Physical Layer Security in IRS-Assisted Cache-Enabled Satellite Communication Networks

Quynh T. Ngo, Khoa T. Phan, Abdun Mahmood and Wei Xiang

***Abstract*—This paper presents a comprehensive analysis of the physical layer security performance of a cache-enabled satellite communication network that incorporates intelligent reflecting surfaces (IRS) in the presence of a passive eavesdropper. In the proposed system, content caches are deployed at both the ground station and the satellite, which can improve system performance by reducing latency and transmission overhead. Moreover, the use of IRS provides an additional layer of security by enabling the manipulation of the reflected signals to impede eavesdropping. Practical channel models are used to derive connection probability and secrecy probability for both the ground station-IRS-user and the satellite-IRS-user links. The obtained results are then used to evaluate the system's secure transmission probability, which is maximized subject to the caching probabilities and transmission rate constraints. The paper presents numerical results to demonstrate the accuracy of the analysis and the effectiveness of deploying IRS and caching to support secure content delivery. The findings provide valuable insights into the potential benefits of utilizing IRS and caching technologies in satellite communication networks for improved physical layer security.**

***Index Terms*—Intelligent reflecting surfaces, edge caching, satellite-terrestrial networks, physical layer security.**

I. Introduction

Integrating satellite communications (satcom) into terrestrial networks is a vital solution to deliver the internet of everything. To overcome high service latency and pricey bandwidth issues in satcom, edge caching, which allows popular contents to be pre-stored at edge devices during off-peak hours, has emerged as a promising solution [1]. Edge caching in satellite-terrestrial network (STN) has been proved to effectively offload the backhaul of terrestrial networks [2], reduce the content delivery time [3], [4], enhance the outage probability [5], and the successful delivery probability [6], etc. Nonetheless, satcom is more exposed to security vulnerabilities due to the openness of transmission medium as well as the large beam coverage area of satellites. To provide wireless transmission confidentiality, two types of approaches are typically employed: the upper-layer cryptographic encryption and the physical layer security (PLS) techniques. The latter approach has attracted much research attention for two reasons. Firstly, unlike cryptography, it does not rely on computational complexity, ensuring security is not compromised by powerful unauthorized devices. Secondly, PLS is highly scalable, making it suitable for a network with decentralized devices of varying computational capabilities and power. This makes it useful for both direct secure data communication and for distributing cryptographic keys in the network [7]. Recently, there have been numerous works investigating PLS in cache-enabled wireless networks, for example see [8]–[14] and references therein. Enabling the caching capability at base stations (BS) and users in a wireless heterogeneous network, [8] designed two transmission schemes at symbol and bit level to improve the transmission security. In these transmission schemes, the BS transmits a combination at symbol and bit level of a requested file with a pre-cached file at user to degrade the eavesdropper's channel. Studying the PLS in cache-enable cellular networks where the caching ability is enabled at micro BSs, [9] and [10] designed the cache placement and file delivery to achieve secure transmissions against randomly distributed eavesdroppers. The secrecy throughput and secrecy energy efficiency have been investigated in [9], while [10] analyzed the secure content delivery probability. The multi-input multi-output transmission in a multi-cell network has been secured by deploying caching to enhance the secrecy rate in [11]. The PLS in a large-scale edge caching network was studied in [12] with a focus on the secure content delivery probability problem. [13] proposed a two-hop edge caching scheme in 6G networks to protect data against being eavesdropped, and the PLS in cache-enabled mmwave heterogeneous networks was studied in [14]. While these studies have investigated PLS in cache-enabled wireless networks, none of them have focused specifically on integrating satcom into terrestrial networks. The integration of satcom into terrestrial networks presents inherent challenges such as channel modeling for satellite and terrestrial communications links, transmission schemes, and caching designs, among others [1]. These challenges make it necessary to explore the potential of PLS in cache-enabled STN to ensure secure and efficient data transmission. Thus, further research is needed to investigate the feasibility and effectiveness of PLS in STN, which would help address the security concerns associated with the openness of the transmission medium and large beam coverage area of satellites.

The recent deployment of intelligent reflecting surfaces (IRS) in wireless communication systems has led to more efficient PLS techniques [15]. An IRS is a metasurface composed of low-power passive reflecting elements that can be reconfigured to modify the amplitude and/or phase of incident signals, reflecting them to a desired location. In PLS systems,

"This work was supported by the La Trobe University Postgraduate Research Scholarship, the La Trobe University Full-Fee Research Scholarship, and the Net Zero Scholarship sponsored by Sonepar/SLS."

Q.T. Ngo is with the School of Electrical and Data Engineering, University of Technology Sydney, NSW, Australia, email: QuynhTu.Ngo@uts.edu.au.
K.T. Phan, A. Mahmood and W. Xiang are with the School of Computing, Engineering and Mathematical Sciences, La Trobe University, VIC, Australia, email: {k.phan, a.mahmood, w.xiang}@latrobe.edu.au.

the IRS is utilized to enhance the signal-to-noise ratio (SNR) at authorized users while simultaneously decreasing the SNR at eavesdroppers. IRS is particularly compelling for wireless systems as it can reshape the wireless environment without incurring huge complexity and cost to enhance PLS [15]. However, research on IRS-assisted PLS systems has not yet matured enough. There are only a few works on IRS-assisted terrestrial PLS systems [16]–[21]. It is important to note that the IRS-related channels in all of these works are investigated with terrestrial channel characteristics. PLS with IRS-space related channels has not yet been addressed.

Motivated by the above discussions, this paper investigates the potential of PLS in a two-tier cache-enabled IRS-assisted STN, where content caches are deployed at both the satellite and ground station. Such systems can find applications in a variety of scenarios where reliable, high-speed connectivity is necessary. By enabling cache at both the BS and satellite, and allowing the IRS to assist both the BS-user link and the satellite-user link, they can provide efficient use of radio resources, reduced communication latency, and increased system capacity. The two-cache tier configuration has been proposed in previous works to improve satellite bandwidth consumption [3] and service delivery time [6]. To improve the cache hit ratio, probabilistic caching is employed at both cache tiers in this study. While this work does not explicitly consider the green communication potential of the system, it should be noted that a cache-enabled IRS-assisted STN can significantly benefit green communication by reducing energy consumption through content caching at the satellite and ground station and enabling passive beamforming with IRS, thus eliminating the need for active transmitting and receiving elements. However, this work focuses on the overall system secure transmission analysis of novel cooperative two-hop content delivery schemes and the optimization of caching probabilities and transmission rates. The main contributions of this paper are summarized as follows.

1) We propose an IRS-assisted cache-enabled STN where a probabilistic caching policy is employed at the two cache tiers. Additionally, a novel two-hop content delivery scheme is introduced, with the IRS providing assistance in securing the transmission from the ground station and satellite to the user.

2) We evaluate the connection probability and secrecy probability of content delivery over two cascaded fading channels: the Rayleigh–Rayleigh fading channel for the ground station-IRS-user link, and the Rayleigh–Shadowed-Rician fading channel for the satellite-IRS-user link, with provided asymptotic and closed-form expressions. Based on these results, we assess the system's secure transmission probability in combination with the probabilistic caching policy.

3) We jointly design the transmission rates and caching probability to maximize the system's secure transmission probability. The non-convex optimization problem is decomposed into two steps. In the first step, we find the transmission rates that maximize the secure transmission probability in the ground station-IRS-user and satellite-IRS-user schemes. In the second step, we derive the caching probability that maximizes the secure transmission probability.

4) We evaluate the PLS performance for the two-tier cache-enabled STN with and without the IRS, as well as the IRS-assisted single-tier versus two-tier cache-enabled STN. The numerical results confirm the validity of the theoretical analysis and verify the independence in optimizing the redundant rate and caching probability. The importance of optimizing the redundant rate to achieve the highest secure transmission probability while saving resources is also highlighted. The results demonstrate that having IRS and two cache tiers enabled can improve the secrecy probability by almost 50% compared to scenarios without IRS and single cache tier.

The remainder of this paper is organized as follows. Section II describes the proposed system model and the two-hop content delivery scheme. Section III analyzes the connection probability and secrecy probability of the transmission for ground station-IRS-user and satellite-IRS-user cases. Section IV jointly designs the transmission rates and the caching probability to maximize the overall system secure transmission probability. The theoretical analysis is validated by numerical results in Section V, and conclusions are made in Section VI.

II. System Model

A. Network model

We consider a two-tier cache-enabled satellite-terrestrial system in Fig. 1, assisted by an IRS. The system comprises a gateway, a GEO satellite (S), a ground station (G), an IRS, a user (U), and an eavesdropper (E), all equipped with single antennas. The IRS is composed of M passive reflecting elements, each capable of independently adjusting the phase of incoming signals. We assume that there is no direct link between the gateway and the ground station due to their remote locations. Additionally, we assume that there is no direct link between the satellite and the users. This can occur in various scenarios where the signal from the satellite is obstructed or weakened, making it difficult or impossible for users to establish a direct link with the satellite. In such cases, an IRS can be used to reflect the satellite signal and establish a link with the users.

There are two caching tiers in the proposed system, one at the ground station G and the other at the satellite S, each with a storage capacity of C_1 and C_2 bits, respectively. To efficiently serve the user's requests, both the satellite and the ground station can pre-cache the content during off-peak hours from the gateway. The file library is hosted by the gateway and consists of N files denoted as $W_1, ..., W_N$, where each file has an equal size of F bits[1]. The user requests a file W_n with probability q_n that follows the Zipf distribution [22], i.e., $q_n = n^{-\alpha}/(\sum_{m=1}^{N} m^{-\alpha})$, where $\alpha \in (0, 1)$. If the requested file is available in one of the cache tiers, a cache hit event occurs, and the file is served directly from that cache. Otherwise, a cache miss event occurs, and the requested content is served from the gateway since it is not possible to pre-cache all contents due to limited caching capacity. Let $\mathcal{A}_i = \left\{a_{i,1}, ..., a_{i,n}, ..., a_{i,N}\right\}$, $i = 1, 2$ denote the caching probabilities with $a_{i,n}$ being the probability that file W_n is

[1] In case of unequal file size, a file fragmentation process can be utilized to divide the files into equal subfiles.

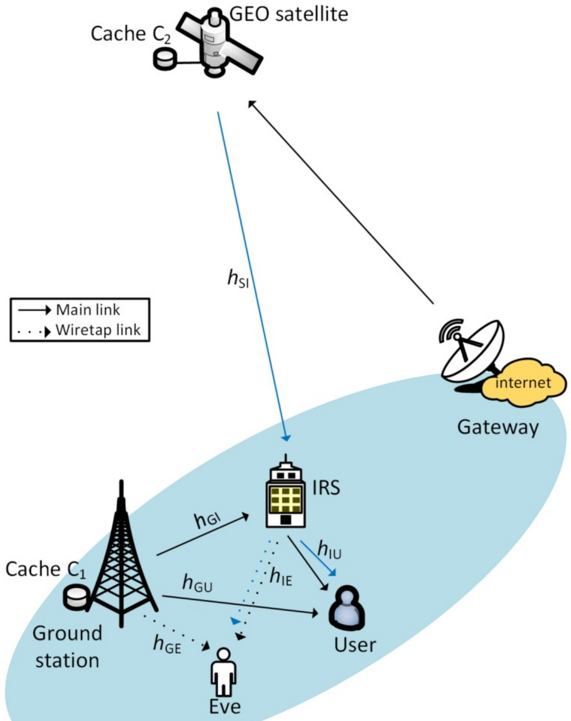

Fig. 1: System model of IRS-assisted two-tier cache-enabled satellite-terrestrial networks.

pre-fetched at cache C_i. The caching probabilities are subject to the condition that the sum of the probabilities of all files stored in a cache tier should not exceed its storage capacity, i.e., $\sum_{n=1}^{N} a_{i,n} \leq C_i/F$, $(i = 1, 2)$ and $0 \leq a_{i,n} \leq 1$, $(i = 1, 2; n = 1, ..., N)$. The whole-file caching strategy is assumed in this work.

B. Channel model

We adopt block-based communications, where a transmission section is accomplished within a coherence time T (seconds). The channel fading consists of large-scale and small-scale fading. The large-scale fading is modeled by the distance-dependent power-law path-loss attenuation $d^{-\alpha_i}$, where d denotes the distance, and α_i represents the path-loss exponent. Since the satellite employed is geostationary, its distance to the devices on the ground can be considered time-invariant. For small-scale fading, shadowed-Rician fading [23] and Rayleigh fading models have been widely adopted for satcom and terrestrial channels. Let $\tilde{h}_{mn}$ denote the small-scale fading coefficient of the link between nodes m and n. **The satellite link** composes of multipath fading, which consists of one line-of-sight (LOS) and multiple weak scatter component, and shadow fading, which has LOS and multiplicative shadow fading [23]. The satellite channel fading coefficient is governed by the following distribution

$$f_{\tilde{h}_{mn}}(x) = \alpha_1 \exp\left(-\frac{x}{b_1}\right) {}_1F_1\left(m_1; 1; \sigma_1 x\right) \qquad (1)$$

with coefficients

$$\alpha_1 = \left(\frac{b_1 m_1}{b_1 m_1 + \Omega_1}\right)^{m_1} \frac{1}{b_1}, \quad \sigma_1 = \frac{\Omega_1}{b_1(b_1 m_1 + \Omega_1)},$$

where b_1 represents the average power of the scatter components; Ω_1 represents the average power of the LOS component; m_1 is the Nakagami parameter; ${}_1F_1(\cdot;\cdot;\cdot)$ is the confluent hypergeometric function of the first kind [24, eq.(9.210.1)]. **The terrestrial link** is modeled as the independent and identically distributed Rayleigh fading channel with the probability density function of

$$f_{\tilde{h}_{mn}}(x) = \frac{1}{\sqrt{\bar{h}_{mn}}} \exp\left(-\frac{x^2}{\bar{h}_{mn}}\right) \qquad (2)$$

where $\bar{h}_{mn}$ is the average channel power gain taking into the effects of small-scale fading.

We assume that the satellite and ground station have access to only the statistical channel state information (CSI) instead of instantaneous CSI for both the main and wiretap channels[2], hence fixed rates are employed as discussed in the following.

C. Security performance metrics

To secure the content delivery, the well-known Wyner's wiretap encoding scheme [25] is employed, where the confidential information is encoded and redundant information is embedded to confuse the eavesdroppers. Let R_s and R_e respectively denote the secrecy data rate and the redundant information rate. The transmission rate of the codewords is defined as $R_t \triangleq R_s + R_e$. If the achievable rate of the legitimate link is more than R_t, the user can recover the secret message and a connection is established. The probability of this event is called connection probability (CP) p_c. If the achievable rate of the wiretap link does not exceed R_e, the eavesdropper is not able to decode the secret message, then the transmission is secured. The probability that this event is referred as secrecy probability (SP) p_s [10], [26]. Mathematically, we have:

$$\begin{aligned} p_c &= \mathbb{P}\left\{\log_2\left(1+\gamma_u\right) \geq R_t\right\}, \\ p_s &= \mathbb{P}\left\{\log_2\left(1+\gamma_e\right) \leq R_e\right\} \end{aligned} \qquad (3)$$

where γ_u and γ_e represent the SNRs of the user and the eavesdropper links, respectively. The content delivery is secured only if both the connectivity and secrecy are guaranteed simultaneously.

D. Content delivery scheme

We consider the following transmission scheme. When the ground station receives a request for file W_n, it acts based on the file caching status.

1) **Case 1:** If W_n is cached locally, the ground station will directly transmit the file to the user (one-hop transmission).
2) **Case 2:** If file W_n is not cached at ground station, it will forward the request to satellite. There are two cases:

[2] The assumption of having knowledge of the statistical CSI of wiretap channels applies to scenarios where unauthorized users, who are not intended recipients of the content, may attempt to eavesdrop. In such cases, the satellite and ground station can obtain the statistical CSI and the location distribution of potential eavesdroppers through extensive information exchange during other time slots.

- If the file is cached at the satellite, which will transmit the file to the user via IRS (one-hop transmission).
- Otherwise, it will be retrieved from gateway, then relayed through satellite to the user (two-hop transmission).

We can see that a secure transmission happens only when the user establishes a reliable connection with ground station or satellite, and the confidentiality of the requested file is guaranteed during the transmission. Hence, the probability of secure one-hop transmission event for file W_n is $p_{\text{secure},1}(n) = a_{1,n}p_{c,1}p_{s,1} + a_{2,n}p_{c,2}p_{s,2}$. The event of secure two-hop transmission for file W_n is equivalent to that the gateway-satellite link is able to support the transmission of the whole file W_n within a half transmission block, and the transmission from satellite to user is secured, and that file W_n is not cached at both satellite and ground station. Let γ_{Gw} denotes the SNR of the gateway-satellite link, the probability that the link can support whole file transmission within a half block is $p_{\text{Gw}} = \mathbb{P}(\frac{1}{2}TB_{\text{Gw}}\log_2(1+\gamma_{\text{Gw}}) \geq F)$. The probability of secure transmission from satellite to user is $p_{c,2}p_{s,2}$. The probability that file W_n is not cached at both tiers is $1 - a_{1,n} - a_{2,n}$, note that for effective cache utilization we do not cache the same file at both tiers. Hence, the probability of secure two-hop transmission event can be expressed as $p_{\text{secure},2}(n) = (1 - a_{1,n} - a_{2,n})p_{\text{Gw}}p_{c,2}p_{s,2}$. The CP and SP, $p_{c,1}$ and $p_{s,1}$, are calculated as in (3); $p_{c,2} = \mathbb{P}(\frac{1}{2}\log_2(1+\gamma_u) \geq R_t)$; $p_{s,2} = \mathbb{P}(\frac{1}{2}\log_2(1+\gamma_e) \leq R_e)$.

The secure transmission probability (STP) of the system can be expressed as:

$$p_{\text{secure}} = \sum_{n=1}^{N} q_n(p_{\text{secure},1}(n) + p_{\text{secure},2}(n)) \tag{4}$$

where q_n represents the probability that file W_n is requested.

III. Secure transmission probability analysis

With the assistance of IRS, the signal propagates to the user by the adjusted reflections of the IRS. The IRS is assumed to have perfect knowledge on the CSI of the user.

1) Ground station-IRS-user.

When file W_n is served directly from ground station, the received signal at user consists of the direct signal transmitted by ground station and the reflected signal from IRS, which can be expressed as

$$y_{\text{U},1} = \sqrt{P_1}h_{\text{GU}}x_1 + \sqrt{P_1}\left(\textstyle\sum_{i=1}^{M} h_{\text{GI}_i}h_{\text{I}_i\text{U}}e^{j\phi_{1,i}}\right)x_1 + w_n, \tag{5}$$

where h_{GU} is the channel coefficient of the direct G-U link; h_{GI_i} and $h_{\text{I}_i\text{U}}$ respectively represent the channel coefficients of the indirect link from G to the i-th element of IRS to U; $\phi_{1,i}$ is the adjustable phase induced by the i-th reflecting element of IRS; x_1 represents the transmit signal by ground station with transmit power P_1; and $w_n \sim \mathcal{CN}(0, \sigma^2_{n,\text{U}})$ is the additive white Gaussian noise (AWGN) at U with zero mean and variance $\sigma^2_{n,\text{U}}$. The channel coefficients comprises of large-scale fading and small-scale fading, i.e.,

$$h_{\text{GU}} = \tilde{h}_{\text{GU}}d_{\text{GU}}^{-\alpha_g} \tag{6}$$

where $\tilde{h}_{\text{GU}}$ is modeled as in (2), d_{GU} denotes the distance between G and U, and α_g is the terrestrial path-loss exponent. h_{GI_i} and $h_{\text{I}_i\text{U}}$ are modeled similarly. The reflected signal from IRS, $\sqrt{P_1}\left(\sum_{i=1}^{M} h_{\text{GI}_i}h_{\text{I}_i\text{U}}e^{j\phi_{1,i}}\right)x_1$, is modeled as when each of the IRS elements receives the incoming signal from the ground station independently and reflects the signal with adjusted phase to the user. Then, the received signal from all IRS elements are modeled as a superposition of all the corresponding reflected signals [27].

The result CP and SP of this case can be expressed as

$$\begin{aligned} p_{c,1} =& \mathbb{P}\left\{\log_2\left(1 + \frac{P_1|h_{\text{GU}} + \sum_{i=1}^{M} h_{\text{GI}_i}h_{\text{I}_i\text{U}}e^{j\phi_{1,i}}|^2}{\sigma^2_{n,U}}\right) \geq R_{t,1}\right\}, \\ p_{s,1} =& \mathbb{P}\left\{\log_2\left(1 + \frac{P_1|h_{\text{GE}} + \sum_{i=1}^{M} h_{\text{GI}_i}h_{\text{I}_i\text{E}}e^{j\phi_{1,i}}|^2}{\sigma^2_{n,E}}\right) \leq R_{e,1}\right\} \end{aligned} \tag{7}$$

where $R_{t,1}$, $R_{e,1}$ represent the codeword transmitting rate and redundant rate in **Case 1**, respectively; h_{GE}, $h_{\text{I}_i\text{E}}$ are respectively the channel coefficients of G-E and the i-th element of IRS-E links; $\sigma^2_{n,E}$ is the variance of the AWGN at E. Note that $\phi_{1,i}$ is adjusted to maximize the SNR at the user, i.e., $\phi_{1,i}$ can be equal to negative of phase $h_{GI_i}h_{I_iU}$, hence, $p_{c,1}$ (and following $p_{c,2}$) is independent of $\phi_{1,i}$.

2) Satellite-IRS-user.

The user receives only the reflected signal from IRS in this case. Let x_2 denote the transmit signal by satellite with transmit power P_2, the CP and SP of this case are

$$\begin{aligned} p_{c,2} =& \mathbb{P}\left\{\frac{1}{2}\log_2\left(1 + \frac{P_2|\sum_{i=1}^{M} h_{\text{SI}_i}h_{\text{I}_i\text{U}}e^{j\phi_{2,i}}|^2}{\sigma^2_{n,U}}\right) \geq R_{t,2}\right\}, \\ p_{s,2} =& \mathbb{P}\left\{\frac{1}{2}\log_2\left(1 + \frac{P_2|\sum_{i=1}^{M} h_{\text{SI}_i}h_{\text{I}_i\text{E}}e^{j\phi_{2,i}}|^2}{\sigma^2_{n,E}}\right) \leq R_{e,2}\right\} \end{aligned} \tag{8}$$

where $\phi_{2,i}$ represents the phase shift of the i-th element of IRS in **Case 2**; $h_{\text{SI}_i} = \tilde{h}_{\text{SI}_i}d_{\text{SI}}^{-\alpha_s}$ is the channel coefficients of S-IRS link in which $\tilde{h}_{\text{SI}_i}$ follows shadowed-Rician fading in (1), d_{SI} is the distance between satellite and IRS, α_s is the satellite path-loss exponent; $R_{t,2}$ and $R_{e,2}$ are respectively the threshold transmitting rate and redundant rate for secure transmission of **Case 2**.

A. Connection probability analysis

Case 1: Ground station-IRS-user.

The connection probability is found in a closed-form using the moment-matching method.

Let $z_1 = \frac{\sigma^2_{n,\text{U}}}{P_1}(2^{R_{t,1}} - 1)$, then from (7), $p_{c,1} = \mathbb{P}\left\{|h_{\text{GU}} + \sum_{i=1}^{M} h_{\text{GI}_i}h_{\text{I}_i\text{U}}e^{j\phi_{1,i}}|^2 \geq z_1\right\}$.

Theorem 1. *For a given z_1, the connection probability is obtained as follows,*

$$p_{c,1} = 1 - \frac{\gamma(k_c, z_1/w_c)}{\Gamma(k_c)} \tag{9}$$

with the shape parameter $k_c = \frac{|\mathbb{E}(X_c)|^2}{Var(X_c)}$ and the scale parameter $w_c = \frac{Var(X_c)}{\mathbb{E}(X_c)}$ where

$$\mathbb{E}(X_c) =2\bar{h}_{\mathrm{GU}}^2 d_{\mathrm{GU}}^{-2\alpha_g} + 2\bar{h}_{\mathrm{GU}}(d_{\mathrm{GU}} d_{\mathrm{IU}} d_{\mathrm{GI}})^{-\alpha_g} \sum_{i=1}^{M} \Delta_i + (d_{\mathrm{IU}} d_{\mathrm{GI}})^{-2\alpha_g} \Theta_2,$$

$$\begin{aligned} Var(X_c) = {} & 20\bar{h}_{\mathrm{GU}}^4 d_{\mathrm{GU}}^{-4\alpha_g} + 8\bar{h}_{\mathrm{GU}}^3 d_{\mathrm{GU}}^{-3\alpha_g} (d_{\mathrm{IU}} d_{\mathrm{GI}})^{-\alpha_g} \left(3\sum_{i=1}^{M} \Delta_i - 1\right) \\ & + 4\bar{h}_{\mathrm{GU}}^2 (d_{\mathrm{GU}} d_{\mathrm{IU}} d_{\mathrm{GI}})^{-2\alpha_g} \left(3\Theta_2 - \sum_{i=1}^{M} \Delta_i\right) + (d_{\mathrm{IU}} d_{\mathrm{GI}})^{-4\alpha_g} \Theta_4 \\ & + 4\bar{h}_{\mathrm{GU}} d_{\mathrm{GU}}^{-\alpha_g} (d_{\mathrm{IU}} d_{\mathrm{GI}})^{-3\alpha_g} \Theta_3 - 4\bar{h}_{\mathrm{GU}}^2 (d_{\mathrm{GU}} d_{\mathrm{IU}} d_{\mathrm{GI}})^{-2\alpha_g} \left(\sum_{i=1}^{M} \Delta_i\right)^2 \\ & - (d_{\mathrm{IU}} d_{\mathrm{GI}})^{-3\alpha_g} \Theta_2 \left((d_{\mathrm{IU}} d_{\mathrm{GI}})^{-\alpha_g} \Theta_2 + 4\bar{h}_{\mathrm{GU}} d_{\mathrm{GU}}^{-\alpha_g} \sum_{i=1}^{M} \Delta_i\right). \end{aligned}$$

Here, $\Theta_l = \sum_{r_1+\cdots+r_M=l} \left\{ \binom{l}{r_1,\cdots,r_M} \prod_{i=1}^{M} (r_i!)^2 \Delta_i^{r_i} \right\}, l=2,3,4$, $\Delta_i = \bar{h}_{\mathrm{I}_i\mathrm{U}} \bar{h}_{\mathrm{GI}_i} e^{j\phi_{1,i}}$, $\gamma(a,x) = \int_0^x t^{a-1} e^{-t} dt$ *denotes the lower incomplete Gamma function, and* $\Gamma(a)$ *denotes the Gamma function.*

Proof. Please see Appendix A. □

Case 2: Satellite-IRS-user.

Since the term $|\sum_{i=1}^{M} h_{\mathrm{SI}_i} h_{\mathrm{I}_i\mathrm{U}} e^{j\phi_{2,i}}|^2$ in (8) is the squared sum of product of exponential and shadowed-Rician random variables, it is challenging to derive a closed-form expression for $p_{c,2}$. However, we can derive the asymptotic expression of $p_{c,2}$ as follows.

Corollary 1. *In high SNR regime, the connection probability $p_{c,2}$ is obtained as follows,*

$$p_{c,2} \approx 1 - \prod_{i=1}^{M} \left(\left(\sum_{n=1}^{\infty} \frac{(\sigma_{1_i} b_{1_i})^n}{n!} (m_{1_i})_n \beta(1,n) \right) \times \frac{d_{\mathrm{SI}}^{-\alpha_s} \alpha_{1_i} \sqrt{z_2}}{\bar{h}_{\mathrm{I}_i\mathrm{U}} d_{\mathrm{IU}}^{-\alpha_g} e^{j\phi_{2,i}}} \right) \tag{10}$$

where $z_2 = \frac{\sigma_{n,\mathrm{U}}^2}{P_2}(2^{2R_{t,2}} - 1)$, *and* $\beta(1,n)$ *denotes the Beta function.*

Proof. Let $z_2 = \frac{\sigma_{n,\mathrm{U}}^2}{P_2}(2^{2R_{t,2}} - 1)$, then from (8) we have $p_{c,2} = \mathbb{P}\left\{ |\sum_{i=1}^{M} h_{\mathrm{SI}_i} h_{\mathrm{I}_i\mathrm{U}} e^{j\phi_{2,i}}|^2 \geq z_2 \right\}$.

Proposition 1. *The connection probability of the Satellite-IRS-user case is expressed using integral form as*

$$\begin{aligned} p_{c,2} = 1 - \prod_{i=1}^{M} \Bigg(\int_0^{\dot{u}_i} d_{\mathrm{SI}}^{-\alpha_s} \alpha_{1_i} b_{1_i} z_2 u_i \Bigg(\sum_{n=1}^{\infty} \frac{(\sigma_{1_i} b_{1_i})^n (m_{1_i})_n}{n!(1)_n} \\ \times \left(\frac{\sqrt{z_2} u_i}{2} \right)^n K_n(\sqrt{z_2} u_i) \Bigg) du_i \Bigg) \end{aligned} \tag{11}$$

where $(.)_n$ *denotes the Pochhammer symbol,* $K_n(.)$ *is the modified Bessel function of the second kind with order* n *[24, eq.(8.432)], and* $\dot{u}_i = \frac{2}{(\bar{h}_{\mathrm{I}_i\mathrm{U}} d_{\mathrm{IU}}^{-\alpha_g} e^{j\phi_{2,i}} b_{1_i})^{1/2} z_2^{1/4}}$.

Proof. Please see Appendix B. □

In high SNR regime, $P_2 \to \infty$, the asymptotic approximation of $K_n(\sqrt{z_2} u_i)$ [28, eq.(9.6.9)] is

$$K_n(\sqrt{z_2} u_i) \approx \frac{1}{2}\Gamma(n) \left(\frac{\sqrt{z_2} u_i}{2} \right)^{-n}. \tag{12}$$

Substituting (12) into (11), the result can be obtained. □

It is worth noting that the infinite summation term in (10) converges, and its numerical value can be found through partial sum method.

Remark 1. *The results from **Theorem 1** and **Corollary 1** demonstrate the significant impact of transmit power and transmission rate on the connection probability. Increasing transmit power leads to an increase in connection probability, while increasing transmission rate results in a decrease in connection probability for both cases.*

B. Secrecy probability analysis

The SP derivations are similar to that of CP above. However, it is worth noting that the IRS does not have the eavesdropper's CSI. There is no reflection adjustment at IRS in order to maximize the SNR at eavesdropper; Hence, the value of $\phi_{j,i}, j = 1, 2$ (the reflection adjustment at IRS to maximize the SNR at user) remain the same as in the connection probability analysis.

Case 1: Ground station-IRS-user.

Let $s_1 = \frac{\sigma_{n,\mathrm{E}}^2}{P_1}(2^{R_{e,1}} - 1)$, then from (7) we have $p_{s,1} = \mathbb{P}\left\{ |h_{\mathrm{GE}} + \sum_{i=1}^{M} h_{\mathrm{GI}_i} h_{\mathrm{I}_i\mathrm{E}} e^{j\phi_{1,i}}|^2 \leq s_1 \right\}$.

Proposition 2. *Based on the analysis for (9), the secrecy probability for a given s_1 is given by*

$$p_{s,1} = \frac{\gamma(k_s, s_1/w_s)}{\Gamma(k_s)} \tag{13}$$

with the shape parameter $k_s = \frac{|\mathbb{E}(X_s)|^2}{Var(X_s)}$ and the scale parameter $w_s = \frac{Var(X_s)}{\mathbb{E}(X_s)}$, where

$$\mathbb{E}(X_s) =2\bar{h}_{\mathrm{GE}}^2 d_{\mathrm{GE}}^{-2\alpha_g} + 2\bar{h}_{\mathrm{GE}}(d_{\mathrm{GE}} d_{\mathrm{IE}} d_{\mathrm{GI}})^{-\alpha_g} \sum_{i=1}^{M} \dot{\Delta}_i + (d_{\mathrm{IE}} d_{\mathrm{GI}})^{-2\alpha_g} \dot{\Theta}_2,$$

$$\begin{aligned} Var(X_s) = {} & 20\bar{h}_{\mathrm{GE}}^4 d_{\mathrm{GE}}^{-4\alpha_g} + 8\bar{h}_{\mathrm{GE}}^3 d_{\mathrm{GE}}^{-3\alpha_g} (d_{\mathrm{IE}} d_{\mathrm{GI}})^{-\alpha_g} \left(3\sum_{i=1}^{M} \dot{\Delta}_i - 1\right) \\ & + 4\bar{h}_{\mathrm{GE}}^2 (d_{\mathrm{GE}} d_{\mathrm{IE}} d_{\mathrm{GI}})^{-2\alpha_g} \left(3\Theta_2 - \sum_{i=1}^{M} \dot{\Delta}_i\right) + (d_{\mathrm{IE}} d_{\mathrm{GI}})^{-4\alpha_g} \dot{\Theta}_4 \\ & + 4\bar{h}_{\mathrm{GE}} d_{\mathrm{GE}}^{-\alpha_g} (d_{\mathrm{IE}} d_{\mathrm{GI}})^{-3\alpha_g} \dot{\Theta}_3 - 4\bar{h}_{\mathrm{GE}}^2 (d_{\mathrm{GE}} d_{\mathrm{IE}} d_{\mathrm{GI}})^{-2\alpha_g} \left(\sum_{i=1}^{M} \dot{\Delta}_i\right)^2 \\ & - (d_{\mathrm{IE}} d_{\mathrm{GI}})^{-3\alpha_g} \dot{\Theta}_2 \left((d_{\mathrm{IE}} d_{\mathrm{GI}})^{-\alpha_g} \dot{\Theta}_2 + 4\bar{h}_{\mathrm{GE}} d_{\mathrm{GE}}^{-\alpha_g} \sum_{i=1}^{M} \dot{\Delta}_i\right) \end{aligned}$$

in which $\dot{\Theta}_l = \sum_{r_1+\cdots+r_M=l} \left\{ \binom{l}{r_1,\cdots,r_M} \prod_{i=1}^{M} (r_i!)^2 \dot{\Delta}_i^{r_i} \right\}, l=2,3,4$ *and* $\dot{\Delta}_i = \bar{h}_{\mathrm{I}_i\mathrm{E}} \bar{h}_{\mathrm{GI}_i} e^{j\phi_{1,i}}$.

Case 2: Satellite-IRS-user.

Let $s_2 = \frac{\sigma_{n,\mathrm{E}}^2}{P_2}(2^{2R_{e,2}} - 1)$, from (8) the secrecy probability is $p_{s,2} = \mathbb{P}\left\{ |\sum_{i=1}^{M} h_{\mathrm{SI}_i} h_{\mathrm{I}_i\mathrm{E}} e^{j\phi_{2,i}}|^2 \leq s_2 \right\}$.

Proposition 3. *Similar to the analysis of (10), in high SNR regime, $p_{s,2}$ can be given as*

$$p_{s,2} \approx \prod_{i=1}^{M} \left(\left(\sum_{n=1}^{\infty} \frac{(\sigma_{1_i} b_{1_i})^n}{n!} (m_{1_i})_n \beta(1,n) \right) \frac{d_{\mathrm{SI}}^{-\alpha_s} \alpha_{1_i} \sqrt{s_2}}{\bar{h}_{\mathrm{I}_i\mathrm{E}} d_{\mathrm{IE}}^{-\alpha_g} e^{j\phi_{2,i}}} \right). \tag{14}$$

Remark 2. *The results indicate that the secrecy probability decreases with an increase in the transmit power, while the connection probability and secrecy probability are both affected by the redundant information rate. Specifically, increasing the redundant information rate leads to a rise in the secrecy probability and a reduction in the connection probability.*

IV. Secure Content Delivery Probability Maximization

The redundant rate and caching probability play crucial roles in enhancing the system STP. R_e prompts the trade-off between transmission reliability and secrecy since it affects both the CP and SP. The caching probability directly affects the STP since it triggers the probability of adopting one-hop or two-hop transmission schemes. Hence, in this section the optimal redundant rate $R_{e,i}$, $i = 1, 2$ and caching probability $\mathcal{A}_i$, $i = 1, 2$ are jointly designed to maximize the system STP. The optimization problem can be formed as

$$\begin{aligned} \max_{R_{e,i}, \mathcal{A}_i} p_{\text{secure}} &= \sum_{n=1}^{N} q_n (p_{\text{secure},1}(n) + p_{\text{secure},2}(n)) \\ \text{s.t.} &\sum_{n=1}^{N} a_{i,n} F \le C_i \quad (i = 1,2) \\ & 0 \le a_{i,n} \le 1 \quad (i = 1,2) \\ & R_{e,i} \ge 0 \quad (i = 1,2). \end{aligned} \tag{15}$$

This is a non-convex optimization problem. Observing p_{secure}, $(p_{c,i} p_{s,i})$ and q_n are all independent of $a_{i,n}$; Hence, the optimization of the redundant rate $R_{e,i}$ and the caching probability $\mathcal{A}_i$ is independent of each other. The maximizing p_{secure} problem can be decomposed into two steps: (i) determining the optimal $R_{e,i}$ to maximize $(p_{c,i} p_{s,i})$ for each case in the transmission scheme; (ii) designing the optimal $\mathcal{A}_i$ for the two cache tiers to maximize p_{secure}.

A. Optimization of redundant rate $R_{e,i}$

The first-step problem of (15) can be formulated as

$$\max_{R_{e,i} \ge 0} \varphi_i = p_{c,i} p_{s,i}. \tag{16}$$

Let $\beta_{e,i} = 2^{R_{e,i}} - 1$ and $\beta_{s,i} = 2^{R_{s,i}} - 1$. Since $R_{t,i} = R_{e,i} + R_{s,i}$, then $\beta_{t,i} = (1 + \beta_{s,i})\beta_{e,i} + \beta_{s,i}$.

Case 1: Ground station-IRS-user.
Problem (16) can be recast as

$$\max_{\beta_{e,1} \ge 0} \varphi_1 = \left(1 - \frac{\gamma(k_c, A_{\mathrm{U}_1}(\beta_{e,1} + B_1))}{\Gamma(k_c)} \right) \frac{\gamma(k_s, A_{\mathrm{E}_1}\beta_{e,1})}{\Gamma(k_s)} \tag{17}$$

where $A_{\mathrm{U}_1} = \frac{\sigma_{n,\mathrm{U}}^2 (1+\beta_{s,1})}{P_1 w_c}$, $A_{\mathrm{E}_1} = \frac{\sigma_{n,\mathrm{E}}^2}{P_1 w_s}$, and $B_1 = \frac{\beta_{s,1}}{1+\beta_{s,1}}$.

Solution to problem (17) is presented in the following theorem.

Theorem 2. *φ_1 is quasi-concave on $\beta_{e,1}$, and the optimal $\beta_{e,1}^*$ that maximizes φ_1 is the unique zero-crossing of $\frac{\partial \varphi_1}{\partial \beta_{e,1}}$, with*

$$\begin{aligned} \frac{\partial \varphi_1}{\partial \beta_{e,1}} =& \frac{\gamma(k_s, A_{\mathrm{E}_1}\beta_{e,1})}{\Gamma(k_c)\Gamma(k_s)} A_{\mathrm{U}_1}^{k_c} e^{-A_{\mathrm{U}_1}(\beta_{e,1}+B_1)} (\beta_{e,1} + B_1)^{k_c - 1} \\ & - \left(1 - \frac{\gamma(k_c, A_{\mathrm{U}_1}(\beta_{e,1} + B_1))}{\Gamma(k_c)} \right) A_{\mathrm{E}_1}^{k_s} e^{-A_{\mathrm{E}_1}\beta_{e,1}} \beta_{e,1}^{k_s - 1}. \end{aligned} \tag{18}$$

Proof. Let's consider $\frac{\partial \varphi_1}{\partial \beta_{e,1}}$ at two boundaries, where $\beta_{e,1} = 0$ and $\beta_{e,1} \to \infty$. There has $\frac{\partial \varphi_1}{\partial \beta_{e,1}}|_{\beta_{e,1}=0} > 0$. When $\beta_{e,1} \to \infty$, both $\gamma(k_c, A_{\mathrm{U}_1}(\beta_{e,1} + B_1)) \to 0$ and $\gamma(k_s, A_{\mathrm{E}_1}\beta_{e,1}) \to 0$ for $\{A_{\mathrm{U}_1}, A_{\mathrm{E}_1}\} > 0$; hence, $\frac{\partial \varphi_1}{\partial \beta_{e,1}}|_{\beta_{e,1}\to\infty} < 0$.
Since φ is continuous and $\frac{\partial \varphi_1}{\partial \beta_{e,1}}$ is initially positive then negative as $\beta_{e,1}$ increases, there is at least one zero-crossing of $\frac{\partial \varphi_1}{\partial \beta_{e,1}}$.

Let $\beta_{e,1}^*$ denote an arbitrary value such that $\frac{\partial \varphi_1}{\partial \beta_{e,1}}|_{\beta_{e,1}=\beta_{e,1}^*} = 0$. Then, second derivative $\frac{\partial^2 \varphi_1}{\partial \beta_{e,1}^2}$ at $\beta_{e,1} = \beta_{e,1}^*$ is negative,

$$\begin{aligned} \frac{\partial^2 \varphi_1}{\partial \beta_{e,1}^2}|_{\beta_{e,1}=\beta_{e,1}^*} =& -\frac{\gamma(k_s, A_{\mathrm{E}_1}\beta_{e,1})}{\Gamma(k_c)\Gamma(k_s)} A_{\mathrm{U}_1}^{k_c} e^{-A_{\mathrm{U}_1}(\beta_{e,1}+B_1)} (\beta_{e,1} + B_1)^{k_c - 2} \\ & \times \left(A_{\mathrm{U}_1} + A_{\mathrm{E}_1} + \frac{k_s + k_c}{\beta_{e,1} + B_1} + \frac{B_1(k_s + 1)}{(\beta_{e,1} + B_1)\beta_{e,1}} \right) \\ & - \frac{2 A_{\mathrm{U}_1}^{k_c} A_{\mathrm{E}_1}^{k_s}}{\Gamma(k_c)} e^{-A_{\mathrm{U}_1}(\beta_{e,1}+B_1) - A_{\mathrm{E}_1}\beta_{e,1}} (\beta_{e,1} + B_1)^{k_c - 1} \beta_{e,1}^{k_s - 1}. \end{aligned} \tag{19}$$

This proves that function $\varphi_1(\beta_{e,1})$ is quasi-concave [29], and $\beta_{e,1}^*$ is the unique zero-crossing of $\frac{\partial \varphi_1}{\partial \beta_{e,1}}$. Hence, $\beta_{e,1}^*$ is the solution to problem (17). $\beta_{e,1}^*$ can be found through a bisection search when $\frac{\partial \varphi_1}{\partial \beta_{e,1}} = 0$. □

Case 2: Satellite-IRS-user.
Problem (16) can be rewritten as

$$\max_{\beta_{e,2} \ge 0} \varphi_2 = \left(1 - A_{\mathrm{U}_2}(\beta_{e,2} + B_2)^{M/2} \right) A_{\mathrm{E}_2} \beta_{e,2}^{M/2} \tag{20}$$

where $B_2 = \frac{\beta_{s,2}}{1+\beta_{s,2}}$,

$$\begin{aligned} A_{\mathrm{U}_2} =& \left(\frac{\sigma_{n,\mathrm{U}}^2 (1 + \beta_{s,2})}{P_2} \right)^{M/2} \left(\prod_{i=1}^{M} \left(\sum_{n=1}^{\infty} \frac{(\sigma_{1_i} b_{1_i})^n}{n!} (m_{1_i})_n \beta(1,n) \right) \right. \\ & \left. \times \frac{d_{\mathrm{SI}}^{-\alpha_s} \alpha_{1_i}}{\bar{h}_{\mathrm{I}_i\mathrm{U}} d_{\mathrm{IU}}^{-\alpha_g} e^{j\phi_{2,i}}} \right), \\ A_{\mathrm{E}_2} =& \left(\frac{\sigma_{n,\mathrm{E}}^2}{P_2} \right)^{M/2} \left(\prod_{i=1}^{M} \left(\sum_{n=1}^{\infty} \frac{(\sigma_{1_i} b_{1_i})^n}{n!} (m_{1_i})_n \beta(1,n) \right) \frac{d_{\mathrm{SI}}^{-\alpha_s} \alpha_{1_i}}{\bar{h}_{\mathrm{I}_i\mathrm{E}} d_{\mathrm{IE}}^{-\alpha_g} e^{j\phi_{2,i}}} \right). \end{aligned}$$

Solution to problem (20) is described in the following theorem.

Theorem 3. *The function $\varphi_2(\beta_{e,2})$ is concave when $\beta_{e,2} > 0$, and the maximum of φ_2 is achieved at $\beta_{e,2} = \beta_{e,2}^*$ such that $1 - A_{\mathrm{U}_2}(2\beta_{e,2}^* + B_2)(\beta_{e,2}^* + B_2)^{M/2-1} = 0$.*

Proof. The first derivative of $\varphi_2(\beta_{e,2})$ results into

$$\frac{\partial \varphi_2}{\partial \beta_{e,2}} = \left(\frac{M}{2} A_{\mathrm{E}_2} \beta_{e,2}^{M/2-1} \right) \left(1 - A_{\mathrm{U}_2}(2\beta_{e,2} + B_2)(\beta_{e,2} + B_2)^{M/2-1} \right). \tag{21}$$

Since $\left(\frac{M}{2}A_{\mathrm{E}_2}\beta_{e,2}^{M/2-1}\right)$ is always positive, whether $\frac{\partial\varphi_2}{\partial\beta_{e,2}}$ is positive or negative depends on the second term, $\left(1 - A_{\mathrm{U}_2}(2\beta_{e,2}+B_2)(\beta_{e,2}+B_2)^{M/2-1}\right)$. It can be showed that the second term monotonically decreases with respect to $\beta_{e,2}$ as below.

Let $\beta^*_{e,2}$ denote an arbitrary value such that $\left(1 - A_{\mathrm{U}_2}(2\beta^*_{e,2}+B_2)(\beta^*_{e,2}+B_2)^{M/2-1}\right) = 0$. The second derivative $\frac{\partial^2\varphi_2}{\partial\beta_{e,2}^2}$ at $\beta_{e,2} = \beta^*_{e,2}$ is negative,

$$\frac{\partial^2\varphi_2}{\partial\beta_{e,2}^2}|_{\beta_{e,2}=\beta^*_{e,2}} = -MA_{\mathrm{E}_2}A_{\mathrm{U}_2}\beta_{e,2}^{M/2-1}(\beta_{e,2}+B_2)^{M/2-1} - \frac{M}{2}\left(\frac{M-1}{2}\right)A_{\mathrm{E}_2}A_{\mathrm{U}_2}(2\beta_{e,2}+B_2)\beta_{e,2}^{M/2-1}(\beta_{e,2}+B_2)^{M/2-2}. \tag{22}$$

This shows that φ_2 is a concave function when $\beta_{e,2} > 0$. The optimal $\beta^*_{e,2}$ maximizing φ_2 is characterized by $\frac{\partial\varphi_2}{\partial\beta^*_{e,2}} = 0$. □

B. Optimization of caching probability $\mathcal{A}_i$

The second-step problem of (15) can be formulated as

$$\begin{aligned}\max_{\mathcal{A}_i} p_{\text{secure}} &= \sum_{n=1}^{N} q_n(p_{\text{secure},1}(n) + p_{\text{secure},2}(n))\\ \text{s.t.} &\sum_{n=1}^{N} a_{i,n}F \le C_i \quad (i=1,2)\\ &0 \le a_{i,n} \le 1 \quad (i=1,2).\end{aligned} \tag{23}$$

Remark 3. *Function p_{secure} in (23) is a monotonically increasing multivariable function of $a_{i,n}$. Hence, the optimal solutions for (23) can be found using exhaustive search.*

Proof. We have

$$\begin{aligned}p_{\text{secure}} &= \sum_{n=1}^{N} q_n(p_{\text{secure},1}(n) + p_{\text{secure},2}(n))\\ &= \sum_{n=1}^{N} q_n(\varphi_1 - p_{\text{Gw}}\varphi_2)a_{1,n} + q_n(1-p_{\text{Gw}})\varphi_2 a_{2,n} + q_n p_{\text{Gw}}\varphi_2\end{aligned}$$

where φ_1 and φ_2 are found in Subsection IV-A; p_{Gw} is obtained as follows,

$$\begin{aligned}p_{\text{Gw}} =&\mathbb{P}(\frac{1}{2}TB_{\text{Gw}}\log_2(1+\gamma_{\text{Gw}}) \ge F)\\ =&\mathbb{P}(\gamma_{\text{Gw}} > \gamma_{th}) = 1 - F_{\gamma_{\text{Gw}}}(\gamma_{th}),\end{aligned}$$

in which $\gamma_{\text{Gw}} = |h_{\text{GwS}}|^2P_0/\sigma_{n,\mathrm{S}}^2$, $\gamma_{th} = 2^{2F/TB_{\text{Gw}}} - 1$, and

$$\begin{aligned}F_{\gamma_{\text{Gw}}}(\gamma_{th}) =& \frac{\alpha_2\gamma_{th}\sigma_{n,\mathrm{S}}^2}{P_0}{}_1F_1(m_2;2;\frac{\sigma_2\gamma_{th}\sigma_{n,\mathrm{S}}^2}{P_0})\\ &+ \sum_{j=1}^{\infty}(-1)^j\frac{\alpha_2\gamma_{th}^{j+1}\sigma_{n,\mathrm{S}}^{2(j+1)}}{(j+1)!b_2^jP_0^{j+1}}{}_2F_2(j+1,m_2;j+2,1;\frac{\sigma_2\gamma_{th}\sigma_{n,\mathrm{S}}^2}{P_0}).\end{aligned}$$

Here, h_{GwS} denotes the channel coefficient of the gateway-satellite link; B_{Gw} denotes the bandwidth of the gateway-satellite link; P_0 is the gateway transmit power; $\sigma_{n,\mathrm{S}}^2$ represents the variance of the AWGN at satellite; $(m_2; b_2; \Omega_2)$ is the satellite uplink channel parameter as in (1); ${}_2F_2$ is the confluent hypergeometric function of the second kind. $F_{\gamma_{\text{Gw}}}(\gamma_{th})$ is found following [30, eq.(3)]. □

V. Numerical Results

In this section, the numerical results are presented to validate the theoretical analysis. The simulation is done using Monté Carlo method. Throughout the experiments in this paper, the value of key parameters are always set as in Table I, unless otherwise specified. The user and eavesdropper are randomly placed inside a circle with radius $10\,km$ and center at ground station G.

TABLE I: Parameters used for numerical results.

Parameter	**Description**	**Value**
N	Number of files	500
F	File size	100 Mb
C_1/C_2	Cache capacity	30/10 Gb
M	IRS reflective elements	50
α_s/α_g	Path-loss exponent	2/3
$d_{\mathrm{SI}} = d_{\mathrm{GwS}}/d_{\mathrm{GI}}$	Distance	$35,786/5\,km$
$\sigma_{n,\mathrm{S}}^2 = \sigma_{n,\mathrm{U}}^2 = \sigma_{n,\mathrm{E}}^2$	Receiver noise	$-130\,dBm/Hz$
$m_{1_i}/b_{1_i}/\Omega_{1_i}$	Sat. downlink parameter	5/0.251/0.279
$m_2/b_2/\Omega_2$	Sat. uplink parameter	4/0.126/0.835
$R_{e,1} = R_{e,2}$	Redundant rate	$5\,bits/s/Hz$
$R_{s,1} = R_{s,2}$	Secrecy rate	$1\,bits/s/Hz$
$P_0/P_1/P_2$	Transmit power	$30/3/20\,W$

Fig. 2 and Fig. 3 depict the CP and SP when the satellite and ground station transmit powers vary. The results from Monté Carlo simulation match well with the theoretical values. The asymptotic $p_{c,2}$ in (10) and $p_{s,2}$ in (14) achieve high accuracy comparing to their exact values in the integral forms. As expected in the theoretical analysis, when the transmit power increases, the CP increases and the SP decreases. It is also observed from Fig. 2 that the satellite-IRS-user scheme provide better reliability performance than that of the ground station-IRS-user scheme. For transmission secrecy in Fig. 3,

Fig. 2: Connection probability vs. transmit power.

Fig. 3: Secrecy probability vs. transmit power.

the ground station-IRS-user scheme performs better; and both schemes yield higher SP in the low transmit power regime but get small value of SP in the high transmit power regime.

In Figs. 4 and 5, the CP and SP are plotted as functions of the redundant rate $R_{e,i}$. The high accuracies of the theoretical results to the simulation and the asymptotic values to the exact values are confirmed. The behavior of CP and SP of the two schemes is expected as the CP decreases and the SP increases when increasing the redundant rate. The CP in ground station-IRS-user case reaches saturation at $R_{e,1} = 6.5\, bits/s/Hz$, and the SP does at $R_{e,1} = 8\, bits/s/Hz$. In satellite-IRS-user case, the CP starts to decrease very slowly when $R_{e,2}$ passes 12.5 $bits/s/Hz$, and the SP reaches saturation at $R_{e,2} = 11.5\, bits/s/Hz$.

The system STP in (4) versus the redundant rate with different caching probability is depicted in Fig. 6. It is observed that p_{secure} increases significantly when the redundant rates pass $5\, bits/s/Hz$, and p_{secure} reaches is maximal value at $R_{e,i} = 11.25\, bits/s/Hz$. As indicated by the dash line in Fig. 6, at the maximum p_{secure}, the value of $R_{e,i}$ is not affected by different caching probability of $[\mathcal{A}_1, \mathcal{A}_2]_i$, which verifies the independence in optimizing the redundant rate and the caching probability. Fig. 7 shows the relationship between the number of IRS reflective elements and the STP. Larger number of reflective elements improves the system transmission security. When $R_{e,1}$ and $R_{e,2}$ are set to $5\, bits/s/Hz$, double the reflective elements enhances the p_{secure} by up to 25% in the less-than-50-element regime. When $R_{e,1}$ and $R_{e,2}$ are set to $11.25 bits/s/Hz$, which is the value where p_{secure} is highest in Fig. 6, double the reflective elements can improve the p_{secure} by up to 18% in the more-than-50-element regime. Note that even the p_{secure} is improved when using larger IRS, the p_{secure} is in a low range of probability when $R_{e,1}$ and $R_{e,2}$ are set to $5\, bits/s/Hz$ and in a higher range for the other case. This implies the importance of optimizing the redundant rates $R_{e,i}$ to not only achieve the maximum p_{secure} but also save the resources.

Fig. 4: Connection probability vs. redundant rate.

Fig. 5: Secrecy probability vs. redundant rate.

To confirm the effect of having IRS in the system on the transmission secrecy, the simulation is set up for the ground

Fig. 6: System secure transmission probability vs. redundant rate.

Fig. 7: System secure transmission probability vs. number of reflective elements on IRS.

station-IRS-user scheme with and without IRS. The cache enabled terrestrial system without IRS is adopted from [9], [10], [13] with single base station. The results are presented in Fig. 8. The secrecy probability in case of having only the direct link from ground station to user is significantly less than the one having IRS. Having IRS can improve the secrecy probability by at most 50% when $R_{e,1}$ passes $8\, bits/s/Hz$.

Fig. 8: The secure transmission probability of ground station-IRS-user scheme with and without IRS.

In Fig. 9, the secrecy performance between two-tier versus single-tier cache-enabled systems is compared. The single-tier cache-enabled system is adopted from [2], [31] where the caching capability is only enabled at ground station with the caching probability $\mathcal{A}_1$. It is observed that our proposed system outperforms the single-tier cache-enabled system by almost 50% at the maximum p_{secure}. And the result once again confirms the independence in optimizing the redundant rate and the caching probability of single-tier and/or two-tier cache.

Fig. 10 shows how the optimal redundant rates solution $R^*_{e,i}$ is influenced by the secrecy rates. These are the solutions for the first-step optimization problem in (16). Corresponding to the optimal $R^*_{e,i}$, the optimal system STP is depicted in Fig. 11. These optimal p^*_{secure} values are obtained as the solutions for the optimization problem in (15) after achieving the optimal caching probability $[\mathcal{A}^*_1, \mathcal{A}^*_2]$. At $R_{s,1} = R_{s,2} = 1\, bits/s/Hz$, the optimal p^*_{secure} is at 80% with $R^*_{e,1} = 5.5\, bits/s/Hz$ and $R^*_{e,2} = 11\, bits/s/Hz$, while the non-optimized p_{secure} (in Fig. 6) only achieves its highest value at 72% with $R_{e,1} = R_{e,2} = 11.25\, bits/s/Hz$. To further compare the optimal probabilistic caching policy, the system STP under ground station and satellite most popular caching policies [6] are also provided in Fig. 11. As expected, the optimal probabilistic caching policy gives the best performance. The ground station most popular caching policy performance is not as good as that of the ground station most popular caching policy and surpasses its opponent when the secrecy rates are more than $3.5\, bits/s/Hz$.

Fig. 9: The secure transmission probability comparison between single-tier vs. two-tier cache-enabled systems.

Fig. 10: The optimal redundant rate, $R_{e,i}$ with respect to secrecy rate.

VI. Conclusions

In this paper, we proposed a novel two-hop content delivery scheme in an IRS-assisted cache-enabled STN with probabilistic caching policies at both the satellite and ground station. We evaluated the system's connection probability and secrecy probability using asymptotic and closed-form expressions. By jointly designing the transmission rates and caching probability, we were able to maximize the system's secure transmission probability. Our numerical results confirmed the validity of the theoretical analysis and demonstrated that having an IRS and two cache tiers can improve the secrecy probability by almost 50%. Moreover, our results emphasized the importance of optimizing the redundant rate to achieve the highest secure transmission probability while saving resources.

Fig. 11: The optimal secure transmission probability, p^*_{secure} vs. secrecy rate, $R_{s,i}$.

Appendix A
Proof of Theorem 1

Let $X_c = \left|h_{\text{GU}} + \sum_{i=1}^{M} h_{\text{GI}_i} h_{\text{I}_i\text{U}} e^{j\phi_{1,i}}\right|^2$ with its mean value is computed as follows,

$$\begin{aligned}\mathbb{E}(X_c) =& \mathbb{E}\left\{\left|h_{\text{GU}} + \sum_{i=1}^{M} h_{\text{GI}_i} h_{\text{I}_i\text{U}} e^{j\phi_{1,i}}\right|^2\right\}\\ =& \mathbb{E}\{|h_{\text{GU}}|^2\} + 2\mathbb{E}\left\{h_{\text{GU}} \sum_{i=1}^{M} h_{\text{GI}_i} h_{\text{I}_i\text{U}} e^{j\phi_{1,i}}\right\} \qquad (24)\\ &+ \mathbb{E}\left\{\left|\sum_{i=1}^{M} h_{\text{GI}_i} h_{\text{I}_i\text{U}} e^{j\phi_{1,i}}\right|^2\right\}.\end{aligned}$$

Let denote $\bar{h}_{mn}$ the average channel power gain of the link between node m and n, then

$$\mathbb{E}(X_c) = 2\bar{h}_{\mathrm{GU}}^2 d_{\mathrm{GU}}^{-2\alpha_g} + 2\bar{h}_{\mathrm{GU}}(d_{\mathrm{GU}}d_{\mathrm{IU}}d_{\mathrm{GI}})^{-\alpha_g}\sum_{i=1}^{M}\Delta_i$$
$$+ (d_{\mathrm{IU}}d_{\mathrm{GI}})^{-2\alpha_g}\sum_{r_1+\cdots+r_M=2}\left\{\binom{2}{r_1,\cdots,r_M}\prod_{i=1}^{M}(r_i!)^2\Delta_i^{r_i}\right\} \tag{25}$$

where $\Delta_i = \bar{h}_{\mathrm{I}_i\mathrm{U}}\bar{h}_{\mathrm{GI}_i}e^{j\phi_{1,i}}$ and $\binom{2}{r_1,\cdots,r_M} = \frac{2!}{r_1!\cdots r_M!}$.

The second moment of X_c, denoted as $\mathbb{E}(X_c^2)$, is computed as follows,

$$\begin{aligned}\mathbb{E}(X_c^2) =&\mathbb{E}\left\{\left|h_{\mathrm{GU}} + \sum_{i=1}^{M}h_{\mathrm{GI}_i}h_{\mathrm{I}_i\mathrm{U}}e^{j\phi_{1,i}}\right|^4\right\}\\ =&\mathbb{E}\Bigg\{\Bigg|\underbrace{|h_{\mathrm{GU}}|^2}_{a} + \underbrace{2h_{\mathrm{GU}}\sum_{i=1}^{M}h_{\mathrm{GI}_i}h_{\mathrm{I}_i\mathrm{U}}e^{j\phi_{1,i}}}_{b}\\ &+ \underbrace{\left|\sum_{i=1}^{M}h_{\mathrm{GI}_i}h_{\mathrm{I}_i\mathrm{U}}e^{j\phi_{1,i}}\right|^2}_{c}\Bigg|^2\Bigg\}\\ =&\mathbb{E}\{|a|^2\} + 2\mathbb{E}\{ab\} + 2\mathbb{E}\{bc\} + 2\mathbb{E}\{ac\}\\ &+ \mathbb{E}\{|b|^2\} + \mathbb{E}\{|c|^2\}.\end{aligned} \tag{26}$$

$\mathbb{E}\{|a|^2\} = \mathbb{E}\{|h_{\mathrm{GU}}|^4\} = 4!\bar{h}_{\mathrm{GU}}^4 d_{\mathrm{GU}}^{-4\alpha_g}$ is calculated as the fourth moment of the exponential random variable h_{GU}.

Let $\Theta_l = \sum_{r_1+\cdots+r_M=l}\left\{\binom{l}{r_1,\cdots,r_M}\prod_{i=1}^{M}(r_i!)^2\Delta_i^{r_i}\right\}$, $l = 2, 3, 4$. Using multinomial theorem, the other terms in (26) can be obtained as

$$\begin{aligned}\mathbb{E}\{ab\} &= 12\bar{h}_{\mathrm{GU}}^3 d_{\mathrm{GU}}^{-3\alpha_g}(d_{\mathrm{IU}}d_{\mathrm{GI}})^{-\alpha_g}\sum_{i=1}^{M}\Delta_i,\\ \mathbb{E}\{bc\} &= 2\bar{h}_{\mathrm{GU}}d_{\mathrm{GU}}^{-\alpha_g}(d_{\mathrm{IU}}d_{\mathrm{GI}})^{-3\alpha_g}\Theta_3,\\ \mathbb{E}\{ac\} &= 2\bar{h}_{\mathrm{GU}}^2(d_{\mathrm{GU}}d_{\mathrm{IU}}d_{\mathrm{GI}})^{-2\alpha_g}\Theta_2,\\ \mathbb{E}\{|b|^2\} &= 8\bar{h}_{\mathrm{GU}}^2(d_{\mathrm{GU}}d_{\mathrm{IU}}d_{\mathrm{GI}})^{-2\alpha_g}\Theta_2,\\ \mathbb{E}\{|c|^2\} &= (d_{\mathrm{IU}}d_{\mathrm{GI}})^{-4\alpha_g}\Theta_4.\end{aligned}$$

The variance of random variable X_c is computed as

$$\begin{aligned}\mathrm{Var}(X_c) =&\mathbb{E}(X_c^2) - |\mathbb{E}(X_c)|^2\\ =&20\bar{h}_{\mathrm{GU}}^4 d_{\mathrm{GU}}^{-4\alpha_g} + 8\bar{h}_{\mathrm{GU}}^3 d_{\mathrm{GU}}^{-3\alpha_g}(d_{\mathrm{IU}}d_{\mathrm{GI}})^{-\alpha_g}\left(3\sum_{i=1}^{M}\Delta_i - 1\right)\\ &+ 4\bar{h}_{\mathrm{GU}}^2(d_{\mathrm{GU}}d_{\mathrm{IU}}d_{\mathrm{GI}})^{-2\alpha_g}\left(3\Theta_2 - \sum_{i=1}^{M}\Delta_i\right)\\ &+ 4\bar{h}_{\mathrm{GU}}d_{\mathrm{GU}}^{-\alpha_g}(d_{\mathrm{IU}}d_{\mathrm{GI}})^{-3\alpha_g}\Theta_3 + (d_{\mathrm{IU}}d_{\mathrm{GI}})^{-4\alpha_g}\Theta_4\\ &- 4\bar{h}_{\mathrm{GU}}^2(d_{\mathrm{GU}}d_{\mathrm{IU}}d_{\mathrm{GI}})^{-2\alpha_g}\left(\sum_{i=1}^{M}\Delta_i\right)^2\\ &- (d_{\mathrm{IU}}d_{\mathrm{GI}})^{-3\alpha_g}\Theta_2\left((d_{\mathrm{IU}}d_{\mathrm{GI}})^{-\alpha_g}\Theta_2 + 4\bar{h}_{\mathrm{GU}}d_{\mathrm{GU}}^{-\alpha_g}\sum_{i=1}^{M}\Delta_i\right).\end{aligned} \tag{27}$$

Matching random variable X_c to Gamma distribution with shape parameter $k_c = \frac{|\mathbb{E}(X_c)|^2}{\mathrm{Var}(X_c)}$ and scale parameter $w_c = \frac{\mathrm{Var}(X_c)}{\mathbb{E}(X_c)}$. Exploiting (25) and (27), the closed-form expression of $p_{c,1}$ is obtained.

Appendix B
Proof of Proposition 1

Let define a new variable $Y_i = h_{\mathrm{I}_i\mathrm{U}}e^{j\phi_{2,i}}$ which has the density function $f_{Y_i}(y_i) = \frac{1}{\bar{h}_{\mathrm{I}_i\mathrm{U}}d_{\mathrm{IU}}^{-\alpha_g}e^{j\phi_{2,i}}}e^{\frac{-y_i}{\bar{h}_{\mathrm{I}_i\mathrm{U}}d_{\mathrm{IU}}^{-\alpha_g}e^{j\phi_{2,i}}}}$, and $V_i = h_{\mathrm{SI}_i}Y_i$, then

$$p_{c,2} = \mathbb{P}\left\{\sum_{i=1}^{M}V_i \geq \sqrt{z_2}\right\}. \tag{28}$$

The density function $f_{V_i}(v)$ is found using inverse Mellin transform as follows.

Applying Mellin transform for exponential functions [32, eq.(6.3.1)] and higher functions [32, eq.(6.9.9)], then

$$\mathcal{M}\left[f_{Y_i}(y_i), s\right] = \frac{1}{\bar{h}_{\mathrm{I}_i\mathrm{U}}d_{\mathrm{IU}}^{-\alpha_g}e^{j\phi_{2,i}}}^{-s+1}\Gamma(s), \tag{29}$$

and

$$\mathcal{M}\left[f_{h_{\mathrm{SI}_i}}(x_i), s\right] = d_{\mathrm{SI}}^{-\alpha_s}\alpha_{1_i}\left(1/b_{1_i}\right)^{-s}\Gamma(s)\,{}_2F_1\left(m_{1_i}, s; 1; \sigma_{1_i}b_{1_i}\right) \tag{30}$$

where ${}_2F_1(a, b; c; z) = \sum_{n=0}^{\infty}\frac{(a)_n(b)_n}{(c)_n}\frac{z^n}{n!}$ is the Gauss hypergeometric function [24, eq.(9.10.1)] with $(a)_n = \frac{\Gamma(a+n)}{\Gamma(a)}$ denotes the Pochhammer's symbol, and $f_{h_{\mathrm{SI}_i}}(x_i)$ follows Shadowed-Rician distribution in (1).

Upon substituting (29) and (30) into the Mellin transform of $f_{V_i}(v_i)$, which is $\mathcal{M}\left[f_{V_i}(v_i), s\right] = \mathcal{M}\left[f_{h_{\mathrm{SI}_i}}(x_i), s\right]\mathcal{M}\left[f_{Y_i}(y_i), s\right]$ [33], the density function $f_{V_i}(v_i)$ can be expressed as

$$\begin{aligned}f_{V_i}(v_i) =&\frac{2d_{\mathrm{SI}}^{-\alpha_s}\alpha_{1_i}}{\bar{h}_{\mathrm{I}_i\mathrm{U}}d_{\mathrm{IU}}^{-\alpha_g}e^{j\phi_{2,i}}}\sum_{n=1}^{\infty}\Bigg(\frac{(\sigma_{1_i}b_{1_i})^n}{n!}\cdot\frac{(m_{1_i})_n}{(1)_n}\\ &\times\left(\sqrt{\frac{v_i}{(\bar{h}_{\mathrm{I}_i\mathrm{U}}d_{\mathrm{IU}}^{-\alpha_g}e^{j\phi_{2,i}}b_{1_i})}}\right)^n K_n\left(2\sqrt{\frac{v_i}{\bar{h}_{\mathrm{I}_i\mathrm{U}}d_{\mathrm{IU}}^{-\alpha_g}e^{j\phi_{2,i}}b_{1_i}}}\right)\Bigg)\end{aligned} \tag{31}$$

where $K_n(.)$ is the modified Bessel function of the second kind.

Since $\{V_i\}_{i=1}^{M}$ are independent and following the factorization theorem, the join density function can be given by

$$f_{V_1,\ldots,V_M}(v_1, \ldots, v_M) = \prod_{i=1}^{M}f_{V_i}(v_i). \tag{32}$$

Substituting (31) and (32) into (28) then changing $\sqrt{z_2}u_i = 2\sqrt{\frac{v_i}{\bar{h}_{\mathrm{I}_i\mathrm{U}}d_{\mathrm{IU}}^{-\alpha_g}e^{j\phi_{2,i}}b_{1_i}}}$ arrives at (11).

References

[1] Q. T. Ngo, K. T. Phan, W. Xiang, A. Mahmood, and J. Slay, "On edge caching in satellite — IoT networks," *IEEE Internet of Things Mag.*, vol. 4, no. 4, pp. 107–112, 2021.

[2] T. Vu, Y. Poirier, S. Chatzinotas, and N. Maturo, "Modeling and implementation of 5G edge caching over satellite," *Int. J. Sat. Commun. Netw.*, vol. 38, no. 5, pp. 395–406, Mar. 2020.

[3] H. Wu, J. Li, H. Lu, and P. Hong, "A two-layer caching model for content delivery services in satellite-terrestrial networks," in *2016 IEEE Global Commun. Conf. (GLOBECOM)*, DC, USA, 2016, pp. 1–6.

[4] C.-T. Yen, F.-T. Chien, and M.-K. Chang, "Cooperative online caching in small cell networks with limited cache size and unknown content popularity," in *2018 Int. Conf. Comput. Commun. Syst. (ICCCS)*, 2018, pp. 173–177.

[5] K. An, Y. Li, X. Yan, and T. Liang, "On the performance of cache-enabled hybrid satellite-terrestrial relay networks," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1506–1509, Jun. 2019.

[6] Q. T. Ngo, K. T. Phan, W. Xiang, A. Mahmood, and J. Slay, "Two-tier cache-aided full-duplex hybrid satellite-terrestrial communication networks," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 3, pp. 1753–1765, 2022.

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

[8] W. Zhao, Z. Chen, K. Li, N. Liu, B. Xia, and L. Luo, "Caching-aided physical layer security in wireless cache-enabled heterogeneous networks," *IEEE Access*, vol. 6, pp. 68 920–68 931, Dec. 2018.

[9] T. Zheng, H. Wang, and J. Yuan, "Secure and energy-efficient transmissions in cache-enabled heterogeneous cellular networks: Performance analysis and optimization," *IEEE Trans. Commun.*, vol. 66, no. 11, pp. 5554–5567, Nov. 2018.

[10] T. X. Zheng, H. M. Wang, and J. Yuan, "Physical-layer security in cache-enabled cooperative small cell networks against randomly distributed eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 5945–5958, 2018.

[11] L. Xiang, D. W. K. Ng, R. Schober, and V. W. S. Wong, "Cache-enabled physical layer security for video streaming in backhaul-limited cellular networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 2, pp. 736–751, 2018.

[12] S. Zhang, W. Sun, J. Liu, and K. Nei, "Physical layer security in large–scale probabilistic caching: Analysis and optimization," *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1484–1487, 2019.

[13] S. Li, W. Sun, H. Zhang, and Y. Zhang, "Physical layer security for edge caching in 6G networks," in *GLOBECOM 2020 - 2020 IEEE Global Commun. Conf.*, 2020, pp. 1–6.

[14] T.-X. Zheng, H.-W. Liu, N. Zhang, Z. Ding, and V. C. M. Leung, "Secure content delivery in two-tier cache-enabled mmwave heterogeneous networks," *IEEE Trans. Inf. Forensics and Secur.*, vol. 16, pp. 1640–1654, Nov. 2021.

[15] Y. Wang, H. Lu, D. Zhao, Y. Deng, and A. Nallanathan, "Wireless communication in the presence of illegal reconfigurable intelligent surface: Signal leakage and interference attack," *IEEE Wireless Commun.*, vol. 29, no. 3, pp. 131–138, 2022.

[16] H.-M. Wang, J. Bai, and L. Dong, "Intelligent reflecting surfaces assisted secure transmission without eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 27, pp. 1300–1304, 2020.

[17] C. Wang, Z. Li, T.-X. Zheng, D. W. K. Ng, and N. Al-Dhahir, "Intelligent reflecting surface-aided secure broadcasting in millimeter wave symbiotic radio networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 10, pp. 11 050–11 055, 2021.

[18] L. Dong, H.-M. Wang, and J. Bai, "Active reconfigurable intelligent surface aided secure transmission," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 2181–2186, 2022.

[19] W. Wang, X. Liu, J. Tang, N. Zhao, Y. Chen, Z. Ding, and X. Wang, "Beamforming and jamming optimization for IRS-aided secure NOMA networks," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1557–1569, 2022.

[20] X. Wu, J. Ma, Z. Xing, C. Gu, X. Xue, and X. Zeng, "Secure and energy efficient transmission for irs-assisted cognitive radio networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 8, no. 1, pp. 170–185, 2022.

[21] Y. Ge and J. Fan, "Robust secure beamforming for intelligent reflecting surface assisted full-duplex MISO systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 253–264, 2022.

[22] L. Breslau, P. Cao, L. Fan, G. Phillips, and S. Shenker, "Web caching and Zipf-like distributions: Evidence and implications," in *IEEE Conf. Comput. Commun. Soc. (INFOCOM)*, NY, USA, 1999, pp. 126 – 134.

[23] A. Abdi, W. C. Lau, M. 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.

[24] I. S. Gradshteyn and I. M. Ryzhik, *Tables of Integrals, Series and Products*, vol. 6th ed., 2000.

[25] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

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

[27] Q. Wu, S. Zhang, B. Zheng, C. You, and R. Zhang, "Intelligent reflecting surface-aided wireless communications: A tutorial," *IEEE Trans. Commun.*, vol. 69, no. 5, pp. 3313–3351, 2021.

[28] M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions with formulas, graphs, and mathematical tables*. US Government printing office, 1964, vol. 55.

[29] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[30] W. Cao, Y. Zou, Z. Yang, and J. Zhu, "Secrecy outage probability of hybrid satellite-terrestrial relay networks," in *GLOBECOM 2017 - 2017 IEEE Global Commun. Conf.*, Singapore, 2017, pp. 1–5.

[31] A. Kalantari, M. Fittipaldi, S. Chatzinotas, T. X. Vu, and B. Ottersten, "Cache-assisted hybrid satellite-terrestrial backhauling for 5G cellular networks," in *2017 IEEE Global Commun. Conf. (GLOBECOM)*, Singapore, 2017, pp. 1–6.

[32] B. Manuscript, H. Bateman, and A. Erdélyi, "Tables of integral transforms," *The Mathematical Gazette*, vol. 39, p. 337, 1955.

[33] B. Epstein, "Some Applications of the Mellin Transform in Statistics," *The Annals of Mathematical Statistics*, vol. 19, no. 3, pp. 370 – 379, 1948.

Quynh T. Ngo (Member, IEEE) Dr. Quynh Ngo is currently a Postdoctoral Research Fellow at the School of Electrical and Data Engineering, University of Technology Sydney, Sydney, Australia. She received a B.Sc. in Electrical Engineering (Magna Cum Laude) from California State University Los Angeles, CA, USA, in 2013, an M.Sc. in Telecommunications from Vietnam National University - University of Sciences, HCM, Vietnam, in 2016, and a PhD in Computer Science from La Trobe University, Melbourne, Australia, in 2023. Her PhD thesis was nominated for the Nancy Millis Award for the top 5% of theses at La Trobe University. Her research interests include vehicular ad-hoc networks, IoT networks, intelligent non-terrestrial networks, and machine learning in wireless communication and networking. She has been awarded the Jet Propulsion Laboratory Undergraduate Scholar (JPLUS), the visiting research award funded by the Norwegian-Vietnamese Industrial & Infrastructure Safety Consortium, the La Trobe University Postgraduate Research Scholarship, and the Net Zero Scholarship.

Khoa T. Phan (Member, IEEE) Dr. Phan received the B.Eng. degree in telecommunications (First Class Hons.) from the University of New South Wales (UNSW), Sydney, NSW, Australia, in 2006, the M.Sc. degree in electrical engineering from the University of Alberta, Edmonton, AB, Canada, in 2008, and California Institute of Technology (Caltech), Pasadena, CA, USA, in 2009, respectively, and the Ph.D. degree in electrical engineering from McGill University, Montreal, QC, Canada in 2017. He is currently a Senior Lecturer and Australia Research Council (ARC) Discovery Early Career Researcher Award (DECRA) Fellow with the Department of Computer Science and Information Technology, La Trobe University, Victoria, Australia. His current research interests are broadly design, control, optimization, and operation of 5G mobile communications networks with applications in the Internet of Things (IoT), satellite communications, machine-type communications (MTC), smart grids, and cloud computing.

Wei Xiang (Senior Member, IEEE) Professor Wei Xiang is Cisco Research Chair of AI and IoT and Director of the Cisco-La Trobe Centre for AI and IoT at La Trobe University. Previously, he was Foundation Chair and Head of Discipline of IoT Engineering at James Cook University, Cairns, Australia. He is an elected Fellow of the IET in UK and Engineers Australia. He received the TNQ Innovation Award in 2016, and Pearcey Entrepreneurship Award in 2017, and Engineers Australia Cairns Engineer of the Year in 2017. He has published over 250 peer-reviewed papers including 3 books and 200 journal articles. He has severed in a large number of international conferences in the capacity of General Co-Chair, TPC Co-Chair, Symposium Chair, etc. His research interest includes the Internet of Things, wireless communications, machine learning for IoT data analytics, and computer vision.

Abdun Mahmood (Senior Member, IEEE) Dr. Abdun Mahmood received his PhD from the University of Melbourne, Australia, in 2008 the MSc (Research) degree in computer science and the B.Sc. degree in applied physics and electronics from the University of Dhaka, Bangladesh, in 1999 and 1997, respectively. Dr. Mahmood had an academic career in University since 2000, working at University of Dhaka, RMIT University, UNSW Canberra and currently in La Trobe University as an Associate Professor (Reader).

Dr. Mahmood leads a group of researchers focusing on Machine Learning and Cybersecurity including Anomaly Detection in Smart Grid, SCADA security, Memory Forensics, and False Data Injection. Dr. Mahmood has been successful to attract over a $1M+ in grant funding as a CI, including two ARC Linkage Projects.