^m \left(H_u \sqrt{\tan^2\frac{\theta_u}{2} + 1}\right)^{2-\alpha_{tu}}}{(\alpha_{tu} - 2)\mu_{tu}} \\
&{}_2\text{F}_1\left(1, \frac{\alpha_{tu}-2}{\alpha_{tu}}; 2 - \frac{2}{\alpha_{tu}}; -\frac{b_u G_u^m \left(H_u \sqrt{\tan^2\frac{\theta_u}{2} + 1}\right)^{-\alpha_{tu}}}{\mu_{tu}}\right)\Bigg),
\end{aligned} \tag{31}$$

where ${}_2\text{F}_1(\mathfrak{a}, \mathfrak{b}, \mathfrak{c})$ is a Gaussian hypergeometric function. Considering the component sensitivity of UAV antennas, we assume that the minimum received power at the UAV is η_u. Then, with the same method illustrated in (9), the maximum transmission distance from the interfering user to the UAV can be calculated by $\left(P_{tu} G_t G_u^b h_{tu}/\eta_u\right)^{1/\alpha_{tu}}$. Therefore, the Laplace transform of I_{tu}^b can be expressed as

$$\begin{aligned}
&\mathcal{L}_{I_{tu}^b}\left(\frac{b_u}{P_{tu}}\right) \\
&= \exp\left(-\pi\lambda_t \int_{l_{min}^{-\alpha_{tu}}}^{\frac{\eta_u}{P_{tu} G_t G_u^b h_{tu}}} \frac{b_u G_u^b w}{\mu_{tu} + b_u G_u^b w} \left(-\frac{2}{\alpha_{tu}}\right) w^{\frac{-\alpha_{tu}-2}{\alpha_{tu}}} \mathbf{d}w\right),
\end{aligned} \tag{32}$$

where $l_{min} = H_u / \cos\frac{\theta_u}{2}$. Following the similar derivation of $\mathcal{P}_{tu}$, the connectivity of high-altitude link $\mathcal{P}_{us}$ can be calculated as

$$\begin{aligned}
&\mathcal{P}_{us} \\
&= \mathbb{P}\left[\frac{P_{us} G_s^m G_u^m l_{us}^{-\alpha_{us}}}{I_{us} + I_{ts} + \sigma^2} > \gamma_s\right] \\
&= \mathbb{P}\left[d_{us} < \left(\left(\frac{P_{us} G_u^m G_s^m}{\gamma_s \left(I_{us} + I_{ts} + \sigma^2\right)}\right)^{\frac{2}{\alpha_{us}}} - \left(H_s - H_u\right)^2\right)^{\frac{1}{2}}\right] \\
&= \int_{H_{u,\min}}^{H_{u,\max}} \left[1 - \exp\left(-\lambda_u \pi \left(\left(\frac{P_{us} G_u^m G_s^m}{\gamma_s \left(I_{us} + I_{ts} + \sigma^2\right)}\right)^{\frac{2}{\alpha_{us}}} - \left(H_s - h_u\right)^2\right)\right)\right] \\
&\quad \times f_{H_u}(h_u) \mathbf{d}h_u,
\end{aligned} \tag{33}$$

where γ_s is SINR threshold at the satellite. The distance between the UAV bridge and the projection of the satellite on the aerial platform is denoted by d_{us}.

The link connectivity $\mathcal{P}_{us}$ is calculated by inserting (24) and (25) into (33). Finally, according to the results of $\mathcal{P}_{tu}$ and $\mathcal{P}_{us}$, the link connectivity $\mathcal{P}_{\text{con}}^{\text{uav}}$ for the aerial bridge scheme can be obtained. ■

The link connectivity $\mathcal{P}_{\text{con}}^{\text{uav}}$ depends on the connectivity of the low-altitude link and the high-altitude link. Referring to Theorem 4, $\mathcal{P}_{\text{con}}^{\text{uav}}$ is determined by comprehensive system parameters, including the density λ_t and λ_u, the UAV deployment height H_u, the transmit power P_{tu} and P_{us}, as well as antenna beamwidth θ_u.

B. Link Connectivity of Ground Relay Scheme and Direct Link in TSNs

We next present the link connectivity of the ground relay scheme and direct link without protection (i.e., non-protection scheme) with the following results, respectively.

Theorem 5: The link connectivity of the ground relay scheme denoted by $\mathcal{P}_{\text{con}}^{\text{gro}}$ is expressed as

$$\begin{aligned}\mathcal{P}_{\text{con}}^{\text{gro}} =&\left(1-\exp\left(-\lambda_r\pi l_{\max}^2\right)\right)\\ &\times\left[1-\frac{I_{ts}+\sigma^2}{2\rho P_{rs}G_s^mG_r\overline{L_{rs}}}\right.\\ &\times\left(\frac{2\rho m}{2\rho m+\Omega}\right)^m\int_0^{\gamma_s}t^n\exp\left(-\frac{m\left(I_{ts}+\sigma^2\right)}{P_{rs}G_s^mG_r\overline{L_{rs}}(2\rho m+\Omega)}t\right)\mathbf{d}t\\ &\left.\times\sum_{n=0}^{m-1}\frac{(1-m)_n}{(n!)^2}\left(-\frac{\Omega\left(I_{ts}+\sigma^2\right)}{2\rho P_{rs}G_s^mG_r\overline{L_{rs}}\left(2\rho m+\Omega\right)}\right)^n\right].\end{aligned} \tag{34}$$

Proof: For the ground relay scheme, confidential information is first transmitted from the user to a ground relay who appears within the communication range of the user. Then, the ground relay forwards the information to the satellite. According to Definition 2, we have the link connectivity of the ground relay scheme expressed as $\mathcal{P}_{\text{con}}^{\text{gro}}=\mathcal{P}_{tr}\times\mathcal{P}_{rs}$, where $\mathcal{P}_{tr}$ is the connectivity of the link between the target user and the relay, while $\mathcal{P}_{rs}$ denotes the connectivity of the link between the relay and the satellite.

Since only if at least one ground relay appears in the communication range of the target legitimate user, the confidential information can be successfully transmitted to the relay. Thus, we can express $\mathcal{P}_{tr}$ as

$$\mathcal{P}_{tr}=\mathbb{P}[y\geq 1]=1-\mathbb{P}[y=0]=1-\exp(-\lambda_r\pi l_{\max}^2), \tag{35}$$

where y is the number of ground relays appearing in the communication range of a user.

The satellite can successfully decode the confidential information from the relay, only if its received SINR denoted by SINR_s is larger than a threshold γ_s. Thus, the connectivity of direct link $\mathcal{P}_{rs}$ can be expressed as

$$\mathcal{P}_{rs}=1-\mathbb{P}\left[\text{SINR}_s\leq\gamma_s\right]=1-F_{\text{SINR}_s}\left(\gamma_s\right), \tag{36}$$

where $F_{\text{SINR}_s}\left(\gamma_s\right)$ is the CDF of SINR_s. In particular, the received SINR at the satellite can be further derived as

$$\text{SINR}_s=\frac{P_{rs}\overline{L_{rs}}h_{rs}G_s^mG_r}{I_{ts}+\sigma^2}=\frac{\frac{P_{rs}\overline{L_{rs}}h_{rs}G_s^mG_r}{\sigma^2}}{\frac{I_{ts}}{\sigma^2}+1}=\frac{\text{SNR}_s}{C}, \tag{37}$$

where $\text{SNR}_s=\frac{P_{rs}\overline{L_{rs}}h_{rs}G_s^mG_r}{\sigma^2}$ denotes the signal-to-noise ratio (SNR) at the satellite, and $C=\frac{I_{ts}}{\sigma^2}+1$. Specifically, $\overline{L_{rs}}$ is the average free-space path loss for the signal transmitted by the ground relay, and following the same derivation as $\overline{L_{ts}}$ illustrated in (51) (details given in Appendix B), $\overline{L_{rs}}$ can be calculated. Meanwhile, I_{ts} can be calculated according to Lemma 4. Based on (6), the PDF of SNR_s can be given by

$$\begin{aligned}f_{\text{SNR}_s}(x)=&\frac{1}{2\rho\overline{\text{SNR}_s}}\left(\frac{2\rho m}{2\rho m+\Omega}\right)^m\\ &\times\exp\left(-\frac{x}{2\rho\overline{\text{SNR}_s}}\left(1-\frac{\Omega}{2\rho m+\Omega}\right)\right)\\ &\times\sum_{n=0}^{m-1}\frac{(1-m)_n}{(n!)^2}\left(-\frac{\Omega x}{2\rho\overline{\text{SNR}_s}\left(2\rho m+\Omega\right)}\right)^n,\end{aligned} \tag{38}$$

where $\overline{\text{SNR}_s}=\frac{P_{rs}\overline{L_{rs}}G_s^mG_r}{\sigma^2}$. We can further calculate the PDF of SINR_s by $f_{\text{SINR}_s}(x)=Cf_{\text{SNR}_s}(Cx)$. Then, the CDF of SINR_s can be calculated as

$$\begin{aligned}F_{\text{SINR}_s}(x)=&\int_0^x f_{\text{SINR}_s}(t)dt=\frac{C}{2\rho\overline{\text{SNR}_s}}\left(\frac{2\rho m}{2\rho m+\Omega}\right)^m\\ &\times\int_0^x t^n\exp\left(-\frac{Cm}{\overline{\text{SNR}_s}\left(2\rho m+\Omega\right)}t\right)\mathbf{d}t\\ &\times\sum_{n=0}^{m-1}\frac{(1-m)_n}{(n!)^2}\left(-\frac{\Omega C}{2\rho\overline{\text{SNR}_s}\left(2\rho m+\Omega\right)}\right)^n.\end{aligned} \tag{39}$$

Finally, inserting (39) into (36), we can obtain the link connectivity $\mathcal{P}_{rs}$. Finally, we can have the link connectivity of the ground relay scheme $\mathcal{P}_{\text{con}}^{\text{gro}}$. ■

According to Theorem 5, the link connectivity $\mathcal{P}_{\text{con}}^{\text{gro}}$ is determined by the connectivity of the ground links and the high-attitude link. Hence, the density λ_t and λ_r as well as the transmit power P_{tr} and P_{rs} are the dominated parameters for $\mathcal{P}_{\text{con}}^{\text{gro}}$.

Then, we present the link connectivity of non-protection scheme denoted by $\mathcal{P}_{\text{con}}^{\text{non}}$ in Theorem 6.

Theorem 6: The link connectivity of non-protection scheme $\mathcal{P}_{\text{con}}^{\text{non}}$ is expressed as

$$\begin{aligned}\mathcal{P}_{\text{con}}^{\text{non}}=&1-\frac{I_{ts}+\sigma^2}{2\rho P_{ts}G_s^mG_t\overline{L_{ts}}}\left(\frac{2\rho m}{2\rho m+\Omega}\right)^m\\ &\times\int_0^{\gamma_s}t^n\exp\left(-\frac{m\left(I_{ts}+\sigma^2\right)}{P_{ts}G_s^mG_t\overline{L_{ts}}\left(2\rho m+\Omega\right)}t\right)\mathbf{d}t\\ &\times\sum_{n=0}^{m-1}\frac{(1-m)_n}{(n!)^2}\left(-\frac{\Omega\left(I_{ts}+\sigma^2\right)}{2\rho P_{ts}G_s^mG_t\overline{L_{ts}}\left(2\rho m+\Omega\right)}\right)^n.\end{aligned} \tag{40}$$

Proof: Without any protection, the user directly establishes a transmission link with the satellite without any protection. Therefore, following the same derivation of $\mathcal{P}_{rs}$ in Theorem 5, we can obtain the link connectivity of non-protection scheme. ■

As shown in Theorem 6, the link connectivity $\mathcal{P}_{\text{con}}^{\text{non}}$ only relies on the connectivity of the ground link. Hence, $\mathcal{P}_{\text{con}}^{\text{non}}$ is significantly related to the transmit power P_{ts}.

In the aerial bridge scheme, UAV bridges cost extra energy for confidential information transmission while terrestrial users save the energy consumed on transmitting, especially for energy-constrained devices, e.g., IoT nodes. Then, we analyze the whole energy consumption of the aerial bridge scheme and non-protection scheme. In order to guarantee that no extra energy is consumed, we have the following corollary.

Corollary 1: The transmit power of UAV bridges should satisfy the following relation, if all saved energy on terrestrial users is used by UAV bridges.

$$P_{us} = \frac{\lambda_t}{\lambda_u}(P_{ts} - P_{tu}). \tag{41}$$

Form Corollary 1, we can find that the transmit power of UAV bridges related to the ratio of the number of terrestrial users and the number of UAVs (i.e.,λ_t/λ_u), as well as the decreased power on terrestrial user from the direct link to UAV bridge assisted link (i.e., $P_{ts} - P_{tu}$). Furthermore, based on the above analysis, λ_t/λ_u is always much larger than 1 as the number of users significantly larger than the number of served UAVs. Hence, $P_{us} \ll \frac{\lambda_t}{\lambda_u}(P_{ts} - P_{tu})$, which means that our aerial bridge scheme can significantly save the total energy consumption on data transmission when compared with it of the direct link.

V. Numerical Results and Discussion

In this section, we present numerical results to validate the effectiveness of the aerial bridge scheme and to analyze our theoretical model. Specifically, we first introduce the simulation methodology and compare the performances of the considered scheme with the ground relay scheme, UAV jammer scheme and the non-protection scheme in Section V-A. Then, we investigate the impact of dominating parameters, such as the antenna beamwidth, the density of UAVs and the density of terrestrial users, on both the link connectivity and the eavesdropping probability in Section V-B.

A. Simulations

We conducted numerous simulations to validate the effectiveness of the aerial bridge scheme. Meanwhile, simulations also verify the accuracy of our theoretical model. In the simulations, terrestrial users are randomly distributed in a horizontal plane with the area of 100×100 km^2. Since most communication satellites are located in the Low-Earth orbit, in this paper, the deployment height of the satellite H_s is set as 200 km [42]. For such a deployment height, the antenna beamwidth at the satellite is set as $\theta_s = \pi/180$ to achieve a reasonable coverage. To resist high attenuation caused by long transmission distance and masking effect in the direct link, the transmit power of terrestrial users is set as $P_{ts} = 40$ W. Moreover, referring to [43], the specific channel parameters for TSNs are set as $(m, \rho, \Omega) = (2, 0.251, 0.279)$. The Gaussian white noise is $\sigma^2 = -45$ dBm [44], with the consideration of the receive sensitivity of the antennas at the satellite. In the aerial bridge scheme, UAVs are deployed uniformly at the height $H_u = 700$ m according to the ITU standard [45]. Note that P_{tu} can be set as mW level to further reduce the eavesdropping probability when transmit to the UAV. However, with the consideration of the hardware limitation of the transmitter, we unify the transmit power of terrestrial users as $P_{tu} = 1$ W [46]. Then, we set the transmit power of UAVs as $P_{us} = 30$ W. Since the deployment height of UAVs is hundreds of meters, the transmitted antenna beamwidth at UAVs is set as $\theta_{u'} = \pi/12$ for a viable distance. The SINR threshold values of UAV and eavesdropper are $\gamma_u = 10^{-3}$, $\gamma_e = 10^{-3}$, respectively. The values of main setting parameters are shown in Table I.

TABLE I
Table of Main Simulated Parameters

Parameters	Value
Transmit power of terrestrial users P_{tu} (aerial bridge scheme)	1 W
Transmit power of UAVs P_{us} (aerial bridge scheme)	30 W
Transmit power of terrestrial users P_{ts} (non-protection scheme)	40 W
SINR threshold at UAVs γ_u	10^{-3}
SINR threshold at eavesdroppers γ_e	10^{-3}
Deployment height of UAVs H_u	$[500, 1000]$ m
Deployment height of the satellite H_s	200 km
Antenna beamwidth at UAVs $\theta_{u'}$	$\pi/12$
Antenna beamwidth at the satellite θ_s	$\pi/180$

We denote the simulation results of the eavesdropping probability and the link connectivity by $\mathcal{P}_{\text{eave}}^{\text{sim}}$ and $\mathcal{P}_{\text{con}}^{\text{sim}}$, respectively, which are acquired by

$$\mathcal{P}_{\text{eave}}^{\text{sim}} = \frac{\text{the number of successful eavesdropping links}}{N_E}, \tag{42}$$

$$\mathcal{P}_{\text{con}}^{\text{sim}} = \frac{\text{the number of successful legitimate links}}{N_L}, \tag{43}$$

where N_E and N_L denote the total number of eavesdropping links and legitimate communication links, respectively. To relieve the complexity of simulations, we adopt the idealistic antenna model (i.e., the isotopic model and the keyhole model) to track our analysis on scheme effectiveness and theoretical accuracy. Moreover, the performance of the aerial bridge scheme has no distinct differences between the ideal antenna model and the realistic antenna model (i.e., the omin-directional model and the iris model) referring to our analysis in Section V-C. It is worth noting that a link can be successfully established only if the SINR at the receiver is larger than a specified threshold. Moreover, in order to validate the effectiveness of the aerial bridge scheme, we compare it with the ground relay scheme and the non-protection scheme. Simulation results are presented as follows.

In Fig. 4, we compare the eavesdropping probability $\mathcal{P}_{\text{eave}}$ under the aerial bridge scheme with that under the non-protection scheme, the ground relay scheme and the UAV jammer scheme. It is worth mentioning that in the UAV jammer scheme, UAVs are randomly deployed on the aerial platform as jammers to disturb the ground eavesdropper. As shown in Fig. 4, markers are the simulation results while curves represent the analytical ones. First, we find that the

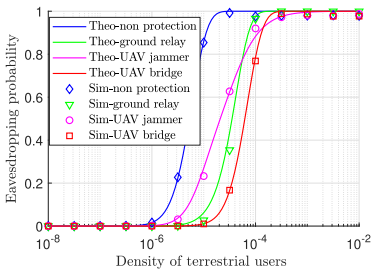


Fig. 4. Eavesdropping probability $\mathcal{P}_{\text{eave}}$ under different schemes.

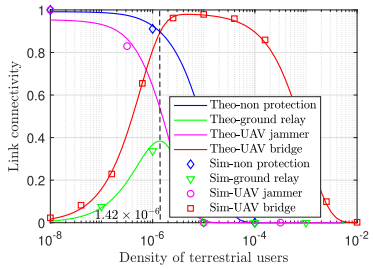
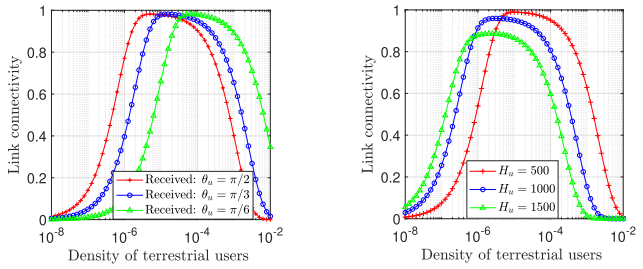


Fig. 5. Link connectivity $\mathcal{P}_{\text{con}}$ under different schemes.

simulation results obey the analytical results, which verifies the accuracy of our theoretical model. Moreover, the eavesdropping probability is increasing with the increment of the density of terrestrial users λ_t. Then, we find that the other three schemes can effectively reduce the eavesdropping probability compared with the non-protection scheme. In fact, legitimated communications can be easily wiretapped by the eavesdroppers, since the eavesdropping probability is always 1 when the density λ_t is large. However, the aerial bridge scheme can nearly achieve better performance (i.e., a lower eavesdropping probability) than ground relay and UAV jammer schemes when the density λ_t increases. Therefore, the aerial bridge scheme can achieve significant effectiveness in the prevention of wiretapping.

Next, we compare the aerial bridge scheme, the ground relay scheme, the UAV jammer scheme and the non-protection scheme in terms of the link connectivity $\mathcal{P}_{\text{con}}$. As shown in Fig. 5, the simulation results also match the analytical ones. Moreover, we find that when $\lambda_t < 1.42 \times 10^{-6}$, the link connectivity under the aerial bridge scheme and ground relay scheme are far below that under the non-protection scheme, because the received interference at the satellite is quite small when the number of terrestrial users is extremely small. Therefore, most terrestrial users can directly establish links with the satellite. However, when $\lambda_t \geq 1.42 \times 10^{-6}$, the aerial bridge scheme can significantly increase the link connectivity while the link connectivity is radically decreased without protection. It means that *the aerial bridge scheme is appropriate for an extremely large number of terrestrial users to assist the construction of legitimate links*. By contrast, we can observe that the ground relay scheme nearly has no assistance in increasing the link connectivity. Meanwhile, combined with the results in Fig. 4, we also find that it is difficult for the UAV jammer scheme to balance low eavesdropping probability and high link connectivity.



(a) $\mathcal{P}_{\text{con}}^{\text{uav}}$ versus θ_u. (b) $\mathcal{P}_{\text{con}}^{\text{uav}}$ versus H_u.

Fig. 6. Link connectivity $\mathcal{P}_{\text{con}}^{\text{uav}}$ with the density of terrestrial users λ_t under different values of the received antenna beamwidth at UAVs θ_u and the deployment height of UAVs H_u.

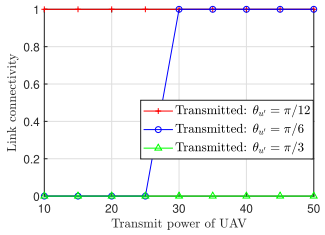


Fig. 7. Link connectivity $\mathcal{P}_{\text{con}}^{\text{uav}}$ versus transmit power of UAVs P_{us} under different transmitted antenna beamwidth at UAVs $\theta_{u'}$.

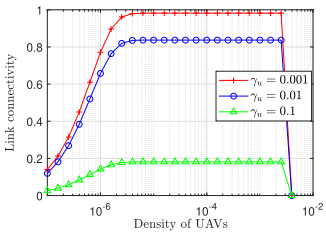


Fig. 8. Link connectivity $\mathcal{P}_{\text{con}}^{\text{uav}}$ versus density of UAVs λ_u.

B. Discussion on Impacts of Parameters

In this subsection, we investigate the impacts of dominating parameter settings of aerial bridges on the link connectivity $\mathcal{P}_{\text{con}}^{\text{uav}}$ and the eavesdropping probability $\mathcal{P}_{\text{eave}}^{\text{uav}}$, respectively. In particular, we discuss the results and provide conducive insights for the practical deployment.

1) Link Connectivity: The link connectivity $\mathcal{P}_{\text{con}}^{\text{uav}}$ is especially related to the deployment of UAVs, including the antenna beamwidth of UAVs θ_u and $\theta_{u'}$, the deployment height of UAVs H_u, the transmit power of UAVs P_{us} and the density of UAVs λ_u.

Fig. 6 plots the analytical results of the link connectivity $\mathcal{P}_{\text{con}}^{\text{uav}}$ against the density of terrestrial users λ_t for different values of the received antenna beamwidth at UAVs θ_u and the deployment height of UAVs H_u. We can observe from Fig. 6 that $\mathcal{P}_{\text{con}}^{\text{uav}}$ first increases with λ_t, then $\mathcal{P}_{\text{con}}^{\text{uav}}$ decreases when λ_t further increasing. Specifically, in Fig. 6(a), we investigate the impacts of θ_u on $\mathcal{P}_{\text{con}}^{\text{uav}}$. First, we can observe that the variation trends of $\mathcal{P}_{\text{con}}^{\text{uav}}$ are almost constant, whatever the values of θ_u are changed. Therefore, in the aerial bridge scheme, *a high link connectivity can be guaranteed by adjusting the received antenna beamwidth at UAVs* when the number of terrestrial users dramatically changes. Furthermore, we analyze the variation of $\mathcal{P}_{\text{con}}^{\text{uav}}$ under different values of H_u in Fig. 6(b). We find when the density of terrestrial users is extremely

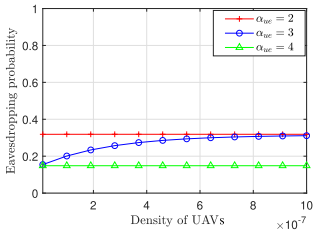


Fig. 9. Eavesdropping probability $\mathcal{P}_{\text{eave}}^{\text{con}}$ versus the density of UAVs λ_u under different values of path loss factor α_{ue}.

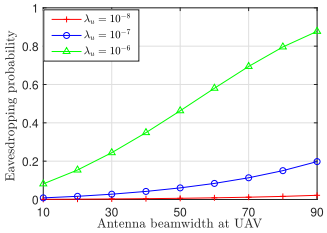


Fig. 10. Avesdropping probability $\mathcal{P}_{\text{eave}}^{\text{uav}}$ versus received antenna beamwidth at UAVs θ_u under different values of density of UAVs λ_u.

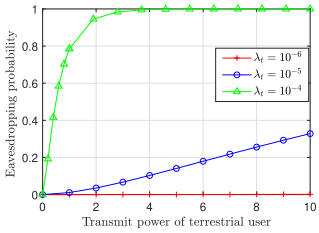
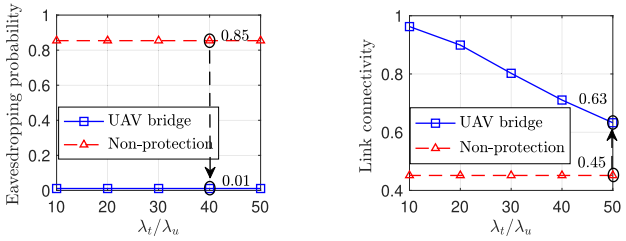


Fig. 11. Eavesdropping probability $\mathcal{P}_{\text{eave}}^{\text{uav}}$ versus transmit power of a terrestrial user P_{tu} under different values of density of terrestrial users λ_t.



(a) $\mathcal{P}_{\text{eave}}^{\text{uav}}$ and $\mathcal{P}_{\text{eave}}^{\text{non}}$. (b) $\mathcal{P}_{\text{con}}^{\text{uav}}$ and $\mathcal{P}_{\text{con}}^{\text{non}}$.

Fig. 12. Performance of UAV bridge scheme under different λ_t/λ_u.

low, increasing H_u can achieve a high $\mathcal{P}_{\text{con}}^{\text{uav}}$. Similarly, *in the aerial bridge scheme, the link connectivity can be significantly improved by decreasing* H_u, when there are a number of terrestrial users in the network.

Fig. 7 demonstrates the effects of the transmitted antenna beamwidth at UAVs $\theta_{u'}$ and the transmit power of UAVs P_{us} on the link connectivity $\mathcal{P}_{\text{con}}^{\text{uav}}$. According to (33), P_{us} and $\theta_{u'}$ are two vital factors which decide the connectivity of the high-altitude link $\mathcal{P}_{us}$, and then, further dominate the value of $\mathcal{P}_{\text{con}}^{\text{uav}}$. Thus, as shown in Fig. 7, the increment of P_{us} can significantly improve the link connectivity. In addition, when the reduction of $\theta_{u'}$ makes a UAV obtain a larger main lobe gain (i.e., $\theta_{u'} = \pi/12$), the value of $\mathcal{P}_{\text{con}}^{\text{uav}}$ is almost constant whatever P_{us} is changed. Therefore, for the aerial bridge scheme, *both decreasing transmitted antenna beamwidth of UAVs and increasing transmit power of UAVs can achieve a high link connectivity*.

Furthermore, we analyze the impact of the density of UAVs λ_u on the link connectivity $\mathcal{P}_{\text{con}}^{\text{uav}}$ under different SINR thresholds at UAVs γ_u. As shown in Fig. 8, the curves of $\mathcal{P}_{\text{con}}^{\text{uav}}$ rise first and then almost keep constant. When λ_u further increases, the values of $\mathcal{P}_{\text{con}}^{\text{uav}}$ finally drop down to 0. The reason is that the increment of λ_u can cause a large number of UAVs, resulting in extra cumulative interference I_{us}. According to (27) and (33), when I_{us} increases to a threshold value, $\mathcal{P}_{us}$ then experiences a sudden drop from a positive value to zero, since the legitimate link between the UAV and the satellite cannot be established. Thus, the unrestricted increment of the number of UAVs cannot benefit the improvement of the link connectivity. Meanwhile, we can observe that the value of $\mathcal{P}_{\text{con}}^{\text{uav}}$ is much higher, with a lower SINR threshold γ_u. Consequently, *the proposed scheme can improve the link connectivity by decreasing the SINR threshold at UAVs*, when the number of UAVs in the network is limited.

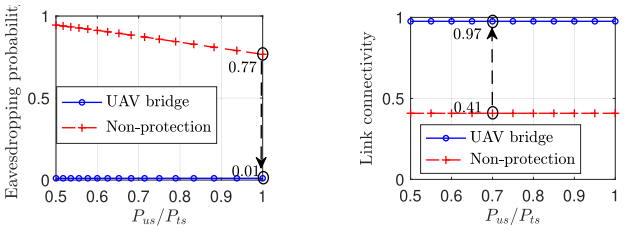
2) Eavesdropping Probability: We further analyze the influence of the dominating parameters on the eavesdropping probability. Fig. 9 demonstrates the eavesdropping probability $\mathcal{P}_{\text{eave}}^{\text{uav}}$ varies with the density of UAVs λ_u under different path-loss factors α_{ue}. As shown in Fig. 9, the curve of $\alpha_{ue} = 3$ rises first, and then gradually tends to be flat as λ_u increases. By contrast, when $\alpha_{ue} = 2$, the values of $\mathcal{P}_{\text{eave}}^{\text{uav}}$ are almost stable. When $\alpha_{ue} = 4$, the eavesdropper cannot wiretap any confidential information through the low-altitude link whatever the density λ_u is changed. Obviously, *the aerial bridge scheme can significantly reduce the eavesdropping probability* under most channel conditions.

In Fig. 10, we analyze the impact of the received antenna beamwidth at UAV θ_u on the eavesdropping probability $\mathcal{P}_{\text{eave}}^{\text{uav}}$ under the different density of UAVs λ_u. First, we find that the curves of $\mathcal{P}_{\text{eave}}^{\text{uav}}$ are rising as θ_u increases. Moreover, the value of $\mathcal{P}_{\text{eave}}^{\text{uav}}$ under a lower density of UAVs (i.e., $\lambda_u = 10^{-8}$) is much smaller than $\mathcal{P}_{\text{eave}}^{\text{uav}}$ under a higher λ_u. Meanwhile, as λ_u increases from 10^{-7} to 10^{-6}, the increment of $\mathcal{P}_{\text{eave}}^{\text{uav}}$ is particularly obvious. Therefore, *the aerial bridge scheme can reduce the eavesdropping probability by narrowing the received antenna beamwidth at UAVs*, especially, when there are a large number of UAVs deployed in TSNs.

Fig. 11 plots the eavesdropping probability $\mathcal{P}_{\text{eave}}^{\text{uav}}$ versus the transmit power of terrestrial users P_{tu}. We can find that $\mathcal{P}_{\text{eave}}^{\text{uav}}$ increases with the transmit power P_{tu}. Meanwhile, the increment of terrestrial users also influences the eavesdropping probability. Specifically, when the density of users is large (i.e., $\lambda_t = 10^{-4}$), the eavesdropper has more opportunities to wiretap confidential information, resulting in a higher eavesdropping probability. However, the eavesdropping probability can be significantly decreased by reducing the transmit power of terrestrial users. To conclude, the aerial bridge scheme is also appropriate for a large number of terrestrial users to *guarantee the security of transmission by properly controlling transmit power.*

C. Discussion on the Deployment of UAV Bridges

In Fig. 12, we analyze the performance of the UAV bridge scheme under different λ_t/λ_u. Particularly, we compare the eavesdropping probability and link connectivity of the UAV



(a) $\mathcal{P}_{\text{eave}}^{\text{uav}}$ and $\mathcal{P}_{\text{eave}}^{\text{non}}$. (b) $\mathcal{P}_{\text{con}}^{\text{uav}}$ and $\mathcal{P}_{\text{con}}^{\text{non}}$.

Fig. 13. Performance of UAV bridge scheme under different P_{us}/P_{ts}.

bridge scheme with those of the non-protection scheme. Herein, we fix the density of terrestrial users λ_t as 10^{-5}, while the density of UAVs λ_u is reduced as the ratio λ_t/λ_u increases. As shown in Fig. 12(a), the eavesdropping probability of the UAV bridge scheme is relatively stable for different λ_t/λ_u, because it is difficult for the eavesdropper to wiretap the confidential information leakage from the side/back lobe of antennas at the UAV. In addition, the UAV bridge scheme can significantly reduce the eavesdropping probability (i.e., from 0.85 to 0.01), since terrestrial users communicate with a low transmit power. Fig. 12(b) plots the link connectivity of the UAV bridge scheme versus the ratio λ_t/λ_u. We can find that $\mathcal{P}_{\text{con}}^{\text{uav}}$ decreases with the increment of λ_t/λ_u. Nonetheless, our scheme still performs advancements in improving link connectivity.

As shown in Fig. 13, we then discuss the performance of the UAV bridge scheme under different P_{us}/P_{ts}. Specifically, we fix the transmit power of terrestrial users to the satellite P_{us}(in the non-protection scheme), while the transmit power of UAVs P_{us} increased with the increment of the ratio P_{us}/P_{ts}. In Fig. 13(a), we can find that the eavesdropping probability is reduced as P_{us}/P_{ts}, it is because a larger value of P_{us} makes eavesdroppers more opportunities to wiretap confidential information from UAVs. Moreover, the increased value of P_{us} cannot significantly increase the link connectivity, as the link connectivity is relatively stable in Fig. 13(b). Compared with transmit power for the non-protection scheme, i.e., P_{ts}, UAV bridges can significantly save the transmit power. Consequently, the reasonable transmit power is necessary for UAV bridges, excessive increment of P_{us} can make extra confidential information leakage while cannot enhance the link connectivity.

D. Discussion on Distribution and Antenna Model

To track the accuracy of our network model, we evaluate the theoretical model by simulating the distribution of terrestrial users and the radiation pattern of antennas.

As shown in Fig. 14, we simulate the distribution of terrestrial users following the Poisson point process (PPP) and the Poisson cluster process (PCP), respectively. Comparing PPP (depicted in Fig. 14(a)) with PCP (depicted in Fig. 14(b)), we can find that there are unobvious differences between their distributions, especially for TSNs with an extremely long transmission distance. To further investigate the effect of the distribution model on the performance of UAV bridges, we analyze the eavesdropping probability and the link connectivity under different models, as shown in Fig. 15.

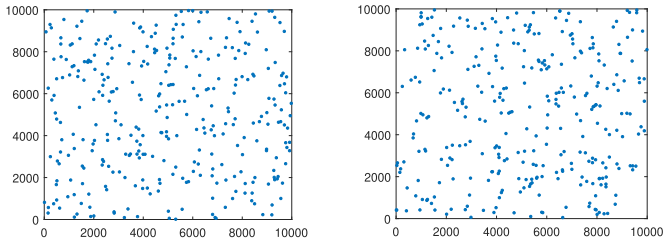
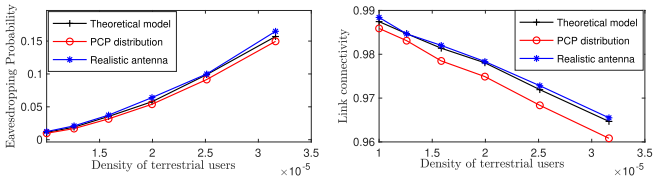
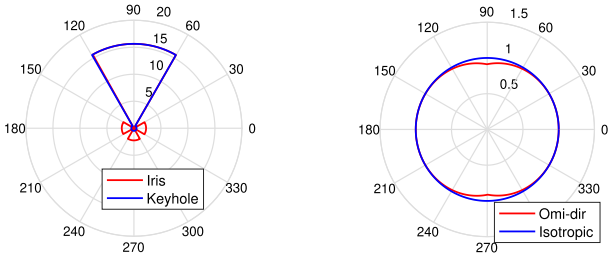


Fig. 14. Distribution of terrestrial users.



(a) Simulations of eavesdropping probability. (b) Simulations of connectivity.

Fig. 15. Performance under different network model (i.e., PPP verses PCP) and antenna model (i.e., keyhole verses iris).



(a) Omni-directional antenna. (b) Directional antenna.

Fig. 16. Radiation pattern of antennas.

Note that, in our theoretical model (i.e., the red curve), we adopt PPP as the distribution of terrestrial users. Compared with the performance of our analysis with aerial bridge under the PPP model, the illustrated performance under the PCP model (i.e., blue curve) has quite slight differences.

Moreover, we analyze the impacts of the antenna models on the performance of our aerial bridge. Owing to the integration of antenna elements, forming an antenna array, such as the uniform plane array (UPA). There will be an inevitable difference in phase and amplitude because of the various positions of elements, resulting in different antenna gains for different directions. As shown in Fig. 16, we simulate the radiation patterns of the omni-directional antenna model in Fig. 16(a). Then, we model the radiation patterns of directional antenna as illustrated in Fig. 16(b). We can find that there are different antenna gains at different directions. In order to evaluate the impact of antenna models, we conduct simulations on the eavesdropping probability and the link connectivity. In our theoretical model, we adopt the isotropic antenna and the keyhole as antenna models. As shown in Fig. 15, we can find that adopting both the realistic antenna models (i.e., omni-directional antenna and iris models) and idealistic antenna model (i.e., isotropic model and keyhole model) demonstrates the effectiveness of our aerial bridge, since the difference between them is little obvious for both the eavesdropping probability and the link connectivity.

VI. Conclusion

In this paper, we presented an aerial bridge scheme for TSNs in the presence of secret eavesdroppers. To evaluate the eavesdropping risk, we introduced the eavesdropping probability. Additionally, the link connectivity was investigated to validate the reliability of the proposed scheme. We conducted extensive simulations to verify the effectiveness of the aerial bridge scheme. Meanwhile, we compared the performance of our scheme with that of the ground relay, UAV jammer and non-protection schemes. The simulation results revealed that the aerial bridge scheme outperforms the others in terms of decreasing the eavesdropping probability. Moreover, they also verified that our scheme can significantly improve the link connectivity. Further, we discussed the impacts of parameters on the eavesdropping probability and the link connectivity, respectively. The results provided useful insights on the practical deployment of TSNs under the aerial bridge scheme.

Appendix A
Proof of Lemma 3

Note that I_{us} is composed of the main lobe interference I_{us}^m and the side/back lobe interference I_{us}^b. Only if more than one UAV appears in a given region, the interference exists. Therefore, we need to calculate the probabilities that the interfering UAVs appear in the coverage region of the main lobe and the side/back lobe, respectively. Because the UAVs are randomly distributed on the aerial platform, we have the probability that the interfering UAVs appear in the coverage region of the main lobe at the satellite denoted by $\mathcal{P}_{in,u}$, which can be calculated as

$$\begin{aligned}\mathcal{P}_{in,u}(x) &= \mathbb{P}[x \geq 2] = 1 - \mathbb{P}[x=0] - \mathbb{P}[x=1] \\ &= 1 - (1+\lambda_u A_s)\exp(-\lambda_u A_s), \end{aligned} \tag{44}$$

where x is the number of UAVs appearing in the coverage region of the main lobe at the satellite, while $A_s = \pi\left((H_s - H_u)\tan\frac{\theta_s}{2}\right)^2$ denotes the area of a such coverage region.

According to (4), the interference transmitted from a UAV is $P_{us}G_u^m G_s^m l_{us}^{-\alpha_{us}}$. Therefore, the main lobe interference at the satellite from a UAV is calculated by $\mathcal{P}_{in,u}P_{us}G_u^m G_s^m l_{us}^{-\alpha_{us}}$. Then, we can express the main lobe interference I_{us}^m as

$$\begin{aligned} I_{us}^m &= \mathbb{E}\left[\sum_{j\in\Phi_{A_s}} \mathcal{P}_{in,u}P_{us}G_u^m G_s^m l_{js}^{-\alpha_{us}}\right] \\ &= 2\left(\lambda_u \pi D_I\right)^2 \times \mathcal{P}_{in,u}P_{us}G_u^m G_s^m \\ &\quad \times \int_0^{D_I} \left((H_s - H_u)^2 + d_{js}^2\right)^{-\frac{\alpha_{us}}{2}} \mathrm{e}^{-\lambda_u \pi d_{js}^2} d_{js}\mathbf{d}d_{js}. \end{aligned} \tag{45}$$

where $D_I = \min\left\{\left(P_{us}G_u^m G_s^m/\eta_s\right)^{1/\alpha_{us}}, (H_s - H_u)\tan\theta_s/2\right\}$ denotes the interfering range of the main lobe, η_s is the threshold of received power at the satellite, and d_{js} denotes the projection distance between the j-th UAV and the satellite. Following the similar derivation of I_{us}^m, the side/back lobe interference I_{us}^b can be expressed as

$$\begin{aligned} I_{us}^b &= \mathbb{E}\left[\sum_{j\in\Phi_{A_{s'}}} \mathcal{P}_{in,u'}P_{us}G_u^m G_s^b l_{js}^{-\alpha_{us}}\right] \\ &= 2\pi\lambda_u^2 A_{s'} \times \mathcal{P}_{in,u'}P_{us}G_u^m G_s^b \\ &\quad \times \int_{(H_s - H_u)\tan\frac{\theta_s}{2}}^{\left(\frac{P_{us}G_u^m G_s^b}{\eta_s}\right)^{\frac{1}{\alpha_{us}}}} \\ &\quad \times \left((H_s - H_u)^2 + d_{js}^2\right)^{-\frac{\alpha_s}{2}} \mathrm{e}^{-\lambda_u \pi d_{js}^2} d_{js}\mathbf{d}d_{js}. \end{aligned} \tag{46}$$

Unlike the main lobe, the side/back lobe at the satellite has diverse gains under the different models. Specifically, the keyhole model consisting of a joint side/back lobe, can theoretically achieve full coverage of the aerial platform (or ground). In this case, the probability that the interfering UAVs are covered by the side/back lobe $\mathcal{P}_{in,u'}$ is equal to 1. For the iris model consisting of several side/back lobes, referring to (18), $\mathcal{P}_{in,u'}$ can be given as

$$\begin{aligned}\mathcal{P}_{in,u'} &= \mathbb{P}\left[\frac{\pi-\theta_s}{2} - (\psi_s + \theta_s) \leq \phi \leq \frac{\pi-\theta_s}{2} - \psi_s\right] \\ &= F_{\phi_d}\left(\frac{\pi-\theta_s}{2} - \psi_s\right) - F_{\phi_d}\left(\frac{\pi-\theta_s}{2} - (\psi_s+\theta_s)\right) \\ &= \frac{\tan\left(\frac{\pi-\theta_s}{2} - \psi_s\right) - \tan\left(\frac{\pi-3\theta_s}{2} - \psi_s\right)}{2\sqrt{\lambda_u}\left(H_{u,\max} - H_{u,\min}\right)}, \end{aligned}$$

where the solid angle between any two neighbor lobes of the satellite antenna is $\psi_s = \frac{4\pi}{N_s+1} - 2\pi\left(1-\cos\frac{\theta_s}{2}\right)$, N_s denotes the number of side/back lobes at the satellite. However, not all UAVs can effectively interfere with the satellite due to the limitation of receiver sensitivity. Therefore, the actual area of the region covered by the side/back lobe $A_{s'}$ is expressed as

$$A_{s'} = \pi \times \left(\left(\frac{P_{us}G_u^m G_s^b}{\eta_s}\right)^{\frac{2}{\alpha_{us}}} - \left((H_s - H_u)\tan\frac{\theta_s}{2}\right)^2\right)^+, \tag{47}$$

where $(x)^+ = \max\{x, 0\}$, normalizing $A_{s'}$ to be non-negative. To sum up, the cumulative interference I_{us} under the keyhole model can be expressed as $I_{us} = I_{us}^m + \upsilon I_{us}^b$, where $\upsilon = \{0, 1\}$ stands for different cases of interference shown as follows.

Case 1: When the maximum interfering distance of the main lobe is no larger than the maximum coverage range of the main lobe, i.e., $\left(P_{us}G_u^m G_s^m/\eta_s\right)^{1/\alpha_{us}} \leq (H_s - H_u)\tan\frac{\theta_s}{2}$, the interference from UAVs can only be received by the main lobe of the satellite (i.e., $\upsilon = 0$).

Case 2: When the maximum interfering distance of the main lobe is larger than the maximum coverage range of the satellite, i.e., $\left(P_{us}G_u^m G_s^m/\eta_s\right)^{1/\alpha_{us}} > (H_s - H_u)\tan\frac{\theta_s}{2}$, and the maximum interfering distance of the side/back lobes is no larger than the maximum coverage range of the satellite, i.e., $\left(P_{us}G_u^m G_s^b/\eta_s\right)^{1/\alpha_{us}} \leq (H_s - H_u)\tan\frac{\theta_s}{2}$, the interference from UAVs can only be received by the main lobe of the satellite (i.e., $\upsilon = 0$).

Case 3: When the maximum interfering distance of the main lobe is larger than the maximum coverage range of the satellite, i.e., $\left(P_{us}G_u^m G_s^m/\eta_s\right)^{1/\alpha_{us}} > (H_s - H_u)\tan\frac{\theta_s}{2}$, and

the maximum interfering distance of the side/back lobes is larger than the maximum coverage range of the satellite, i.e., $\left(P_{us}G_u^m G_s^b/\eta_s\right)^{1/\alpha_{us}} > (H_s - H_u)\tan\frac{\theta_s}{2}$, the interference from UAVs can be received by both the main lobe and the side/back lobes of the satellite. (i.e., $v = 1$).

Note that for *Case 3*, not all UAVs can interfere with the satellite if the antenna deploys iris model, $A_{s'}$ should be rewritten as

$$A_{s'} = \frac{\pi N_s (H_s - H_u)^2 \tan(\theta_s/2)(\tan(\psi_s + \theta_s) - \tan(\theta_s))}{\cos(\psi_s + \theta_s/2)}. \tag{48}$$

Finally, the received cumulative interference of the satellite from UAVs I_{us} can be obtained.

Appendix B
Proof of Lemma 4

Since the direct link is suffered by heavy shadowing fading and attenuation, the terrestrial users' interference received by the side/back lobes at the satellite is extremely low. Therefore, we only take the cumulative interference from terrestrial users received by the main lobes at the satellite into consideration. When the threshold of received power at the satellite is η_s, we can obtain the maximum interfering distance between an effective interfering user and the satellite, similar to (9). We further denote that the interfering region is deemed as a circle with a radius of the maximum interfering distance. Then, we have the area of the interfering region denoted by A_I as

$$A_I = \pi \min\left\{\left(\frac{P_{ts}G_s^m G_t h_{ts}}{\eta_s}\right)^{\frac{2}{\alpha_{ts}}} - H_s^2, \left(H_s \tan\left(\frac{\theta_s}{2}\right)\right)^2\right\}, \tag{49}$$

where $G_t = \int_{H_s}^{\frac{H_s}{\cos(\theta_s/2)}} 10^{-1.2\arcsin^2(\frac{H_s}{l_{ts}})/\phi_{3\mathrm{dB}}^2} f_{l_{ts}}(x)\mathbf{d}x$, and θ_s is the main lobe beamwidth at the satellite. Referring to the similar derivation procedure of The PDF of ϕ_d, we can obtain the PDF of the elevation angle at the terrestrial user ϕ_o by

$$f_{\phi_o}(\phi) = -\frac{2\pi\lambda_t H_s^2 \cos\phi}{\sin^3\phi}\exp\left(-\frac{\pi\lambda_t H_s^2}{\sin^3\phi}\right). \tag{50}$$

Then, the probability that the interfering users appear in the coverage region of the main lobe at the satellite is expressed as

$$\begin{aligned}\mathcal{P}_{in,s} &= \mathbb{P}[\phi_o > \frac{\pi-\theta_s}{2}] = 1 - \mathbb{P}[\phi_o \le \frac{\pi-\theta_s}{2}] \\ &= 1 - F_{\phi_o}(\frac{\pi-\theta_s}{2}) = 1 - \int_0^{\frac{\pi-\theta_s}{2}} f_{\phi_o}(\phi)\mathrm{d}\phi \\ &= 1 + \int_0^{\frac{\pi-\theta_s}{2}} \frac{2\pi\lambda_t H_s^2\cos\phi}{\sin^3\phi}\exp\left(-\frac{\pi\lambda_t H_s^2}{\sin^3\phi}\right)\mathrm{d}\phi.\end{aligned}$$

The average free-space path loss for the interfering signal, denoted by $\overline{L_{ts}}$, can be calculated as

$$\overline{L_{ts}} = \int_{H_s}^{\frac{H_s}{\cos(\theta_s/2)}} x^{-\alpha_{ts}} f_{l_{ts}}(x)\,\mathbf{d}x. \tag{51}$$

Unlike the derivation of I_{us}, for the cumulative interference from terrestrial users I_{ts}, we first give the PDF of the received power at the satellite referring to (5) and (6) as

$$\begin{aligned}f_R(x) = &\frac{1}{2\rho P_{ts}\overline{L_{ts}}G_s^m G_t}\left(\frac{2\rho m}{2\rho m+\Omega}\right)^m \\ &\times \exp\left(-\frac{x}{2\rho P_{ts}\overline{L_{ts}}G_s^m G_t}\left(1 - \frac{\Omega}{2\rho m+\Omega}\right)\right) \\ &\times \sum_{n=0}^{m-1}\frac{(1-m)_n}{(n!)^2}\left(-\frac{\Omega x}{2\rho P_{ts}\overline{L_{ts}}G_s^m G_t(2\rho m+\Omega)}\right)^n.\end{aligned} \tag{52}$$

Then, the cumulative interference I_{ts} can be expressed as

$$\begin{aligned}I_{ts} &= \mathbb{E}_{t\in\Phi_{A_I}}\left[\sum \mathcal{P}_{in,s}P_{ts}G_s^m G_t h_{ts}\overline{L_{ts}}\right] \\ &= \lambda_t A_I \times \mathcal{P}_{in,s}P_{ts}\overline{L_{ts}}G_s^m G_t (2\rho)^{m-1}(m(2\rho m+\Omega))^{m-2} \\ &\quad\times \sum_{n=0}^{m-1}\frac{(1-m)_n}{(n!)^2}\left(-\frac{\Omega}{2\rho P_{ts}\overline{L_{ts}}G_s^m G_t}\right)^n \Gamma(n+2)m^{-n}.\end{aligned} \tag{53}$$

Particularly, we categorize cases of the fading severity parameter m (within the range of $[0,\infty)$) as follows.

Case 1: When $m = 0$, h_{d} can be simplified as the Rayleigh distribution, the PDF of h_{d} presented in (6) is further expressed as

$$f_{h_{\mathrm{d}}}(x) = \frac{1}{\rho}\exp\left(-\frac{x}{2\rho}\right). \tag{54}$$

Then, the PDF of the received power is given as follows,

$$f_R(x) = \frac{1}{2\rho P_{ts}\overline{L_{ts}}G_s^m G_t}\exp\left(-\frac{x}{2\rho P_{ts}\overline{L_{ts}}G_s^m G_t}\right), \tag{55}$$

and the cumulative interference at the satellite is given by

$$\begin{aligned}I_{ts} = &\lambda_t\pi\min\left\{\left(\frac{P_{ts}G_s^m G_t h_{ts}}{\eta_s}\right)^{\frac{2}{\alpha_{ts}}} \right. \\ &\left. - H_s^2, \left(H_s\tan\left(\frac{\theta_s}{2}\right)\right)^2\right\} \\ &\times \mathcal{P}_{in,s}\int_0^\infty \frac{x}{2\rho P_{ts}\overline{L_{ts}}G_s^m G_t} \\ &\times \exp\left(-\frac{x}{2\rho P_{ts}\overline{L_{ts}}G_s^m G_t}\right)\mathbf{d}x.\end{aligned} \tag{56}$$

Case 2: When $m = \infty$, the h_{d} follows the Rician distribution, then its PDF is expressed as

$$f_{h_{\mathrm{d}}}(x) = \frac{1}{\rho}\exp\left(-\frac{x+\Omega}{2\rho}\right)I_0\left(\frac{\sqrt{\Omega}}{\rho}\right), \tag{57}$$

where $I_n(\cdot)$ is the n th-order modified Bessel function of the first kind. The PDF of the received power is given as follows,

$$\begin{aligned}f_R(x) = &\frac{1}{2\rho P_{ts}\overline{L_{ts}}G_s^m G_t} \\ &\times \exp\left(-\frac{x}{2\rho P_{ts}\overline{L_{ts}}G_s^m G_t} - \frac{\Omega}{2\rho}\right)I_0\left(\frac{\sqrt{\Omega}}{\rho}\right),\end{aligned} \tag{58}$$

and the cumulative interference at the satellite are calculated by

$$I_{ts} = \lambda_t \pi \min\left\{\left(\frac{P_{ts}G_s^m G_t h_{ts}}{\eta_s}\right)^{\frac{2}{\alpha_{ts}}} - H_s^2, \left(H_s \tan\left(\frac{\theta_s}{2}\right)\right)^2\right\} \times \mathcal{P}_{in,s}\int_0^\infty \frac{x}{2\rho P_{ts}\overline{L_{ts}}G_s^m G_t}\exp\left(-\frac{x}{2\rho P_{ts}\overline{L_{ts}}G_s^m G_t}\right)\mathbf{d}x \times I_0\left(\frac{\sqrt{\Omega}}{\rho}\right)\exp\left(-\frac{\Omega}{2\rho}\right). \quad (59)$$

REFERENCES

[1] J. Liu, Y. Shi, Z. M. Fadlullah, and N. Kato, "Space-air-ground integrated network: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2714–2741, 4th Quart., 2018.

[2] P. K. Sharma and D. I. Kim, "Secure 3D mobile UAV relaying for hybrid satellite-terrestrial networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 4, pp. 2770–2784, Apr. 2020.

[3] C. D. V. Bankey and P. K. Upadhyay, "Physical layer security in hybrid satellite-terrestrial relay networks," in *Physical Layer Security*. Cham, Switzerland: Springer, Jan. 2021.

[4] Y. Zhang, J. Ye, G. Pan, and M.-S. Alouini, "Secrecy outage analysis for satellite-terrestrial downlink transmissions," *IEEE Wireless Commun. Lett.*, vol. 9, no. 10, pp. 1643–1647, Oct. 2020.

[5] S. Hong, C. Pan, H. Ren, K. Wang, and A. Nallanathan, "Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface," *IEEE Trans. Commun.*, vol. 68, no. 12, pp. 7851–7866, Sep. 2020.

[6] A. Roy-Chowdhury, J. S. Baras, M. Hadjitheodosiou, and S. Papademetriou, "Security issues in hybrid networks with a satellite component," *IEEE Wireless Commun.*, vol. 12, no. 6, pp. 50–61, Dec. 2005.

[7] H. Cruickshank, M. P. Howarth, S. Iyengar, Z. Sun, and L. Claverotte, "Securing multicast in DVB-RCS satellite systems," *IEEE Wireless Commun.*, vol. 12, no. 5, pp. 38–45, Oct. 2005.

[8] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-layer security in space information networks: A survey," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 33–52, Jan. 2020.

[9] 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.

[10] Z. Lin, M. Lin, W.-P. Zhu, J.-B. Wang, and J. Cheng, "Robust secure beamforming for wireless powered cognitive satellite-terrestrial networks," *IEEE Trans. Cognit. Commun. Netw.*, vol. 7, no. 2, pp. 567–580, Jun. 2021.

[11] X. Chen et al., "Multi-antenna covert communication via full-duplex jamming against a warden with uncertain locations," *IEEE Trans. Wireless Commun.*, vol. 20, no. 8, pp. 5467–5480, Aug. 2021.

[12] C. Liu, N. Yang, R. Malaney, and J. Yuan, "Artificial-noise-aided transmission in multi-antenna relay wiretap channels with spatially random eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7444–7456, Nov. 2016.

[13] B. Li, M. Zhang, Y. Rong, and Z. Han, "Artificial noise-aided secure relay communication with unknown channel knowledge of eavesdropper," *IEEE Trans. Wireless Commun.*, vol. 20, no. 5, pp. 3168–3179, May 2021.

[14] V. Bankey and P. K. Upadhyay, "Physical layer security of multiuser multirelay hybrid satellite-terrestrial relay networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2488–2501, Mar. 2019.

[15] S. Yan, X. Wang, Z. Li, B. Li, and Z. Fei, "Cooperative jamming for physical layer security in hybrid satellite terrestrial relay networks," *China Commun.*, vol. 16, no. 12, pp. 154–164, Dec. 2019.

[16] K. Guo, "Performance analysis of hybrid satellite-terrestrial cooperative networks with relay selection," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 9053–9067, Aug. 2020.

[17] J. Li, S. Han, X. Tai, C. Gao, and Q. Zhang, "Physical layer security enhancement for satellite communication among similar channels: Relay selection and power allocation," *IEEE Syst. J.*, vol. 14, no. 1, pp. 433–444, Mar. 2020.

[18] Z. Yin et al., "UAV-assisted physical layer security in multi-beam satellite-enabled vehicle communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2739–2751, Mar. 2022.

[19] X. Pang, M. Liu, N. Zhao, Y. Chen, Y. Li, and F. R. Yu, "Secrecy analysis of UAV-based mmWave relaying networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 8, pp. 4990–5002, Aug. 2021.

[20] C. Liao, K. Xu, H. Zhu, X. Xia, Q. Su, and N. Sha, "Secure transmission in satellite-UAV integrated system against eavesdropping and jamming: A two-level Stackelberg game model," *China Commun.*, vol. 19, no. 7, pp. 53–66, Jul. 2022.

[21] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Trans. Commun.*, vol. 59, no. 11, pp. 3122–3134, Nov. 2011.

[22] M. Di Renzo and P. Guan, "Stochastic geometry modeling and system-level analysis of uplink heterogeneous cellular networks with multi-antenna base stations," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2453–2476, Jun. 2016.

[23] K. M. S. Huq, J. Rodriguez, and I. E. Otung, "3D network modeling for THz-enabled ultra-fast dense networks: A 6G perspective," *IEEE Commun. Standards Mag.*, vol. 5, no. 2, pp. 84–90, Jun. 2021.

[24] T. S. P. See, X. Qing, Z. N. Chen, and Z. N. Chen, "A wideband horizontally polarized omnidirectional antenna," in *Proc. IEEE 4th Asia–Pacific Conf. Antennas Propag. (APCAP)*, Kuta, Indonesia, Sep. 2015, pp. 294–295.

[25] C. D. Vilor and H. Jafarkhani, "Optimal 3D-UAV trajectory and resource allocation of DL UAV-GE links with directional antennas," in *Proc. GLOBECOM-IEEE Global Commun. Conf.*, Dec. 2020, pp. 1–6.

[26] V. Petrov, J. Kokkoniemi, D. Moltchanov, J. Lehtomaki, M. Juntti, and Y. Koucheryavy, "The impact of interference from the side lanes on mmWave/THz band V2V communication systems with directional antennas," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 5028–5041, Jun. 2018.

[27] H.-N. Dai, K.-W. Ng, and M.-Y. Wu, "On busy-tone based MAC protocol for wireless networks with directional antennas," *Wireless Pers. Commun.*, vol. 73, no. 3, pp. 611–636, Dec. 2013.

[28] C. A. Balanis, *Antenna Theory: Analysis and Design*. Hoboken, NJ, USA: Wiley, 2015.

[29] M. Banagar and H. S. Dhillon, "3D two-hop cellular networks with wireless backhauled UAVs: Modeling and fundamentals," *IEEE Trans. Wireless Commun.*, vol. 21, no. 8, pp. 6417–6433, Aug. 2022.

[30] Q. Wang, H.-N. Dai, Q. Wang, M. K. Shukla, W. Zhang, and C. G. Soares, "On connectivity of UAV-assisted data acquisition for underwater Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5371–5385, Jun. 2020.

[31] Q. Wang, H.-N. Dai, Z. Zheng, M. Imran, and A. V. Vasilakos, "On connectivity of wireless sensor networks with directional antennas," *Sensors*, vol. 17, no. 1, p. 134, 2017. [Online]. Available: https://www.mdpi.com/1424-8220/17/1/134

[32] Y. Zhu, G. Zheng, and M. Fitch, "Secrecy rate analysis of UAV-enabled mmWave networks using Matérn hardcore point processes," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1397–1409, Jul. 2018.

[33] X. Pang, M. Sheng, N. Zhao, J. Tang, D. Niyato, and K.-K. Wong, "When UAV meets IRS: Expanding air-ground networks via passive reflection," *IEEE Wireless Commun.*, vol. 28, no. 5, pp. 164–170, Oct. 2021.

[34] H. Inaltekin, M. Chiang, H. V. Poor, and S. B. Wicker, "On unbounded path-loss models: Effects of singularity on wireless network performance," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1078–1092, Sep. 2009.

[35] G. Noh, H. Chung, and I. Kim, "Outage analysis for terrestrial-satellite spectrum sharing," *IEEE Commun. Lett.*, vol. 24, no. 10, pp. 2280–2284, Oct. 2020.

[36] 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.

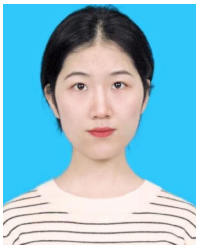
[37] D. Zwillinger and A. Jeffrey, *Table of Integrals, Series, and Products*, 7th ed. Amsterdam, The Netherlands: Academic, 2007.

[38] V. Bankey and P. K. Upadhyay, "Secrecy outage analysis of hybrid satellite-terrestrial relay networks with opportunistic relaying schemes," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Jun. 2017, pp. 1–5.

[39] M. Lin, Y.-W. Jiang, J. Ouyang, and K. An, "The performance of a hybrid satellite-terrestrial cooperative networks with interferences," *Acta Polym. Sin.*, vol. 46, no. 1, pp. 8–14, Jan. 2018.

[40] W. Sun and J. Liu, "2-to-M coordinated multipoint-based uplink transmission in ultra-dense cellular networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8342–8356, Dec. 2018.
[41] Q. Wang, H.-N. Dai, O. Georgiou, Z. Shi, and W. Zhang, "Connectivity of underlay cognitive radio networks with directional antennas," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7003–7017, Aug. 2018.
[42] Y. Wang et al., "Joint resource allocation and UAV trajectory optimization for space–air–ground Internet of remote things networks," *IEEE Syst. J.*, vol. 15, no. 4, pp. 4745–4755, Dec. 2021.
[43] P. K. Sharma, P. K. Upadhyay, D. B. Da Costa, P. S. Bithas, and A. G. Kanatas, "Performance analysis of overlay spectrum sharing in hybrid satellite-terrestrial systems with secondary network selection," *IEEE Trans. Wireless Commun.*, vol. 16, no. 10, pp. 6586–6601, Oct. 2017.
[44] C. Liu, W. Feng, Y. Chen, C.-X. Wang, and N. Ge, "Optimal beamforming for hybrid satellite terrestrial networks with nonlinear PA and imperfect CSIT," *IEEE Wireless Commun. Lett.*, vol. 9, no. 3, pp. 276–280, Mar. 2020.
[45] M. S. Alam, G. K. Kurt, H. Yanikomeroglu, P. Zhu, and N. D. Dao, "High altitude platform station based super macro base station constellations," *IEEE Commun. Mag.*, vol. 59, no. 1, pp. 103–109, Jan. 2021.
[46] Z. Tang, H. Zhou, T. Ma, K. Yu, and X. S. Shen, "Leveraging LEO assisted cloud-edge collaboration for energy efficient computation offloading," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2021, pp. 1–6.

Qubeijian Wang (Member, IEEE) received the B.E. degree in electrical engineering from Xi'an Jiaotong-Liverpool University, Suzhou, China, and the University of Liverpool, Liverpool, U.K., in 2015, the M.E. degree in telecommunications from the University of Melbourne, Parkville, VIC, Australia, in 2017, and the Ph.D. degree in electronic information technology from the Macau University of Science and Technology, Macau, China, in 2020. He is currently an Assistant Professor with the School of Cybersecurity, Northwestern Polytechnical University, Xi'an, China. His research interests include UAV-aided communications, physical-layer security, and large-scale network performance analysis. He serves as a TPC Member for conferences, including IEEE GLOBECOM 2021 and 2022 and VTC2021-Fall and a reviewer for various prestigious IEEE journals and conferences.



Hao Wang received the B.Eng. degree in computer science and technology from the Qingdao University of Technology, Qingdao, China, in 2020, and the M.E. degree in network and information security from Northwestern Polytechnical University, Xi'an, China, in 2023. Her research interests include UAV-aided communications and wireless communication security.

Wen Sun (Senior Member, IEEE) received the B.E. degree from the Harbin Institute of Technology in 2009 and the Ph.D. degree in electrical and computer engineering from the National University of Singapore in 2014. She is currently a Full Professor with Northwestern Polytechnical University. She has published more than 60 peer-reviewed papers in various prestigious IEEE journals and conferences, including IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, and IEEE NETWORK. Her research interests cover a wide range of areas including wireless mobile communications, the IoT, 5G, and blockchain. She was a recipient of the Best Paper Award of IEEE GLOBECOM2019. She was also a recipient of the IEEE TCGCC Outstanding Young Researcher Award 2022. She serves as the Chair for the IEEE ComSoc TCGCC Special Interest Group (SIG) of the Green Digital Twin. She serves as an Associate Editor for *China Communications* and a Guest Editor for IEEE NETWORK and *Digital Communications and Networks*.

Nan Zhao (Senior Member, IEEE) received the Ph.D. degree in information and communication engineering from the Harbin Institute of Technology, Harbin, China, in 2011. He is currently a Professor with the Dalian University of Technology, China. He is serving on the editorial boards for IEEE WIRELESS COMMUNICATIONS and IEEE WIRELESS COMMUNICATIONS LETTERS. He won the best paper awards in IEEE VTC 2017 Spring, ICNC 2018, WCSP 2018, and WCSP 2019. He also received the IEEE Communications Society Asia Pacific Board Outstanding Young Researcher Award in 2018.

Hong-Ning Dai (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from the Department of Computer Science and Engineering, Chinese University of Hong Kong. He is currently with the Department of Computer Science, Hong Kong Baptist University, Hong Kong, as an Associate Professor. His current research interests include blockchain and the Internet of Things. He is a member of the ACM. He has served as an Associate Editor for IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE SYSTEMS JOURNAL, and IEEE ACCESS.

Wei Zhang (Fellow, IEEE) received the Ph.D. degree in electronic engineering from The Chinese University of Hong Kong, Hong Kong, in 2005. He is currently a Professor with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia. His current research interests include unmanned aerial vehicle communications and 5G and beyond. In addition, he has served as a member in various ComSoc boards/standing committees, including Journals Board, Technical Committee Recertification Committee, Finance Standing Committee, Information Technology Committee, and Steering Committee of IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING and Steering Committee of IEEE NETWORKING LETTERS. He was a recipient of six best paper awards from IEEE conferences and ComSoc technical committees. He was an IEEE ComSoc Distinguished Lecturer from 2016 to 2017. Within the IEEE Communications Society (ComSoc), he has taken many leadership positions, including the Member-at-Large on the Board of Governors from 2018 to 2020, the Chair of Wireless Communications Technical Committee from 2019 to 2020, the Vice Director of Asia Pacific Board from 2016 to 2021, the Editor-in-Chief of IEEE WIRELESS COMMUNICATIONS LETTERS from 2016 to 2019, the Technical Program Committee Chair of Asia-Pacific Conference on Communications in 2017 and the IEEE International Conference on Cognitive Computing in 2019, and the Award Committee Chair of Asia Pacific Board and the Technical Committee on Cognitive Networks. He is recently elected as the Vice President of the IEEE Communications Society from 2022 to 2023. He currently serves as an Area Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and the Editor-in-Chief for the *Journal of Communications and Information Networks*. Previously, he served as an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, and IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS C Cognitive Radio Series.