Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 11, No. 04, December 2025.

SECURE PERFORMANCE ANALYSIS OF SATELLITE-TERRESTRIAL NETWORKS-ASSISTED BACKSCATTER DEVICE

Hong-Nhu Nguyen[1], Si-Phu Le[2], Quang-Sy Vu[3], Quang-Sang Nguyen[4] and Erik Chromy[5]

(Received: 10-Sep.-2025, Revised: 26-Oct.-2025, Accepted: 26-Oct.-2025)

ABSTRACT

This study investigates the secrecy performance of a satellite-backscatter device communication system in the presence of a potential eavesdropper. In the considered setup, a satelite transmits signals to a backscatter device, which reflects the modulated information back to the satellite while being subject to interception by an eavesdropper. To capture the practical wireless environment, the analysis is conducted over correlated Nakagami-m fading channels, where the coupling among the forward, backscatter, and wiretap links is explicitly taken into account. We derive exact closed-form analytical expressions for key secrecy metrics; namely, the secrecy outage probability (SOP), the ergodic secrecy capacity (ESC), and the symbol error rate (SER), which provide comprehensive insights into the secure operation of the system. Furthermore, asymptotic expressions are obtained for the SOP, enabling a deeper understanding of the secrecy diversity order under high signal-to-noise ratio (SNR) regimes. The impacts of critical channel and system parameters, such as fading severity, correlation, user power, and eavesdropper power, on the SOP, ESC, and SER are thoroughly examined. Monte Carlo simulations are also performed to validate the accuracy of the theoretical analysis.

KEYWORDS

Backscatter communication, Secrecy outage probability, Ergodic secrecy capacity, Symbol error rate, Physical layer security.

1. INTRODUCTION

Backscatter communications play an important role in the Internet of Things (IoT) due to their low cost and energy efficiency [1]-[2]. Radio Frequency Identification (RFID) is a typical backscatter communication system, which utilizes backscatter modulation to enable data transmission [3]. In contrast to traditional communication systems, RFID includes both forward and backscatter links. Specifically, in [4]-[5], the authors proposed a dyadic backscatter channel model for RFID systems, incorporating both forward and backscatter links. In practice, these links can be correlated, since the transmit and receive antennas at the reader may be very close or even co-located [6]. The authors in [7] analyzed the range performance of ultrahigh-frequency-band passive RFID for single-input single-output (SISO) and multiple-input multiple-output (MIMO) systems with maximal-ratio combining in a pinhole channel, and modeled it as a correlated Nakagami-m distribution. Similar to other wireless systems, privacy and security are also major concerns for RFID systems. Due to their broadcast nature, RFID systems are vulnerable to potential eavesdropping attacks. In the open literature, several works have proposed lightweight cryptography to address RFID security challenges [8]. Although cryptography can provide improved security performance, it incurs high communication overhead and computational complexity.

Recently, physical layer security (PLS) for backscatter networks has received increasing attention. For instance, Li et al. [10] investigated PLS in wireless-powered ambient backscatter cooperative networks, deriving secrecy rate and outage expressions under practical energy-harvesting and cooperation settings. Similarly, Khan et al. [11] analyzed the secrecy performance of energy-harvesting backscatter systems under various tag-selection strategies, while [12] introduced a deep learning-based secure tag-selection

1. H.-N. Nguyen is with the Faculty of Technology and Engineering, Saigon University, Ho Chi Minh City, Vietnam. Email: nhu.nh@sgu.edu.vn
2. S.-P. Le is with the Faculty of Electrical Engineering and Computer Science, VSB-Technical University of Ostrava, Ostrava, Czech Republic. Email: phu.si.le@vsb.cz
3. Q.-S. Vu (Corresponding Author) is with the Advanced Intelligent Technology Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam. Email: vuquangsy@tdtu.edu.vn
4. Q.-S. Nguyen is with the Posts and Telecommunications Institute of Technology, Ho Chi Minh City, Vietnam. Email: sangnq@ptit.edu.vn
5. E. Chromy is with the Faculty of Informatics, Pan-European University, Bratislava, Slovakia. Email: erik.chromy@paneurouni.com

method to mitigate RIS-induced interference, highlighting the growing role of AI in BackCom security. Moreover, the authors in [15] examined the secrecy performance of backscatter communication networks with multiple readers and different tag-selection schemes, demonstrating that optimized reader-tag pairing can significantly improve secrecy capacity. In addition, [16] further extended the analysis by considering Nakagami-m fading and energy-harvesting capability at the tag, providing secrecy-outage analysis under generalized fading conditions and highlighting that both fading characteristics and tag-selection strategies play critical roles in ensuring physical layer security in BackCom networks. To address the limitations of existing RFID systems in terms of cost, size, and computational complexity, we consider physical layer security (PLS) as an alternative to cryptography. The main idea of PLS is to exploit the wireless-channel characteristics to prevent eavesdroppers from obtaining information from the transmitter. The authors in [17] studied the PLS of a single-reader single-tag RFID system, where the reader not only sends the query signal to power the tag, but also injects artificial noise to interfere with an eavesdropper. Moreover, the authors in [18, 19] investigated secrecy-rate maximization in a MIMO RFID system by jointly optimizing the supply energy and the artificial-noise precoding matrix at the reader. Building upon the idea of combining MIMO and intelligent surfaces for rate and security optimization, Paul et al. [9] developed a quantum gradient descent algorithm for rate maximization in MIMO-NOMA systems assisted by STAR-RIS, achieving superior convergence and energy efficiency compared to classical optimization methods. Recent advances in wireless communication have significantly improved satellite-terrestrial integrated networks, especially regarding cooperative relaying and security under practical impairments. For instance, the authors in [20] investigated the outage behavior of satellite-terrestrial full-duplex relay networks under co-channel interference, revealing robust relaying strategies that enhance end-to-end reliability in hybrid space-ground scenarios. Similarly, energy-harvesting-based spectrum access has emerged as a practical solution for resource-constrained systems. A notable contribution by the authors in [21] proposed incremental cooperation and relay-selection mechanisms while considering hardware noise in terrestrial networks, demonstrating the potential of green communication for spectrum efficiency. In the same direction, full-duplex relaying under imperfect channel state information (CSI) has been explored using time-switching protocols, further highlighting the viability of practical wireless relaying models in terrestrial setups [22]. Security remains a paramount concern in such systems, particularly in cognitive and cooperative environments. Addressing this, the authors in [23] presented secrecy-performance enhancement techniques in underlay cognitive radio networks through multi-hop cooperative transmission, including scenarios with hardware impairments. Additionally, the authors in [24] demonstrated how coverage-area granularity directly affects predictive-modeling accuracy for mobility systems in 5G/6G cellular architectures. Considering practical conditions, the authors in [25] analyzed the performance of SWIPT-aided satellite-terrestrial cooperative networks, while [26] addressed secure communication techniques for multi-tag backscatter systems. These insights can be leveraged to enhance security and efficiency in practical IoT deployments. Furthermore, Nguyen et al. [13] analyzed secure wireless communications incorporating energy harvesting and multi-antenna diversity, demonstrating that efficient energy management and antenna diversity can substantially enhance secrecy capacity. In addition, Garai et al. [14] examined ground-to-satellite free-space optical (FSO) communications under atmospheric turbulence, showing that appropriate modulation selection improves reliability in hybrid space-ground systems. However, the aforementioned works have not derived an analytical expression for the system secrecy outage probability (SOP).

Motivation and Contribution

Building on the foundations of RFID and backscatter communications, a growing body of literature has expanded this paradigm to address interference, fading, resource allocation, and physical layer security in more sophisticated scenarios. For instance, interference and fading have been identified as fundamental bottlenecks, with potential mitigation strategies proposed in [30]. To enhance system capacity and connectivity, NOMA-based backscatter communications have been extensively investigated, ranging from comprehensive surveys of IoT applications [31] to fundamental designs and advanced techniques [32]. Beyond multiple access, integrated designs, such as power-efficient beamforming for joint sensing and communication [33] and fluid antenna systems to overcome fading [34], have been explored. In parallel, the integration of backscatter with intelligent meta-surfaces has received great attention. Joint waveform and reflection optimization for secure RIS-based backscatter

was proposed in [35], while [40] analyzed the performance of RIS-assisted ambient backscatter systems. Short-packet communications, essential for ultra-reliable and low-latency IoT, have also been investigated in RIS-assisted NOMA backscatter systems [38]. In addition, symbiotic paradigms have been studied, including power beacon-assisted energy harvesting [39] and cognitive backscatter-enabled blockchain consensus [37]. Moreover, security has likewise remained an active research topic. For example, UAV-assisted backscatter with jamming was investigated in [36], multi-power beacon IoT systems were examined for secrecy performance in [42], and D2D partial NOMA-assisted backscatter networks were analyzed in [41]. Collectively, these studies highlighted the rapid evolution of backscatter communications across efficiency, reliability, and security dimensions. However, analytical characterization of secrecy-outage probability (SOP), ergodic secrecy capacity (ESC), and symbol error rate (SER) under correlated fading channels remains largely unexplored, which motivates our work. Our work provides a comprehensive security analysis of satellite-assisted backscatter communication, offering novel analytical insights and practical design guidelines. The main contributions are summarized as follows:

- **Novel System Modeling under Correlated Fading:** We establish a first-of-its-kind, comprehensive analytical model for the satellite-backscatter-eavesdropper system under correlated Nakagami-m fading channels, explicitly accounting for the practical coupling effect among the forward, backscatter, and wiretap links.
- **Exact Closed-form Secrecy Metrics:** We successfully derive novel and exact closed-form analytical expressions for the key physical layer security metrics: the Secrecy Outage Probability (SOP), the Ergodic Secrecy Capacity (ESC), and the Symbol Error Rate (SER), comprehensively characterizing the system's vulnerability to eavesdropping.
- **Asymptotic Analysis and Diversity Order:** To offer a deeper understanding of system limits, we obtain asymptotic closed-form expressions for the SOP. This enables the explicit characterization of the secrecy diversity order of the considered backscatter system in the high Signal-to-Noise Ratio (SNR) regime.
- **Validation and Design Insights:** Our theoretical derivations are rigorously validated through extensive Monte Carlo simulations. The numerical results provide valuable insights into the crucial impacts of fading severity, correlation, and system parameters, offering practical guidelines for the design and deployment of secure satellite-assisted backscatter communications.

Table 1. Comparison of the uniqueness of our research to related articles.

Context	PLS	BD	Satellite	Nakagami-m	SOP	ESC	SER
Paper [36]	✓	✓			✓		
Paper [40]		✓		✓			✓
Paper [43]	✓	✓		✓	✓	✓	
Paper [44]	✓	✓			✓	✓	
Paper [45]	✓	✓					
Paper [46]	✓		✓	✓	✓	✓	
Paper [47]	✓	✓			✓		
Paper [48]	✓	✓		✓	✓	✓	
Paper [49]	✓	✓					
Paper [50]	✓	✓			✓		
This paper	✓	✓	✓	✓	✓	✓	✓

The remainder of the paper is organized as follows. Section 2 gives an overview of the system model. Section 3 presents the information-theoretic mathematical framework, to achieve the performance of the system. Section 4 presents numerical results and discussions to validate the developed framework as well as deeply explore the impacts of system key parameters, while Section 5 provides concluding remarks.

"Secure Performance Analysis of Satellite-terrestrial Networks-assisted Backscatter Device", H.-N. Nguyen, S.-P. Le, Q.-S. Vu, Q.-S. Nguyen and E. Chromy.

2. SYSTEM MODEL

In this correspondence, we examine a backscatter communication setup consisting of a satellite (S), a single backscatter device (B), and a potential eavesdropper (E) capable of intercepting the data transmitted by B, as illustrated in Fig. 1. The channels are defined as follows: from the transmitting antenna at S to B (denoted by h), from B to the receiving antenna at S (denoted by f), and from B to the eavesdropper (denoted by g), respectively. This setup highlights the intricate dynamics involved in the communication process within such a backscatter system. Understanding these channel gains is crucial for analyzing the overall performance and security implications of the system in practical scenarios. The received signal at the satellite from the backscatter device can be expressed as:

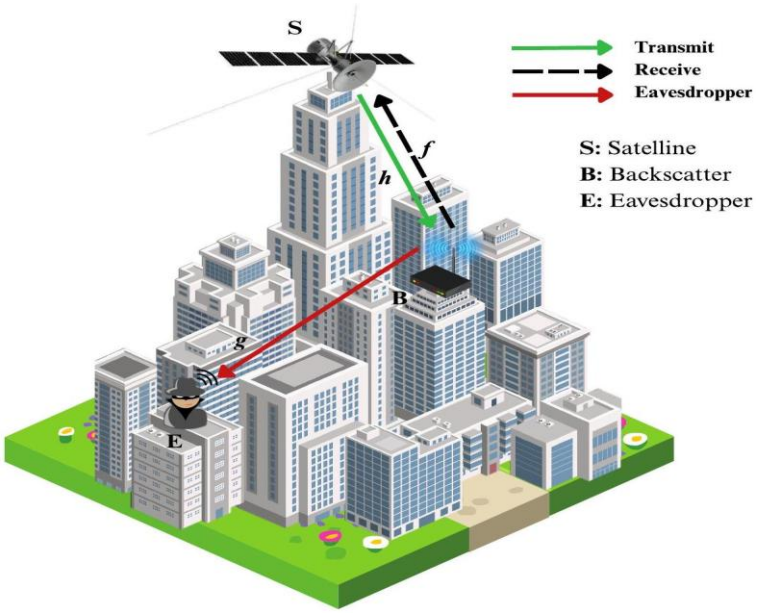

Figure 1. System model.

$$y_{BS} = \sqrt{P_S} hfsb + n_{BS}, \tag{1}$$

where P_S is the normalized transmission powers at the satellite, s is the query signal sent by the satellite, b is the information signal from the backscatter and n_{BS} is the additive white Gaussian noise (AWGN), $n_{BS} \sim \mathcal{CN}(0, \sigma_{BS}^2)$, we set $\mathbb{E}\{|s|^2\} = \mathbb{E}\{|b|^2\} = 1$.

The joint probability density function (PDF) of $|h|^2$ and $|f|^2$ are:

$$\begin{aligned} f_{|h|^2}(x) &= \alpha_1 e^{-\beta_1 x}\, {}_1F_1(m_1; 1; \delta_1 x) \quad , x \geq 0 \\ f_{|f|^2}(x) &= \alpha_2 e^{-\beta_2 x}\, {}_1F_1(m_2; 1; \delta_2 x) \quad , x \geq 0. \end{aligned} \tag{2}$$

For $i \in \{1,2\}$ we set $\alpha_i = \left(2b_i m_i/(2b_i m_i + \Omega_i)\right)^{m_i}/2b_i, \beta_i = 1/2b_i, \delta_i = \Omega_i/(2b_i)(2b_i m_i + \Omega_i)$ with Ω_i and $2b_i$ are the respective average power of the line-of-sight (LoS) and multi-path components, m_i is the fading-severity parameter and ${}_1F_1(\cdot;\cdot;\cdot)$ is the confluent hyper-geometric function of first kind, thereby expressing the probability-density function (PDF) of $f_{|h|^2}(x)$ and $f_{|f|^2}(x)$.

Table 2. Notations of main parameters.

Symbol	Notation	Symbol	Notation
s	Signal at Satelline	Ω_i	The respective average power of the LoS
b	Signal at Backscatter	$2b_i$	The multi-path components
m_i	The fading-severity parameter	$f_X(\cdot)$	Probability-density function (PDF) of X
P_S	Transmit power at S	$F_X(\cdot)$	Cumulative-distribution function (CDF) of X

P_E	Transmit power at E	$\mathbb{E}\{\cdot\}$	Expectation operator
h	Channel gain from U to S	$\lvert\cdot\rvert$	The absolute value of a complex number
f	Channel gain from U to B	$\Gamma(\cdot)$	Gamma function
g	Channel gain from B to S	$\gamma(\cdot,\cdot)$	Lower incomplete Gamma function
ρ_S	The average receive SNR at S	$K_v(\cdot)$	Bessel function of the second kind with v^{th} order
ρ_E	The average receive SNR at E	${}_1F_1(\cdot;\cdot\cdot)$	The confluent hyper-geometric function of first kind
n_{BS}	The additive white Gaussian noise (AWGN)	$W_{\lambda,\mu}(z)$	The Whittaker function
$(.)_{\kappa_i}$	The Pochhammer symbol		

$$f_{|h|^2}(x) = \alpha_1 \sum_{\kappa_1=0}^{m_1-1} \zeta(\kappa_1) x^{\kappa_1} e^{-(\beta_1-\delta_1)x} \quad , x \geq 0 \tag{3a}$$

$$f_{|f|^2}(x) = \alpha_2 \sum_{\kappa_2=0}^{m_2-1} \zeta(\kappa_2) x^{\kappa_2} e^{-(\beta_2-\delta_2)x} \quad , x \geq 0 \tag{3b}$$

where $\zeta(\kappa_i) = (-1)^{\kappa_i}(1-m_i)_{\kappa_i}\delta^{\kappa_i}/(\kappa_i)^2, i \in \{1,2\}$, with $(.)_{\kappa_i}$ is the Pochhammer symbol. The cumulative-distribution function (CDF) of $F_{|h|^2}(x)$ and $F_{|f|^2}(x)$ as:

$$F_{|h|^2}(x) = 1 - \alpha_1 \sum_{\kappa_1=0}^{m_1-1} \sum_{p_1=0}^{\kappa_1} \frac{\zeta(\kappa_1)\Gamma(\kappa_1+1)}{\Gamma(p_1+1)(\beta_1-\delta_1)^{\kappa_1+1-p_1}} \times x^{p_1} e^{-(\beta_1-\delta_1)x} \tag{4a}$$

$$F_{|f|^2}(x) = 1 - \alpha_2 \sum_{\kappa_2=0}^{m_2-1} \sum_{p_2=0}^{\kappa_2} \frac{\zeta(\kappa_2)\Gamma(\kappa_2+1)}{\Gamma(p_2+1)(\beta_2-\delta_2)^{\kappa_2+1-p_2}} \times x^{p_2} e^{-(\beta_2-\delta_2)x} \tag{4b}$$

where $\Gamma(x) = (x-1)!$ is the Gamma function for a positive integral x.

On the other hand, at the E side, the intercepted signal from the backscatter can be written as:

$$y_E = \sqrt{P_E} hgsb + n_E, \tag{5}$$

where P_E is the transmit power of the E, n_E is the AWGN at E, $n_E \sim \mathcal{CN}(0, \sigma_E^2)$, and we assume that h and g are independent from each other, since the E is far from reader, compared to the distance with the B.

Since we consider Nakagami-m faded channels for the terrestrial links of the considered network, the channel gains $|g|^2$, are assumed to follow the Gamma distribution with average power Ω_3 and fading severity m_3. Hence, The PDF and CDF of $f_{|g|^2}(x)$ can be given as:

$$f_{|g|^2}(x) = \frac{\mu^{m_3}}{\Gamma(m_3)} x^{m_3-1} e^{-\mu x}, \tag{6}$$

and

$$F_{|g|^2}(x) = 1 - \frac{\Gamma(m_3, \mu x)}{\Gamma(m_3)} = 1 - e^{-\mu x} \sum_{p_3=0}^{m_3-1} \frac{\mu^{p_3} x^{p_3}}{\Gamma(p_3+1)}, \tag{7}$$

where $\mu = \frac{m_3}{\Omega_3}$.

From (1) and (5), we can derive the received instantaneous signal-to-noise ratios (SNRs) at the reader and E as:

$$\gamma_{BS} = |h|^2 |f|^2 \rho_S, \tag{8}$$

and

"Secure Performance Analysis of Satellite-terrestrial Networks-assisted Backscatter Device", H.-N. Nguyen, S.-P. Le, Q.-S. Vu, Q.-S. Nguyen and E. Chromy.

$$\gamma_E = |h|^2|g|^2\rho_E, \tag{9}$$

where $\rho_S = P_S/\sigma_{sb}^2$ and $\rho_E = P_E/\sigma_E^2$ are the average receive SNR at reader and E, respectively.

Correspondingly, from (8) and (9), the capacity of the reader and eavesdropper's channels can be written as:

$$C_{BS} = \log_2(1+\gamma_{BS}), \tag{10}$$

and

$$C_E = \log_2(1+\gamma_E), \tag{11}$$

respectively. Using (10) and (11), we can express the instantaneous secrecy capacity of RFID (Radio frequency identification) backscatter system as:

$$C_S = [C_{BS} - C_E]^+, \tag{12}$$

where $[x]^+$is defined as $[x]^+ = \max(x, 0)$.

3. PERFORMANCE ANALYSIS

3.1 Security Outage Probability (SOP)

If we denote $R \geq 0$ as the target secrecy rate of S, the secrecy-outage probability of S can be expressed as:

$$\begin{aligned} P_{\text{out}} &= \Pr[C_S < R] = \Pr\left[\log_2\left(\frac{1+\gamma_{BS}}{1+\gamma_E}\right) < R\right] = \Pr\left[\frac{1+|h|^2|f|^2\rho_S}{1+|h|^2|g|^2\rho_E} < \gamma_{\text{th}}\right] \\ &= \Pr\left[|f|^2 < \frac{v}{|h|^2} + |g|^2\omega_E\right], \end{aligned} \tag{13}$$

where $\gamma_{th} = 2^R$ is the secrecy SNR threshold, $v = (\gamma_{th}-1)/\rho_S$ and $\omega_E = \frac{\gamma_{th}\rho_E}{\rho_S}$. Applying formulae (3a), (4b) and (6), P_{out} is calculated as:

$$P_{\text{out}} = \Pr[|f|^2 < \frac{v}{|h|^2} + |g|^2\omega_E] = \int_0^\infty f_{|h|^2}(x)\int_0^\infty f_{|g|^2}(y)\left[F_{|f|^2}\left(\frac{v}{x} + y\omega_E\right)\right]dxdy$$

$$\begin{aligned} &= \sum_{\kappa_1=0}^{m_1-1}\frac{\mu^{m_3}\alpha_1\zeta(\kappa_1)}{\Gamma(m_3)}\Big[\underbrace{\int_0^\infty x^{\kappa_1}e^{-(\beta_1-\delta_1)x}dx}_{\Phi_1} \times \int_0^\infty y^{m_3-1}e^{-\mu y}dy - \alpha_2\sum_{\kappa_2=0}^{m_2-1}\sum_{p_2=0}^{\kappa_2}\sum_{t=0}^{p_2}\binom{p_2}{t} \\ &\times\frac{\omega_E^{p_2-t}v^t\zeta(\kappa_2)\Gamma(\kappa_2+1)}{\Gamma(p_2+1)(\beta_2-\delta_2)^{\kappa_2-p_2+1}} \times \underbrace{\int_0^\infty x^{\kappa_1-t}\,e^{-\frac{(\beta_2-\delta_2)v}{x}-(\beta_1-\delta_1)x}dx}_{\Phi_3} \\ &\times \underbrace{\int_0^\infty y^{m_3+p_2-t-1}e^{-y(\mu+(\beta_2-\delta_2)\omega_E)}dy}_{\Phi_2}\Big] \end{aligned} \tag{14}$$

With the help of [27, Eq. (3.351.3)], Φ_1 and Φ_2 are given by:

$$\Phi_1 = \int_0^\infty x^{\kappa_1}e^{-(\beta_1-\delta_1)x}dx \times \int_0^\infty y^{m_3-1}e^{-\mu y}dy = (\kappa_1)!\,(\beta_1-\delta_1)^{-\kappa_1-1}(m_3-1)!\,\mu^{-m_3}$$

$$\Phi_2 = \int_0^\infty y^{m_3+p_2-t-1}e^{-y(\mu+(\beta_2-\delta_2)\omega_E)}dy = (m_3+p_2-t-1)!\,(\mu+(\beta_2-\delta_2)\omega_E)^{-m_3-p_2+t} \tag{15}$$

With the help of [27, Eq. (3.471.9)], Φ_3 is given by:

$$\Phi_3 = \int_0^\infty x^{\kappa_1-t}e^{-\frac{(\beta_2-\delta_2)v}{x}-(\beta_1-\delta_1)x}dx = 2\left(\frac{(\beta_2-\delta_2)v}{(\beta_1-\delta_1)}\right)^{\frac{\kappa_1-t+1}{2}}K_{\kappa_1-t+1}\left(2\sqrt{(\beta_1-\delta_1)(\beta_2-\delta_2)v}\right) \tag{16}$$

By substituting (15) and (16) into (14), we obtain:

$$\begin{aligned} P_{\text{out}} &= \sum_{\kappa_1=0}^{m_1-1} \frac{\mu^{m_3}\alpha_1\zeta(\kappa_1)}{\Gamma(m_3)}(\kappa_1)!\,(\beta_1-\delta_1)^{-\kappa_1-1}(m_3-1)!\,\mu^{-m_3} \\ &-\alpha_2\sum_{\kappa_2=0}^{m_2-1}\sum_{p_2=0}^{\kappa_2}\sum_{t=0}^{p_2}\binom{p_2}{t}\frac{2\omega_E^{p_2-t}v^t\zeta(\kappa_2)\Gamma(\kappa_2+1)}{\Gamma(p_2+1)(\beta_2-\delta_2)^{\kappa_2-p_2+1}}\left(\frac{(\beta_2-\delta_2)v}{(\beta_1-\delta_1)}\right)^{\frac{\kappa_1-t+1}{2}} \\ &\times K_{\kappa_1-t+1}\left(2\sqrt{(\beta_1-\delta_1)(\beta_2-\delta_2)v}\right)(m_3+p_2-t-1)!\,(\mu+(\beta_2-\delta_2)\omega_E)^{-m_3-p_2+t} \end{aligned} \tag{17}$$

where $K_v(.)$ is the first order modified Bessel function of the second kind.

3.2 Ergodic Secrecy Capacity (ESC) Analysis

In this section, we analyze the system's ESC performance, which is defined as the average of the highest attainable secrecy capacity. To evaluate the ESC, we define the ergodic capacity of the main channel and the wiretap channel as follows.

$$\mathbb{E}\{C_S\} = [\mathbb{E}\{C_{BS}\} - \mathbb{E}\{C_E\}]^+. \tag{18}$$

To obtain the desired outcome, the formulae for the ergodic capacity of the primary and wiretap channels must be considered. (i.e., C_{BS} and C_E). As a result, we simplify C_{BS} using SNR from (8) into (10) and C_E using SNR from (9) into (11) as:

$$\begin{aligned} \mathbb{E}\{C_{BS}\} &= \mathbb{E}\{\log_2(1+\underbrace{\frac{|h|^2|f|^2}{\rho_S}}_{X})\} = \frac{1}{\ln 2}\int_0^\infty \frac{1-F_X(x)}{1+x}dx \\ \mathbb{E}\{C_E\} &= \mathbb{E}\{\log_2(1+\underbrace{\frac{|h|^2|g|^2}{\rho_E}}_{Y})\} = \frac{1}{\ln 2}\int_0^\infty \frac{1-F_Y(y)}{1+y}dy\,. \end{aligned} \tag{19}$$

where $F_X(x)$ with $X = |h|^2|f|^2\rho_S$ and $F_Y(y)$ with $Y = |h|^2|g|^2\rho_E$. Based on (3) and (4), $F_X(x)$ is calculated as:

$$\begin{aligned} F_X(x) &= F_{|h|^2|f|^2\rho_S}(x) = \Pr(|h|^2 < \frac{x}{|f|^2\rho_S}) = \int_0^{+\infty} F_{|h|^2}(\frac{x}{y\rho_S})f_{|f|^2}(y)dy \\ &= \int_0^{+\infty}(1-\alpha_1\sum_{\kappa_1=0}^{m_1-1}\sum_{p_1=0}^{\kappa_1}\frac{\zeta(\kappa_1)\Gamma(\kappa_1+1)}{\Gamma(p_1+1)(\beta_1-\delta_1)^{\kappa_1+1-p_1}}\times(\frac{x}{y\rho_S})^{p_1}e^{-\frac{(\beta_1-\delta_1)x}{y\rho_S}})\times f_{|f|^2}(y)dy \\ &= \int_0^{+\infty} f_{|f|^2}(y)dy - \int_0^{+\infty}\alpha_1\sum_{\kappa_1=0}^{m_1-1}\sum_{p_1=0}^{\kappa_1}\frac{\zeta(\kappa_1)\Gamma(\kappa_1+1)}{\Gamma(p_1+1)(\beta_1-\delta_1)^{\kappa_1+1-p_1}}\times(\frac{x}{y\rho_S})^{p_1}e^{-\frac{(\beta_1-\delta_1)x}{y\rho_S}}\times f_{|f|^2}(y)dy \\ &= 1-\alpha_1\alpha_2\sum_{\kappa_2=0}^{m_2-1}\sum_{\kappa_1=0}^{m_1-1}\sum_{p_1=0}^{\kappa_1}\frac{\zeta(\kappa_1)\zeta(\kappa_2)\Gamma(\kappa_1+1)(\frac{x}{\rho_S})^{p_1}}{\Gamma(p_1+1)(\beta_1-\delta_1)^{\kappa_1+1-p_1}}\underbrace{\int_0^{+\infty} y^{\kappa_2-p_1}e^{-\frac{(\beta_1-\delta_1)x}{y\rho_S}-(\beta_2-\delta_2)y}dy}_{\Xi_1} \end{aligned} \tag{20}$$

By using [27, Eq. (3.471.9)] for Ξ_1, the CDF$F_X(x)$ can be obtained:

$$\begin{aligned} F_X(x) &= 1-2\sum_{\kappa_2=0}^{m_2-1}\sum_{\kappa_1=0}^{m_1-1}\sum_{p_1=0}^{\kappa_1}\frac{\alpha_1\alpha_2\zeta(\kappa_1)\zeta(\kappa_2)}{\rho_S^{(\frac{\kappa_2+p_1+1}{2})}\Gamma(p_1+1)(\beta_2-\delta_2)^{\frac{\kappa_2-p_1+1}{2}}} \\ &\times\frac{\Gamma(\kappa_1+1)(\sqrt{x})^{\kappa_2+p_1+1}}{(\beta_1-\delta_1)^{\frac{2\kappa_1-p_1-\kappa_2+1}{2}}}K_{\kappa_2-p_1+1}\left(2\sqrt{\frac{(\beta_1-\delta_1)(\beta_2-\delta_2)x}{\rho_S}}\right) \end{aligned} \tag{21}$$

Substituting (21) into (19), we obtain:

$$\begin{aligned} \mathbb{E}\{C_{BS}\} &= 2\sum_{\kappa_2=0}^{m_2-1}\sum_{\kappa_1=0}^{m_1-1}\sum_{p_1=0}^{\kappa_1}\frac{\alpha_1\alpha_2\zeta(\kappa_1)\zeta(\kappa_2)\Gamma(\kappa_1+1)}{\ln 2\,\rho_S^{(\kappa_2+p_1+1)/2}\Gamma(p_1+1)} \\ &\times\frac{(\beta_1-\delta_1)^{(\kappa_2+p_1-2\kappa_1-1)/2}}{(\beta_2-\delta_2)^{(\kappa_2-p_1+1)/2}}\int_0^\infty\frac{(\sqrt{x})^{\kappa_2+p_1+1}}{1+x}\times K_{\kappa_2-p_1+1}\left(2\sqrt{\frac{(\beta_1-\delta_1)(\beta_2-\delta_2)x}{\rho_S}}\right)dx \end{aligned} \tag{22}$$

Let $t = 4/\pi\arctan(x) - 1 \Rightarrow \tan(\pi(t+1)/4) = x \Rightarrow (\pi/4)\sec^2(\pi(t+1)/4)dt = dx$, so $\mathbb{E}\{C_{BS}\}$ is given by:

$$\begin{aligned}\mathbb{E}\{C_{BS}\} &= \sum_{\kappa_2=0}^{m_2-1} \sum_{\kappa_1=0}^{m_1-1} \sum_{p_1=0}^{\kappa_1} \frac{\pi\alpha_1\alpha_2\zeta(\kappa_1)\zeta(\kappa_2)}{2\ln 2\rho_S^{(\kappa_2+p_1+1)/2}\Gamma(p_1+1)} \\ &\times \frac{(\beta_1-\delta_1)^{(\kappa_2+p_1-2\kappa_1-1)/2}}{(\beta_2-\delta_2)^{(\kappa_2-p_1+1)/2}} \int_{-1}^{1} \sec^2(\pi(t+1)/4) \\ &\times \frac{\Gamma(\kappa_1+1)(\sqrt{\tan(\pi(t+1)/4)})^{\kappa_2+p_1+1}}{[1+\tan(\pi(t+1)/4)]} \\ &\times K_{\kappa_2-p_1+1}\left(2\sqrt{\frac{\tan(\pi(t+1)/4)}{(\beta_1-\delta_1)^{-1}(\beta_2-\delta_2)^{-1}\rho_S}}\right)dt\end{aligned} \tag{23}$$

Though it is difficult to derive a closed-form expression for (23), we can obtain an accurate approximation for it. Using Gaussian-Chebyshev quadrature [27, Eq. 25.4.38], we have:

$$\begin{aligned}\mathbb{E}\{C_{BS}\} &\approx \sum_{\kappa_2=0}^{m_2-1} \sum_{\kappa_1=0}^{m_1-1} \sum_{p_1=0}^{\kappa_1} \sum_{n=1}^{N} \frac{\pi^2\sqrt{1-\xi_n^2}\alpha_1\alpha_2\zeta(\kappa_1)\zeta(\kappa_2)}{2N\ln 2\rho_S^{(\kappa_2+p_1+1)/2}} \\ &\times \frac{\sec^2(\pi(\xi_n^2+1)/4)(\beta_1-\delta_1)^{(\kappa_2+p_1-2\kappa_1-1)/2}}{(\beta_2-\delta_2)^{(\kappa_2-p_1+1)/2}} \times \frac{\Gamma(\kappa_1+1)(\sqrt{\tan(\pi(\xi_n^2+1)/4)})^{\kappa_2+p_1+1}}{\Gamma(p_1+1)[1+\tan(\pi(\xi_n^2+1)/4)]} \\ &\times K_{\kappa_2-p_1+1}\left(2\sqrt{\frac{\tan(\pi(\xi_n^2+1)/4)}{(\beta_1-\delta_1)^{-1}(\beta_2-\delta_2)^{-1}\rho_S}}\right)\end{aligned} \tag{24}$$

where $\xi_n = \cos\left(\frac{2m-1}{2M}\pi\right)$ and $\sec^2(x) = 1/\cos^2(x)$.

Next, $\mathbb{E}\{C_E\}$ is calculated as:

$$\mathbb{E}\{C_E\} = \frac{1}{\ln 2}\int_0^{\infty} \frac{1-F_Y(x)}{1+x}dx \tag{25}$$

Based on (4) and (6), $F_Y(y)$ is calculated as:

$$\begin{aligned}F_Y(y) &= F_{|h|^2|g|^2\rho_S}(y) = \Pr(|h|^2 < \tfrac{y}{|g|^2\rho_S}) = \int_0^{+\infty} F_{|h|^2}(\tfrac{x}{z\rho_S}) f_{|g|^2}(z)dz \\ &= \int_0^{+\infty} (1-\alpha_1 \sum_{\kappa_1=0}^{m_1-1} \sum_{p_1=0}^{\kappa_1} \frac{\zeta(\kappa_1)\Gamma(\kappa_1+1)}{\Gamma(p_1+1)(\beta_1-\delta_1)^{\kappa_1+1-p_1}} \times (\tfrac{y}{z\rho_E})^{p_1} e^{-\frac{(\beta_1-\delta_1)y}{z\rho_E}}) \times f_{|g|^2}(z)dz \\ &= \int_0^{+\infty} f_{|g|^2}(z)dz - \int_0^{+\infty} \alpha_1 \sum_{\kappa_1=0}^{m_1-1} \sum_{p_1=0}^{\kappa_1} \frac{\zeta(\kappa_1)\Gamma(\kappa_1+1)}{\Gamma(p_1+1)(\beta_1-\delta_1)^{\kappa_1+1-p_1}} \times (\tfrac{y}{z\rho_E})^{p_1} e^{-\frac{(\beta_1-\delta_1)y}{z\rho_E}} \times f_{|g|^2}(z)dz \\ &= 1-\alpha_1 \sum_{\kappa_1=0}^{m_1-1} \sum_{p_1=0}^{\kappa_1} \frac{\mu^{m_3}\zeta(\kappa_1)\Gamma(\kappa_1+1)}{\Gamma(m_3)\Gamma(p_1+1)(\beta_1-\delta_1)^{\kappa_1+1-p_1}} (\tfrac{y}{\rho_E})^{p_1} \underbrace{\int_0^{+\infty} z^{m_3-p_1-1} e^{-\frac{(\beta_1-\delta_1)y}{z\rho_E}-\mu z}dz}_{\Xi_1}\end{aligned} \tag{26}$$

By using [27, Eq. (3.471.9)] for Ξ_2, the CDF$F_Y(y)$ can be obtained:

$$F_Y(y) = 1 - \sum_{\kappa_1=0}^{m_1-1} \sum_{p_1=0}^{\kappa_1} \frac{2\alpha_1\mu^{\frac{m_3+p_1}{2}}\zeta(\kappa_1)\Gamma(\kappa_1+1)y^{\frac{m_3+p_1}{2}}}{\Gamma(m_3)\Gamma(p_1+1)(\beta_1-\delta_1)^{\frac{2\kappa_1-p_1-m_3+2}{2}}\rho_E^{\frac{m_3+p_1}{2}}} K_{m_3-p_1}\left(2\sqrt{\frac{\mu(\beta_1-\delta_1)y}{\rho_E}}\right) \tag{27}$$

Substituting (27) into (25), we can obtain:

$$\mathbb{E}\{C_E\} = \frac{\sum_{\kappa_1=0}^{m_1-1}\sum_{p_1=0}^{\kappa_1} \frac{2\alpha_1\mu^{\frac{m_3+p_1}{2}}\zeta(\kappa_1)\Gamma(\kappa_1+1)}{\Gamma(m_3)\Gamma(p_1+1)(\beta_1-\delta_1)^{\frac{2\kappa_1-p_1-m_3+2}{2}}\rho_E^{\frac{m_3+p_1}{2}}}}{\ln 2} \int_0^{\infty} \frac{x^{\frac{m_3+p_1}{2}}}{1+x} K_{m_3-p_1}\left(2\sqrt{\frac{\mu(\beta_1-\delta_1)x}{\rho_E}}\right)dx. \tag{28}$$

Let $u = 4/\pi\arctan(x) - 1 \Rightarrow \tan(\pi(u+1)/4) = x \Rightarrow (\pi/4)\sec^2(\pi(u+1)/4)du = dx$, so $\mathbb{E}\{C_E\}$ is given by:

$$\begin{aligned}\mathbb{E}\{C_E\} &= \frac{(\frac{\pi}{4})\sum_{\kappa_1=0}^{m_1-1} \sum_{p_1=0}^{\kappa_1} \frac{2\alpha_1\mu^{\frac{m_3+p_1}{2}}\zeta(\kappa_1)\Gamma(\kappa_1+1)}{\Gamma(m_3)\Gamma(p_1+1)(\beta_1-\delta_1)^{\frac{2\kappa_1-p_1-m_3+2}{2}}\rho_E^{\frac{m_3+p_1}{2}}}}{\ln 2} \\ &\times \int_{-1}^{+1} \frac{\tan(\frac{\pi(u+1)}{4})^{\frac{m_3+p_1}{2}}}{1+\tan(\frac{\pi(u+1)}{4})} K_{m_3-p_1}\left(2\sqrt{\frac{\mu(\beta_1-\delta_1)\tan(\frac{\pi(u+1)}{4})}{\rho_E}}\right)\sec^2(\tfrac{\pi(u+1)}{4})du\end{aligned} \tag{29}$$

Although it is difficult to derive a closed-form expression for (29), an accurate approximation can be obtained by using the Gaussian-Chebyshev quadrature [27, Eq. (25.4.38)]. Accordingly, we have:

$$\mathbb{E}\{C_E\} \approx \sum_{m=1}^{M} \sum_{\kappa_1=0}^{m_1-1} \sum_{p_1=0}^{\kappa_1} \frac{\sec^2((\xi_m+1)\frac{\pi}{4})\pi^2\sqrt{1-\xi_m^2}\alpha_1\mu^{\frac{m_3+p_1}{2}}\zeta(\kappa_1)}{2M\ln 2\Gamma(m_3)\Gamma(p_1+1)(\beta_1-\delta_1)^{\frac{2\kappa_1-p_1-m_3+2}{2}}\rho_E^{\frac{m_3+p_1}{2}}} \frac{\Gamma(\kappa_1+1)\tan((\xi_m+1)\frac{\pi}{4})^{\frac{m_3+p_1}{2}}}{1+\tan((\xi_m+1)\frac{\pi}{4})} K_{m_3-p_1}\left(2\sqrt{\frac{\mu(\beta_1-\delta_1)\tan((\xi_m+1)\frac{\pi}{4})}{\rho_E}}\right) \tag{30}$$

where $\xi_m = \cos\left(\frac{2m-1}{2M}\pi\right)$.

By combining (30) and (24) into (18), the approximate expression for the ergodic achievable secrecy rate of the satellite can be expressed as:

$$\begin{aligned}\mathbb{E}\{C_S\} \approx [\sum_{\kappa_2=0}^{m_2-1}\sum_{\kappa_1=0}^{m_1-1}\sum_{p_1=0}^{\kappa_1}\sum_{n=1}^{N}\sum_{m=1}^{M} & \frac{\overline{\pi^2\sqrt{1}-\xi_n^2\alpha_1\alpha_2\zeta(\kappa_1)\zeta(\kappa_2)\sec^2\left(\frac{\pi(\xi_n^2+1)}{4}\right)(\beta_1-\delta_1)^{\frac{\kappa_2+p_1-2\kappa_1-1}{2}}}}{4N\ln 2\Gamma(p_1+1)\rho_S^{\frac{\kappa_2+p_1+1}{2}}(\beta_2-\delta_2)^{\frac{\kappa_2-p_1+1}{2}}} \\ & \times\frac{\Gamma(\kappa_1+1)\pi^2\sqrt{1-\xi_m^2}\alpha_1\zeta(\kappa_1)\Gamma(\kappa_1+1)}{[1+\tan(\pi(\xi_n^2+1)\pi(\xi_n^2+1)4)]\,\mathrm{Mln}\,2\Gamma(m_3)\,\Gamma(p_1+1)\rho_E^{(p_1+m_3)(p_1+m_3)}} \\ \times\frac{\sec^2\left(\frac{\pi(\xi_m+1)}{4}\right)(\beta_1-\delta_1)^{\frac{p_1+m_3-2\kappa_1-2}{2}}\mu^{\frac{m_3+p_1}{2}}\left(\sqrt{\tan(\pi(\xi_m+1))}\right)^{p_1+m_3}}{(\sqrt{\tan(\pi(\xi_n^2+1)\pi(\xi_n^2+1)4)})^{-\kappa_2-p_1-1}} & [1+\tan(\pi(\xi_m+1)\pi(\xi_m+1)4)] \\ \times K_{\kappa_2-p_1+1}\left(2\sqrt{\frac{\tan\left(\frac{\pi(\xi_n^2+1)}{4}\right)}{(\beta_1-\delta_1)^{-1}(\beta_2-\delta_2)^{-1}\rho_S}}\right)K_{m_3-p_1}\left(2\sqrt{\frac{(\beta_1-\delta_1)\mu\tan\left(\frac{\pi(\xi_m+1)}{4}\right)}{\rho_E}}\right)]. & \end{aligned} \tag{31}$$

3.3 Symbol Error Rate (SER)

For the wireless system, the SER is calculated as:

$$SER = \bar{a}\mathbb{E}\{Q(\sqrt{\bar{b}\gamma})\} = \frac{\bar{a}}{\sqrt{2\pi}}\int_0^{\infty} F\left(\frac{t^2}{\bar{b}}\right)e^{-\frac{t^2}{2}}dt \tag{32}$$

where $\bar{a}$ and $\bar{b}$ are constants and depend on the modulation types, e.g. $\bar{a}=1, \bar{b}=2$ for the binary phase-shift keying (BPSK) modulation and $\bar{a}=2, \bar{b}=1$ for quadrature phase shift keying (QPSK) and 4-quadrature amplitude modulation (4-QAM); $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^{\infty} e^{-t^2/2}dt$ is the Gaussian function; γ is the end-to-end SINR of the considered system; $F(x)$ is the CDF of the end-to-end SINR. From the definition of CDF, we can replace $F(x)$ by P_{out} of the system.

From (32), applying the change of variable technique $x = t^2/b$, we can rewrite the SER as [28]:

$$\begin{aligned} SER &= \frac{\bar{a}\sqrt{\bar{b}}}{2\sqrt{2\pi}}\int_0^{\infty}\frac{e^{-bv/2}}{\sqrt{v}}[F_X(x)-F_Y(y)]dv \\ &= \frac{\bar{a}\sqrt{\bar{b}}}{2\sqrt{2\pi}}\left[\int_0^{\infty}\frac{e^{-\frac{bv}{2}}F_X(v)}{\sqrt{v}}dv - \int_0^{\infty}\frac{e^{-\frac{bv}{2}}F_Y(v)}{\sqrt{v}}dv\right]. \end{aligned} \tag{33}$$

By substituting (20) and (27) into (33), we obtain:

$$\begin{aligned} SER = \frac{\bar{a}\sqrt{\bar{b}}}{2\sqrt{2\pi}} \Bigg[& \sum_{\kappa_1=0}^{m_1-1}\sum_{p_1=0}^{\kappa_1}\frac{2\alpha_1\mu^{\frac{m_3+p_1}{2}}\zeta(\kappa_1)\Gamma(\kappa_1+1)}{\Gamma(m_3)\Gamma(p_1+1)(\beta_1-\delta_1)^{\frac{2\kappa_1-p_1-m_3+2}{2}}\rho_E^{\frac{m_3+p_1}{2}}} \\ & \times \underbrace{\int_0^{\infty} e^{\frac{-bv}{2}}v^{\frac{m_3+p_1-1}{2}}K_{m_3-p_1}\left(2\sqrt{\frac{\mu(\beta_1-\delta_1)v}{\rho_E}}\right)dv}_{\Xi_3} \\ & -2\sum_{\kappa_2=0}^{m_2-1}\sum_{\kappa_1=0}^{m_1-1}\sum_{\kappa_1=0}^{\kappa_1}\frac{\alpha_1\alpha_2\zeta(\kappa_1)\zeta(\kappa_2)\Gamma(\kappa_1+1)}{\rho_S^{\left(\frac{\kappa_2+p_1+1}{2}\right)}\Gamma(p_1+1)(\beta_2-\delta_2)^{\frac{\kappa_2-p_1+1}{2}}}(\beta_1-\delta_1)^{\frac{2\kappa_1-p_1-\kappa_2+1}{2}} \\ & \times \underbrace{\int_0^{\infty} e^{\frac{-bv}{2}}v^{\frac{\kappa_2+p_1}{2}}K_{\kappa_2-p_1+1}\left(2\sqrt{\frac{(\beta_1-\delta_1)(\beta_2-\delta_2)v}{\rho_S}}\right)dv}_{\Xi_4} \Bigg] \end{aligned} \tag{34}$$

"Secure Performance Analysis of Satellite-terrestrial Networks-assisted Backscatter Device", H.-N. Nguyen, S.-P. Le, Q.-S. Vu, Q.-S. Nguyen and E. Chromy.

With the help of [29, Eq. (6.643.3)], Ξ_3 and Ξ_4 are calculated as:

$$\begin{aligned}\Xi_3 &= \int_0^\infty v^{\frac{m_3+p_1-1}{2}} e^{\frac{-bv}{2}} K_{m_3-p_1}\left(2\sqrt{\frac{\mu(\beta_1-\delta_1)v}{\rho_E}}\right)dv \\ &= \frac{\Gamma(m_3+\frac{1}{2})\Gamma(p_1+\frac{1}{2})}{2\sqrt{\frac{\mu(\beta_1-\delta_1)}{\rho_E}}} e^{\left(\frac{\mu(\beta_1-\delta_1)}{b\rho_E}\right)} \left(\frac{b}{2}\right)^{\frac{-m_3-p_1}{2}} W_{\frac{-m_3-p_1}{2},\frac{m_3-p_1}{2}}\left(\frac{2\mu(\beta_1-\delta_1)}{b\rho_E}\right) \\ \Xi_4 &= \int_0^\infty v^{\frac{\kappa_2+p_1}{2}} e^{\frac{-bv}{2}} K_{\kappa_2-p_1+1}\left(2\sqrt{\frac{(\beta_1-\delta_1)(\beta_2-\delta_2)v}{\rho_S}}\right)dv \\ &= \frac{\Gamma\left(\kappa_2+\frac{3}{2}\right)\Gamma\left(p_1+\frac{1}{2}\right)}{2\sqrt{\frac{(\beta_1-\delta_1)(\beta_2-\delta_2)}{\rho_S}}} e^{\left(\frac{(\beta_1-\delta_1)(\beta_2-\delta_2)}{b\rho_S}\right)} \left(\frac{b}{2}\right)^{\frac{-\kappa_2-p_1-1}{2}} W_{\frac{-\kappa_2-p_1-1}{2},\frac{\kappa_2-p_1+1}{2}}\left(\frac{2(\beta_1-\delta_1)(\beta_2-\delta_2)}{b\rho_S}\right).\end{aligned} \tag{35}$$

By substituting Ξ_3 and Ξ_4 into (34), we have:

$$\begin{aligned}SER = \frac{\bar{a}\sqrt{\bar{b}}}{2\sqrt{2\pi}}\Big[\sum_{\kappa_1=0}^{m_1-1} \sum_{p_1=0}^{\kappa_1} &\frac{2^{(p_1+m_3)/2}\mu^{(m_3+p_1-1)/2}\alpha_1\zeta(\kappa_1)\Gamma(\kappa_1+1)\Gamma((2m_3+1)/2)\Gamma((2p_1+1)/2)}{\Gamma(m_3)\Gamma(p_1+1)\bar{b}^{(p_1+m_3)/2}\rho_E^{(p_1+m_3-1)/2}(\beta_1-\delta_1)^{(2\kappa_1-p_1-m_3+3)/2}} \\ \times e^{\frac{(\beta_1-\delta_1)\mu}{\bar{b}\rho_E}} W_{-\frac{p_1+m_3}{2},\frac{m_3-p_1}{2}}((2(\beta_1-\delta_1)\mu)/\bar{b}\rho_E) - \sum_{\kappa_2=0}^{m_2-1} \sum_{\kappa_1=0}^{m_1-1} \sum_{p_1=0}^{\kappa_1} &\frac{2^{(\kappa_2+p_1+1)/2}\alpha_1\alpha_2\zeta(\kappa_1)\zeta(\kappa_2)\Gamma(\kappa_1+1)}{\rho_S^{(\kappa_2+p_1)/2}\Gamma(p_1+1)(\beta_2-\delta_2)^{(\kappa_2-p_1+2)/2}} \\ \times \frac{\Gamma((2\kappa_2+3)/2)\Gamma((2p_1+1)/2)}{\bar{b}^{(\kappa_2+p_1+1)/2}(\beta_1-\delta_1)^{(2\kappa_1-p_1-\kappa_2+2)/2}} e^{\frac{(\beta_1-\delta_1)(\beta_2-\delta_2)}{\bar{b}\rho_S}} &W_{-\frac{\kappa_2+p_1+1}{2},\frac{\kappa_2-p_1+1}{2}}((2(\beta_1-\delta_1)(\beta_2-\delta_2))/2)\Big].\end{aligned} \tag{36}$$

4. NUMERICAL RESULTS AND SIMULATIONS

This section employs Monte Carlo simulations to validate the proposed mathematical frameworks and provide insights under various conditions. Simulation parameters are detailed in Table 3.

Table 3. Simulation parameters.

Symbol	Parameter name	Value
ρ_S	Transmit power to noise ratio at S	0 to 40 (dB)
ρ_E	Transmit power to noise ratio at E	0 to 20(dB)
R	Target rate	1.5 to 3bps/Hz
N	The Gauss-Chevbyshev parameter	100
M	The Gauss-Chevbyshev parameter	100
m_i	The fading-severity parameter	5
Ω_i	The respective average power of the LoS	0.279
b_i	The multi-path components	0.251

Figure 2 clearly illustrates the relationship between the Secrecy Outage Probability (SOP) and the average Satellite Signal-to-Noise Ratio (ρ_S in dB), while validating the analytical results against simulations and comparing performance with a reference scheme. The close proximity of the analysis (solid lines) and simulation (data points) results confirms the accuracy of the derived closed-form analytical expressions for SOP. As ρ_S increases, the SOP decreases significantly, a trend directly attributable to the satellite allocating higher transmit power, which in turn enhances the instantaneous received SNR and overall system security. Conversely, the SOP rises as the target Secrecy Rate Threshold (R) increases (from 1.5 to 3), reflecting the more stringent requirement for secure communication. Furthermore, the proposed system demonstrates superior performance by achieving a lower SOP compared to the "Backscatter Random Selection" scheme [5], highlighting the effectiveness of the current model in the correlated Nakagami-m fading environment.

Figure 3 investigates the effect of the average Eavesdropper Signal-to-Noise Ratio (ρ_E) on the Secrecy Outage Probability (SOP) as a function of ρ_S, with a fixed target secrecy rate of $R = 2$. Similar to Figure 2, the SOP continues to decrease as ρ_S increases, indicating that secure performance is enhanced with higher satellite transmit power. Furthermore, the analytical and simulation results (black curves) show an excellent match, reinforcing the reliability of the theoretical framework. Crucially, Figure 3 clearly demonstrates that the secrecy performance is degraded as ρ_E increases (from 5 dB to 15 dB), resulting

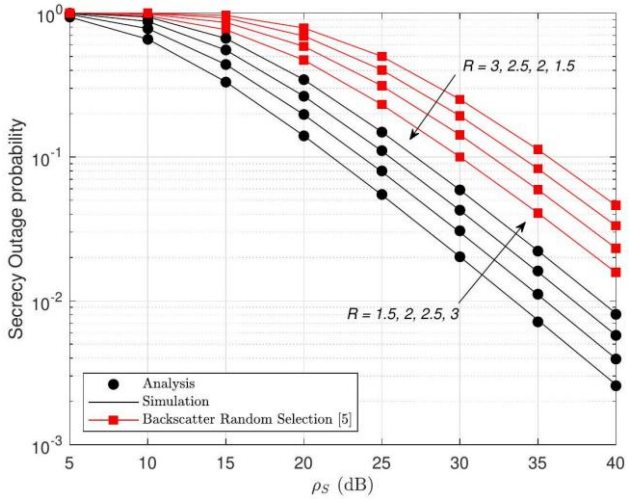

Figure 2. Secrecy-outage probability *versus* ρ_S.

in an increase in SOP and an upward shift of the curves. This occurs because a higher eavesdropper power increases the Eavesdropper's Channel Capacity (C_E), thus reducing the achievable Secrecy Capacity ($C_S = [C_{BS} - C_E]^+$). Notably, in the high ρ_S regime, the SOP curves for different ρ_E values tend to be parallel. This suggests that the secrecy-diversity order of the system is independent of the eavesdropper's power (ρ_E). Finally, the proposed system maintains a lower SOP compared to the reference "Backscatter Random Selection" scheme [5] across all considered ρ_E scenarios.

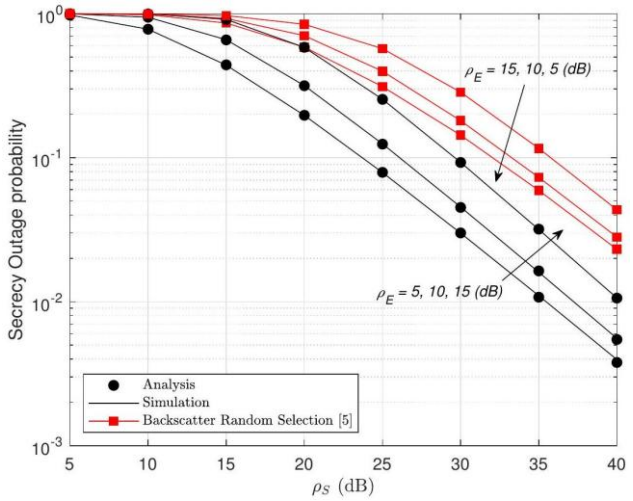

Figure 3. Secrecy-outage probability *versus* ρ_S for different values of ρ_E, with $R = 2$.

Figure 4 depicts the Ergodic Achievable Secrecy Rate (ESC) versus the average satellite SNR, ρ_S, for various eavesdropper SNR values, ρ_E, with the fading-severity parameter fixed at $m = 5$. In terms of the main channel, the ESC consistently increases with ρ_S. This behavior confirms that allocating more transmit power to the signal effectively enhances the system's ergodic-secrecy capacity. Conversely, the ESC is significantly degraded as the eavesdropper's SNR, ρ_E, increases from 0 dB to 20 dB . This degradation is expected, because a higher ρ_E provides the eavesdropper with better channel quality, increasing its capacity and reducing the net secrecy capacity, C_S. Furthermore, the curves illustrate a key secure communication property: for $\rho_E > 0$, the ESC is zero until ρ_S surpasses a minimum threshold. This required ρ_S threshold is directly proportional to ρ_E, meaning that the system must overcome the eavesdropper's channel quality to achieve a positive secrecy rate (e.g. the ESC only becomes positive around $\rho_S \approx 20$ dB when $\rho_E = 20$ dB).

Figure 5 presents the Symbol Error Rate (SER) as a function of the average satellite SNR (ρ_S), with the fading-severity parameter fixed at $m = 51$. The results indicate that the SER decreases sharply as ρ_S increases, which is consistent with theory, since higher transmit power raises the overall SNR and reduces the probability of error. The tight congruence between the Analytical and Simulation data points (for both BPSK and 4QAM) confirms the accuracy of the derived closed-form analytical SER

"Secure Performance Analysis of Satellite-terrestrial Networks-assisted Backscatter Device", H.-N. Nguyen, S.-P. Le, Q.-S. Vu, Q.-S. Nguyen and E. Chromy.

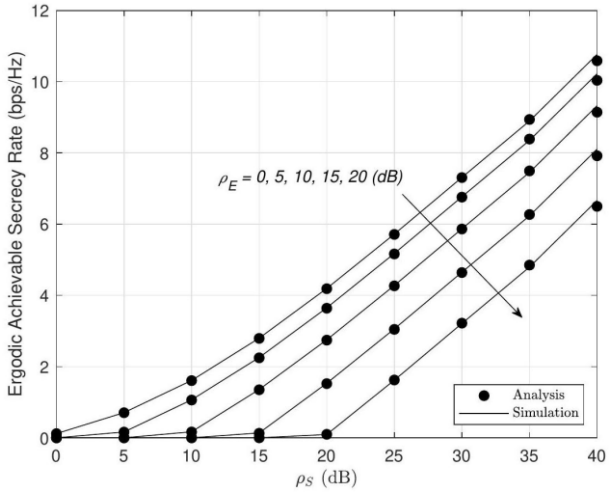

Figure 4. The ergodic-secrecy rate *versus* ρ_S, with $m = 5$.

expressions. Most significantly, the plot illustrates that BPSK achieves a lower SER (better performance) than 4QAM across the entire range of ρ_S examined. This difference stems from BPSK being a lower-order modulation scheme (1 bit/symbol) compared to 4QAM (2 bits/symbol), thus offering superior robustness against errors under the same SNR conditions. In summary, these findings provide practical guidance for selecting an appropriate modulation scheme to optimize the reliability of the backscatter link in the satellite-terrestrial system.

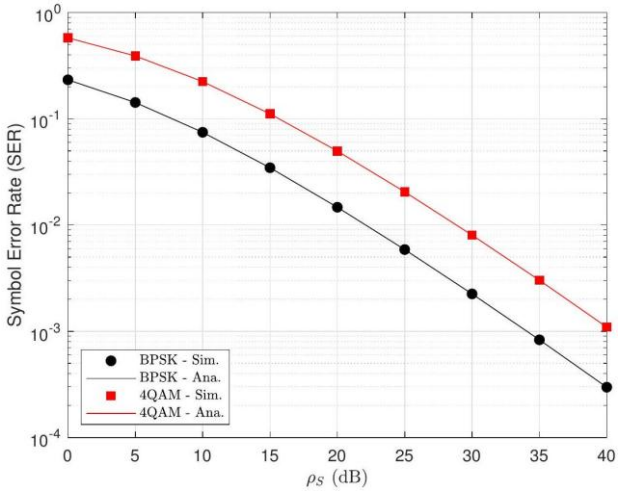

Figure 5. Symbol error rate *versus* ρ_S, with $m = 5$.

5. CONCLUSIONS

This paper has presented a comprehensive secrecy-performance analysis of a two-way satellite-terrestrial backscatter communication system in the presence of an eavesdropper. Closed-form analytical expressions for key secrecy metrics, including the SOP, ESC, and SER, were derived under correlated Nakagami-m fading channels, providing quantitative insights into the system's vulnerability to eavesdropping. The analytical findings were further verified through extensive Monte Carlo simulations, confirming their accuracy across various channel and system configurations. The results revealed that both the satellite transmit power and channel correlation play critical roles in determining the system's secrecy performance. Specifically, increasing the satellite transmit power (ρ_S) dramatically reduces the SOP and enhances the ESC, while a higher eavesdropper power (ρ_E) markedly deteriorates both metrics, thereby defining a minimum ρ_S threshold necessary to achieve a positive secrecy capacity. Furthermore, regarding symbol reliability, BPSK modulation consistently achieved a lower SER than 4QAM, confirming its superior robustness for backscatter links under the examined fading conditions. Although asymptotic analysis was not explicitly included to maintain clarity and conciseness, the derived closed-form expressions and simulation results already capture the key secrecy trends across the entire SNR

range. Future work could extend this study to more complex multi-tag or multi-eavesdropper scenarios, explore AI-driven physical layer security schemes, and perform energy efficiency optimization under practical hardware constraints. Moreover, incorporating cooperative relaying and artificial-noise generation represents a promising direction for further enhancing secrecy performance in next-generation satellite-IoT backscatter systems.

REFERENCES

[1] J. Qian, F. Gao, G. Wang, S. Jin and H. Zhu, "Noncoherent Detections for Ambient Backscatter System," IEEE Trans. on Wireless Communications, vol. 16, no. 3, pp. 1412-1422, March 2017.

[2] C. Zhong et al., "Wireless Information and Power Transfer with Full Duplex Relaying," IEEE Trans. on Communications, vol. 62, no. 10, pp. 3447-3461, Oct. 2014.

[3] G. Wang, F. Gao, R. Fan and C. Tellambura, "Ambient Backscatter Communication Systems: Detection and Performance Analysis," IEEE Trans. on Communications, vol. 64, no. 11, pp. 4836-4846, Nov. 2016.

[4] J. D. Griffin and G. D. Durgin, "Gains for RF Tags Using Multiple Antennas," IEEE Transactions on Antennas and Propagation, vol. 56, no. 2, pp. 563-570, DOI: 10.1109/TAP.2007.915423, Feb. 2008.

[5] G. Lu, Z. Liu, Y. Ye and X. Chu, "System Outage Probability and Diversity Analysis of a SWIPT-based two-way DF Relay Network under Transceiver Hardware Impairments," China Communications, vol. 20, no. 10, pp. 120-135, DOI:10.23919/JCC.ea.2021-0184.202302, 2023.

[6] J. D. Griffin and G. D. Durgin, "Link Envelope Correlation in the Backscatter Channel," IEEE Communications Letters, vol. 11, no. 9, pp. 735-737, Sep. 2007.

[7] D. -Y. Kim et al., "Reverse-link Interrogation Range of a UHF MIMO-RFID System in Nakagami-m Fading Channels," IEEE Transactions on Industrial Electronics, vol. 57, no. 4, pp. 1468-1477, April 2010.

[8] E. Vahedi, R. K. Ward and I. F. Blake, "Security Analysis and Complexity Comparison of Some Recent Lightweight RFID Protocols," Proc. of the 4th Int. Conf. on Computational Intelligence Security Inf. Syst.", vol. 6694, pp. 92-99, Spain, Jun. 2011.

[9] A. Paul et al., "Designing Quantum Gradient Descent Algorithm for MIMO NOMA Rate Maximization with STAR-RIS," IEEE Wireless Communications Letters, vol. 14, no. 4, pp. 959-963, April 2025.

[10] X. Li et al., "Physical Layer Security for Wireless-powered Ambient Backscatter Cooperative Communication Networks," IEEE Transactions on Cognitive Communications and Networking, vol. 9, no. 4, pp. 927-939, Aug. 2023.

[11] Y. Khan, A. Afzal, A. Dubey and A. Saxena, "Secrecy Performance of Energy-harvesting Backscatter Communication Network under Different Tag Selection Schemes," IEEE Journal of Radio Frequency Identification, vol. 8, pp. 43-48, DOI: 10.1109/JRFID.2024.3371877, 2024.

[12] Y. Khan et al., "Deep Learning-based Secure Tag Selection in BackCom Network with RIS-induced Interference," IEEE Journal of Radio Frequency Identification, vol. 9, pp. 797-806, 2025.

[13] N. Q. Sang, T. C. Hung, T. T. Duy, M. Tran and B. Seo Kim, "Securing Wireless Communications with Energy Harvesting and Multi-antenna Diversity," Jordanian Journal of Computers and Information Technology (JJCIT), vol. 11, no. 2, pp. 197-210, DOI: 10.5455/jjcit.71-1732244909, June 2025.

[14] M. Garai, M. Sliti and A. Elfikky, "Ground-to-Satellite FSO Communication: Evaluating Modulation Techniques under Cloud and Turbulence Effects," Jordanian Journal of Computers and Information Technology (JJCIT), vol. 11, no. 2, pp. 260-278, DOI: 10.5455/jjcit.71-1735327157, June 2025.

[15] Y. Khan, A. Dubey and S. K. Soman, "Secrecy Performance of Backscatter Communication Networks with Multiple Reader and Tag Selection Schemes," Proc. of the IEEE 2025 National Conf. on Communications (NCC), pp. 1-6, Mar. 2025.

[16] M. Nafees, D. Dharmendra and A. Kumar, "Secrecy Analysis of Energy Harvesting Backscatter Communications with Tag Selection in Nakagami-m Fading," arXiv preprint, arXiv: 2503.12400, 2025.

[17] W. Saad, X. Zhou, Z. Han and H. V. Poor, "On the Physical Layer Security of Backscatter Wireless Systems," IEEE Transactions on Wireless Communications, vol. 13, no. 6, pp. 3442-3451, June 2014.

[18] Q. Yang, H. -M. Wang, Y. Zhang and Z. Han, "Physical Layer Security in MIMO Backscatter Wireless Systems," IEEE Transactions on Wireless Communications, vol. 15, no. 11, pp. 7547-7560, Nov. 2016.

[19] T. Pecorella, L. Brilli and L. Mucchi, "The Role of Physical Layer Security in IoT: A Novel Perspective ", Information, vol. 7, no. 3, http://www.mdpi.com/2078-2489/7/3/49, 2016.

[20] T. N. Nguyen et al., "Outage Performance of Satellite Terrestrial Full-duplex Relaying Networks with Co-channel Interference," IEEE Wireless Communi. Letters, vol. 11, no. 7, pp. 1478-1482, July 2022.

[21] T. N. Nguyen et al., "Energy Harvesting-based Spectrum Access with Incremental Cooperation, Relay Selection and Hardware Noises", Radio Engineering, vol. 26, no. 1, pp. 240-250, 2017.

[22] T. N. Nguyen, D. T. Do and P. T. Tran, "Time Switching for Wireless Communications with Full-duplex Relaying in Imperfect CSI Condition ", KSII Transactions on Internet and Information Systems, vol. 10, no. 11, pp. 5455-5475, DOI: 10.3837/tiis.2016.09.011, Sep. 2016.

[23] P. T. Tin, D. T. Hung, T. N. Nguyen and T. T. Duy, "Secrecy Performance Enhancement for Underlay Cognitive Radio Networks Employing Cooperative Multi-hop Transmission with and without Presence

of Hardware Impairments", Entropy, vol. 21, no. 2, pp. 217, Feb. 2019.

[24] P. Fazio, "On the Effect of Coverage Range Extent on Next-cell Prediction Error for Vehicular Mobility in 5G/6G Networks: A Novel Theoretic Model," IEEE Transactions on Vehicular Technology, vol. 74, no. 1, pp. 1489-1503, DOI: 10.1109/TVT.2024.3453450, Jan. 2025.

[25] Z. Li, G. Wang and M. Yang, "Performance Analysis of SWIPT-aided Satellite-terrestrial Cooperative Network", Proc. of the 2022 2nd Asia-Pacific Conf. on Communications Technology and Computer Science (ACCTCS), pp. 252-256, Shenyang, China, DOI:10.1109/ACCTCS53867.2022.00059, 2022.

[26] Y. Zhang et al., "Secure Communications for Multi-tag Backscatter Systems," IEEE Wireless Communication Letters, vol. 8, no. 4, pp. 1146-1149, DOI: 10.1109/LWC.2019.2909199, Aug. 2019.

[27] I. S. Gradshteyn and I. M. Ryzhik, Table of Integrals, Series and Products, 6th Edn., ISBN-13: 978-0-12-373637-6, New York, NY, USA: Academic Press, 2000.

[28] N. I. Miridakis et al., "Dual-hop Communication over a Satellite Relay and Shadowed Rician Channels," IEEE Transactions on Vehicular Technology, vol. 64, no. 9, pp. 4031-4040, Sept. 2015.

[29] S. Neumark, Solution of Cubic and Quartic Equations, ISBN: 978-0-08-011220-6, Oxford: Pergamon Press, 1965.

[30] B. Gu, D. Li, H. Ding, G. Wang and C. Tellambura, "Breaking the Interference and Fading Gridlock in Backscatter Communications: State-of-the-Art, Design Challenges and Future Directions," IEEE Communications Surveys & Tutorials, vol. 27, no. 2, pp. 870-911, 2025.

[31] S. Mondal et al., "A Comprehensive Survey on NOMA-based Backscatter Communication for IoT Applications," IEEE Internet of Things Journal, vol. 12, no. 12, pp. 18929-18953, 2025.

[32] M. Ahmed et al., "NOMA-based Backscatter Communications: Fundamentals, Applications and Advancements," IEEE Internet of Things Journal, vol. 11, no. 11, pp. 19303-19327, 2024.

[33] S. Zargari, D. Galappaththige and C. Tellambura, "Transmit Power-efficient Beamforming Design for Integrated Sensing and Backscatter Communication," IEEE Open Journal of the Communications Society, vol. 6, pp. 775-792, DOI: 10.1109/OJCOMS.2025.3527860, 2025.

[34] F. R. Ghadi, M. Kaveh, K.-K. Wong and Y. Zhang, "Performance Analysis of FAS-aided Backscatter Communications," IEEE Wireless Communications Letters, vol. 13, no. 9, pp. 2412-2416, 2024.

[35] F. Xia, Z. Fei, X. Wang, P. Liu, J. Guo and Q. Wu, "Joint Waveform and Reflection Design for Sensing-assisted Secure RIS-based Backscatter Communication," IEEE Wireless Communications Letters, vol. 13, no. 5, pp. 1523-1527, DOI: 10.1109/LWC.2024.3381163, 2024.

[36] S. Jia et al., "Secrecy Performance Analysis of UAV-assisted Ambient Backscatter Communications with Jamming," IEEE Transactions on Wireless Communications, vol. 23, no. 12, pp. 18111-18125, 2024.

[37] H. Luo et al., "Symbiotic Blockchain Consensus: Cognitive Backscatter Communications-enabled Wireless Blockchain Consensus," IEEE/ACM Trans. on Networking, vol. 32, no. 6, pp. 5372-5387, 2024.

[38] L. S. Phu et al., "Enhancing Short-packet Communications: BLER Performance in RIS-assisted Ambient Backscatter NOMA Systems," PLoS ONE, vol. 20, no. 8, pp. 1-26, Aug. 2025.

[39] T. C. Hung, V. M. Bui, T. N. Nguyen and M. Voznak, "Power Beacon-assisted Energy Harvesting Symbiotic Radio Networks: Outage Performance," PLoS ONE, vol. 20, no. 2, pp. 1-16, Feb. 2025.

[40] A.-T. Le et al., "Performance Analysis of RIS-assisted Ambient Backscatter Communication Systems," IEEE Wireless Communications Letters, vol. 13, no. 3, pp. 791-795, 2024.

[41] T.-H. T. Pham et al., "Performance Analysis in D2D Partial NOMA-assisted Backscatter Communication," Advances in Electrical & Electronic Engineering, vol. 23, no. 3, DOI: 10.15598/aeee.v23i3.250314, 2025.

[42] T. C. Hung, Q. Sang Nguyen, V. M. Bui, T.-Q. Thi and N.-L. Nguyen, "Multi-power Beacon Empowered Secure in IoT Networks: Secrecy Outage Probability Analysis," Advances in Electrical & Electronic Engineering, vol. 23, no. 2, DOI: 10.15598/aeee.v23i2.241112, 2025.

[43] Y. Pei, X. Yue, C. Huang and Z. Lu, "Secrecy Performance Analysis of RIS-assisted Ambient Backscatter Communication Networks," IEEE Transactions on Green Communications and Networking, vol. 8, no. 3, pp. 1222-1232, DOI: 10.1109/TGCN.2024.3365692, 2024.

[44] Y. Khan et al., "Secrecy Analysis of Energy Harvesting Backscatter Communication Networks with Multiple Eavesdroppers and Different Tag Selection Schemes," IEEE Transactions on Green Communications and Networking, Early Access, p. 1, DOI: 10.1109/TGCN.2025.3563107, 2025.

[45] J. Li, P. Wang, L. Jiao, Z. Yan, K. Zeng and Y. Yang, "Security Analysis of Triangle Channel-based Physical Layer Key Generation in Wireless Backscatter Communications," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 948-964, DOI: 10.1109/TIFS.2022.3224852, 2023.

[46] R. Singh, I. Ahmad and J. Huusko, "The Role of Physical Layer Security in Satellite-based Networks," Proc. of the 2023 Joint European Conf. on Networks and Communications & 6G Summit (EuCNC/6G Summit), pp. 36-41, DOI: 10.1109/EuCNC/6GSummit58263.2023.10188370, 2023.

[47] S. Jia, R. Wang, Y. Xu, Y. Lou, D. Zhang and T. Sato, "Secrecy Analysis of ABCom-based Intelligent Transportation Systems with Jamming," IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 3, pp. 2880-2892, DOI: 10.1109/TITS.2023.3250427, 2024.

[48] Z. Liu, Y. Ye, X. Chu and H. Sun, "Secrecy Performance of Backscatter Communications with Multiple Self-powered Tags," IEEE Communications Letters, vol. 26, no. 12, pp. 2875-2879, 2022.
[49] L. Bai, Q. Chen, T. Bai and J. Wang, "UAV-enabled Secure Multiuser Backscatter Communications with Planar Array," IEEE Journal on Selected Areas in Communications, vol. 40, no. 10, p. 29462961, 2022.
[50] Y. Lei, Y. Ye, X. Chu, G. Chen and G. Lu, "On the Strict Secrecy Outage Probability of Wirelessly Powered Backscatter Communications," IEEE Transactions on Vehicular Technology, vol. 74, no. 5, pp. 8345-8350, DOI: 10.1109/TVT.2024.3523389, 2025.

ملخص البحث:

تبحث هذه الدّراسة في الأداء الآمن لجهاز التّشتُّت الخلفي في نظام اتّصال بين الأقمار الصّناعية والمحطّات الأرضية في حال وجود احتمال لاختراق النّظام. وفي النّظام المقترح، يقوم قمر صناعي بإرسال إشاراتٍ إلى جهاز تشتُّت خلفي يعمل بدوره على عكس المعلومات المعدّلة لتعود إلى القمر الصناعي بينما يتعرّض النّظام إلى محاولة اختراق.

ويتمّ تحليل النّظام المقترح عبر تجارب تُجرى على عددٍ من مؤشّرات الأداء الآمن للحصول على تشغيل آمن للنّظام. كذلك تُجرى تجارب للحصول على فهمٍ شاملٍ وأكثر عمقاً للتّشغيل الآمن للنّظام في ظلّ قيمٍ عالية لنسبة الإشارة إلى الضّجيج. ومن ناحيةٍ أخرى، تمّ إجراء عمليات محاكاة مونتي كارلو للتّحقُّق من دقّة التّحليل النّظري. وقد أسفرت التّجارب عن تأكيد دقّة عمل النّظام المقترح بشكل آمن.