EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Ensuring Security in Multi-Tag Backscatter Communication Systems

Zilin You[1,2,*], Zhihong Liang[1,2], Siliang Suo[1,2], Lifeng Mai[1,2], and Qiaoling Lin[1,2]

[1]Electric Power Research Institute, CSG, Guangzhou Guangdong, China
[2]Guangdong Provincial Key Laboratory of Power System Network Security, Guangzhou Guangdong, China

Abstract

This paper studies the security performance of a multi-tag backscatter communication system for power data network, where a reader exchanges its information with multiple distributed tags in the presence of an eavesdropper. The system security performance is assessed using the secrecy outage probability (SOP), which quantifies the likelihood that the system secrecy capacity drops below a specified threshold. The paper provides a mathematical analysis on the communication links, considering Rayleigh fading, and investigates the effect of system monostatic and bistatic RFID configurations on the overall security. An optimal tag selection scheme is proposed to maximize the secrecy capacity by choosing the tag with the best link between the reader and the eavesdropper. Moreover, an analytical expression is derived for the system SOP, which incorporates the joint probability distributions of channel gains and the asymptotic SOP is provided as the signal-to-noise ratio increases. Simulation results are presented to verify the theoretical analysis, where the simulation results closely match the analytical predictions, confirming the accuracy of the proposed SOP analysis. Moreover, the asymptotic analysis offers an upper bound on the outage probability, consistent with theoretical analysis.

Received on 09 July 2025; accepted on 11 December 2025; published on 12 January 2026

Keywords: Power data network, multi-tag, secure transmission, backscatter communication.

doi:10.4108/eetsis.9691

1. Introduction

Internet of Things (IoT) has been developed to support ubiquitous connectivity, large-scale sensing, and intelligent data processing , viewed as the core features of next-generation cyber-physical systems [1–3]. Various IoT techniques have been proposed, in which perception, network, and application layers are typically distinguished, and heterogeneous devices have been integrated through standardized communication protocols [4–6]. Security, privacy, and interoperability of IoT networks have been investigated, and a variety of lightweight cryptographic schemes, edge-computing framework, and middleware platforms have been designed to address these issues in resource-constrained environments [7, 8]. Within this broader context, radio-frequency identification (RFID) technology has been extensively examined as a key enabling component of IoT perception, through which automatic identification, tracking, and data collection of physical objects are realized [9–11]. Low-cost passive and active RFID tags have been investigated for supply chain management, smart retail, healthcare, and industrial monitoring, and numerous anti-collision algorithms, RFID middleware solutions, and security-enhanced tag¨Creader protocols have been proposed, thereby demonstrating how RFID-based systems can be seamlessly embedded into large-scale IoT deployments.

In various IoT applications, especially in power data networks, RFID technology has evolved in both hardware and communication protocols [12–14]. Initially, passive RFID systems were developed, where information was transmitted via radio waves without the need for an internal power source in the tag. These systems were widely adopted for inventory tracking and access control applications due to the simplicity and cost-effectiveness. Over time, active RFID tags, which incorporated the own power

*Corresponding author. Email: zilinYou123@hotmail.com

sources, were introduced, offering extended read ranges and additional capabilities such as real-time location tracking [15, 16]. As RFID technology evolved, the efficiency and scalability of large-scale deployments of IoT networks were studied, where some sophisticated communication techniques have been proposed. One of the notable techniques is the integration of backscatter communication, a technique in which the RFID tag reflects the incident radio signal to transmit information back to the reader, which can help reduce the power consumption and enable communication in environments where energy efficiency is critical [17–19]. Backscatter communication has become a key enabler for the next generation of IoT systems, allowing for ultra-low-power, high-efficiency data transmission over long distances, further enhancing the utility of RFID in diverse applications, including smart cities and wireless sensor networks.

In recent years, physical-layer security (PLS) has attracted much attention for communication systems, driven by the need for more robust security mechanisms beyond traditional cryptographic methods [20–22]. PLS leverages the inherent properties of the physical communication channel, such as channel randomness and interference, to provide security against eavesdropping. In this field, secure transmission techniques have been proposed to exploit channel state information at both the transmitter and receiver, enabling the creation of secrecy regions where information can be transmitted securely. Moreover, multi-antenna techniques, such as beamforming and multi-input multi-output (MIMO) systems, have been proposed to enhance the ability to increase signal strength in the legitimate communication link while simultaneously reducing the eavesdropper's ability to intercept the signal [23–25]. A critical aspect of PLS is the analysis of secrecy outage probability (SOP), which quantifies the likelihood that the secrecy capacity of the channel falls below a required threshold, resulting in a security breach. The SOP of communication systems has been widely studied, with analytical expressions were developed to evaluate the impact of various parameters, such as transmit power, noise levels, fading conditions, and the presence of eavesdroppers, on the overall security performance. Various techniques, such as power allocation strategies, cooperative jamming, and the use of artificial noise, have been proposed to mitigate SOP and enhance security in both single-user and multi-user systems, ensuring secure communication even under challenging propagation conditions [26–28].

This paper investigates the security performance of a multi-tag backscatter communication system, where a reader interacts with several distributed tags in the presence of an eavesdropper. The system security performance is evaluated through the SOP analysis, and a mathematical analysis on the communication links is developed, accounting for Rayleigh fading, and the impact of system monostatic and bistatic RFID configuration on the security is investigated. An optimal tag selection scheme is designed to maximize the system secrecy capacity by selecting the tag with the best links between the reader and the eavesdropper. Then, an analytical expression for the SOP is derived, incorporating the joint probability distributions of various channel gains, and the system SOP asymptotic behavior is studied as the signal-to-noise ratio increases. To validate the theoretical analysis, simulation results are provided, and a detailed comparison between simulated, analytical, and asymptotic results is presented. These comparisons confirm that as the signal-to-noise ratio increases, the outage probability decreases, thereby enhancing the system security. The simulation results closely align with the analytical predictions, affirming the validity of the proposed model, while the asymptotic approximation offers an upper bound on the outage probability, consistent with theoretical expectations.

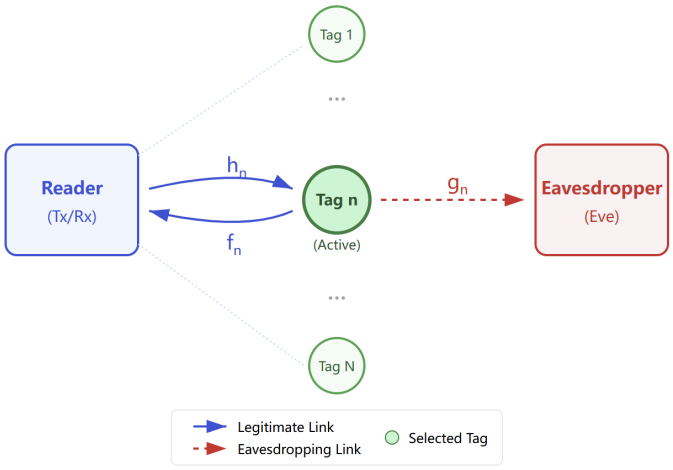

Figure 1. System model of a multi-tag backscatter communication system.

2. System Model

Fig. 1 illustrates the system model of a multi-tag backscatter communication setup, consisting of a reader, N spatially distributed tags, and an eavesdropper attempting to intercept the signals transmitted by the tags. In this system, h_n denotes the channel gain from the reader's transmitting antenna to the n-th tag, f_n represents the channel gain from the n-th tag to the reader's receiving antenna, and g_n refers to the channel gain from the n-th tag to the eavesdropper. It is assumed that the channel gains for all communication links follow a Rayleigh distribution, given by,

$$h_n \sim \mathcal{CN}(0, a), \quad f_n \sim \mathcal{CN}(0, b), \quad g_n \sim \mathcal{CN}(0, c), \quad (1)$$

where $\mathrm{CN}(\mu, \sigma^2)$ denote the complex Gaussian distribution with mean μ and variance σ^2. The reader receives the signal from the n-th tag,

$$y_{rn} = h_n f_n s b + n_r. \tag{2}$$

In an RFID backscatter system, the system architecture plays a crucial role in shaping the behavior of the communication links. The correlation between the forward link h_n and the backscatter link f_n varies depending on the system configuration. In a monostatic setup, where the transmit and receive antennas are colocated on the reader, the forward and backscatter links exhibit perfect correlation. Conversely, in a bistatic RFID configuration, where the antennas are spatially separated, the correlation between these two links is only partial. This architectural distinction has a substantial impact on both system performance and security. Moreover, the bistatic arrangement offers practical advantages for deployment, such as reducing interference and improving communication reliability. The distributions of the squared magnitudes $|h_n|^2$ and $|f_n|^2$ are given by,

$$f_{|h_n|^2,|f_n|^2}(x_1, x_2) = \exp\left(-\frac{x_1}{(1-\lambda)a} - \frac{x_2}{(1-\lambda)b}\right)\frac{1}{ab(1-\lambda)} \times I_0\left(\frac{2\sqrt{\lambda x_1 x_2}}{\sqrt{ab(1-\lambda)}}\right), \tag{3}$$

where $\lambda \in [0, 1]$ represents the correlation between the channels, which is defined as,

$$\lambda = \frac{\mathrm{Cov}(X_1, X_2)}{\sqrt{\mathrm{Var}(X_1)\mathrm{Var}(X_2)}}. \tag{4}$$

Additionally, $I_0(\cdot)$ denotes the modified Bessel function of the first kind, it can be expressed as an infinite series,

$$I_0(x) = \sum_{m=0}^{\infty} \frac{(x/2)^{2m}}{(m!)^2}. \tag{5}$$

The signal captured by the eavesdropper from the n-th tag is,

$$y_{en} = h_n g_n s b + n_e, \tag{6}$$

where n_e represents the additive white Gaussian noise (AWGN) at the eavesdropper, modeled as $n_e \sim \mathcal{CN}(0, \sigma_e^2)$. We assume that the channels h_n and g_n are independent, given that the eavesdropper is positioned at a much greater distance from the reader, significantly farther than from the tag, the instantaneous signal-to-noise ratios (SNRs) at both the reader and the eavesdropper can be determined using (2) and (6) as,

$$\zeta_{rn} = \frac{|h_n f_n|^2 P_s}{\sigma_r^2}, \tag{7}$$

$$\zeta_{en} = \frac{|h_n g_n|^2 P_s}{\sigma_e^2}. \tag{8}$$

Here, the transmission power is denoted as $P_s = \mathbb{E}|s|^2$, while ζ_{rn} and ζ_{en} represent the average SNRs at the reader and the eavesdropper, respectively. By applying (7) and (8), the channel capacities for both the reader and the eavesdropper can be given by,

$$C_{rn} = \log_2(1 + \zeta_{rn}), \tag{9}$$

$$C_{en} = \log_2(1 + \zeta_{en}), \tag{10}$$

By utilizing the previously obtained capacity expressions, we can calculate the instantaneous secrecy capacity for the multi-tag RFID backscatter system as:

$$C_{sn} = C_{rn} - C_{en} = \begin{cases} \log_2\left(\frac{1+\zeta_{rn}}{1+\zeta_{en}}\right), & \zeta_{rn} \geq \zeta_{en}, \\ 0, & \zeta_{rn} < \zeta_{en}. \end{cases} \tag{11}$$

In the multi-tag backscatter communication system under consideration, we assume that the reader possesses complete channel state information (CSI) for the wireless links. Utilizing this CSI, the reader selects one tag from the set of N available tags to transmit the information. To optimize the system secrecy capacity, the tag selection strategy is devised from the secrecy capacity expression in (11). The optimal tag, n^*, is then selected as:

$$n^* = \arg \max_{1 \leq n \leq N} \left(\frac{1 + |h_n f_n|^2 \zeta_{rn}}{1 + |h_n g_n|^2 \zeta_{en}}\right). \tag{12}$$

This optimal tag selection (TS) strategy ensures that the selected tag for transmission can optimize the disparity in channel conditions between the reader and the eavesdropper, ultimately enhancing the overall secrecy capacity.

3. Secrecy Outage Probability Analysis

In this section, we analyze the secrecy outage probability (SOP) for the multi-tag RFID backscatter system, a key metric for assessing system security. The SOP represents the likelihood that the instantaneous secrecy capacity falls below a predefined threshold R_s. We assess the system's SOP under the condition of optimal tag selection. The system SOP P_{out} is given by, The optimal tag, n^*, is then selected as:

$$P_{\text{out}} = \Pr\left[\log_2\left(\frac{1 + \zeta_{rn^*}}{1 + \zeta_{en^*}}\right) < R_s\right], \tag{13}$$

which can also be expressed as,

$$P_{\text{out}} = \Pr\left[1 + |h_{n^*} f_{n^*}|^2 \zeta_r < \zeta_s, \quad 1 + |h_{n^*} g_{n^*}|^2 \zeta_e < \zeta_s\right], \tag{14}$$

or equivalently,

$$P_{\text{out}} = \Pr\left[\max_{1\le n\le N}\left(1+|h_n f_n|^2\zeta_r\right) < \zeta_s, \quad 1+|h_n g_n|^2\zeta_e < \zeta_s\right]. \tag{15}$$

Here, $\zeta_s = 2^{R_s}$ represents the secrecy SNR threshold. Given the assumption that the tags are independent, the expression can be reformulated as,

$$P_{\text{out}} = \Pr\left[\left(1+|h_1 f_1|^2\zeta_r\right) < \zeta_s, \quad \left(1+|h_1 g_1|^2\zeta_e\right) < \zeta_s\right]^N, \tag{16}$$

which can be simplified as,

$$P_{\text{out}} = \Pr\left[\left(|h_1|^2(\zeta_r|f_1|^2 - \zeta_e\zeta_s|g_1|^2)\right) < \zeta_s - 1\right]^N. \tag{17}$$

Let

$$w_1 = |h_1|^2, \quad w_2 = |f_1|^2, \quad w_3 = |g_1|^2, \tag{18}$$

and define

$$u = \zeta_r w_2 - \zeta_e\zeta_s w_3. \tag{19}$$

The system SOP expression becomes,

$$P_{\text{out}} = \Pr\left[\max_{1\le n\le N}\left(1+|h_n f_n|^2\zeta_r\right) < \zeta_s\right]. \tag{20}$$

To derive the SOP, we begin by determining the probability density function (PDF) of u. By applying fundamental statistical techniques for the difference of two random variables, the PDF of u can be expressed as,

$$f(u) = \begin{cases} \frac{1}{\zeta_e\zeta_s c+b\zeta_r}\exp\left(-\frac{u}{b\zeta_r}\right), & u \ge 0, \\ \frac{1}{\zeta_e\zeta_s c+b\zeta_r}\exp\left(\frac{u}{c\zeta_s\zeta_e}\right), & u < 0. \end{cases} \tag{21}$$

This distribution is crucial for computing the SOP, as it captures the likelihood of the difference between the forward and backscatter channels falling below the secrecy threshold. Based on the positive and negative u, (17) can be rewritten as,

$$\begin{aligned} P_{\text{out}} &= \{\Pr[w_1 u < \zeta_s - 1]\}^N \\ &= \Pr\left[0 < w_1 < \frac{\zeta_s - 1}{u} \quad \text{or} \quad u > 0\right] \\ &\quad + \Pr[w_1 > 0 \quad \text{and} \quad u < 0] \\ &= (I_1 + I_2)^N, \end{aligned} \tag{22}$$

where

$$I_1 = \int_0^\infty \int_0^{\zeta_s^{-1}u} f(w_1, w_2) f(u)\, dw_1 du dw_2, \tag{23}$$

$$I_2 = \int_0^\infty \int_{-\infty}^0 f(w_1, w_2) f(u)\, dw_1 du dw_2. \tag{24}$$

In this context, $f(w_1, w_2)$ represents the joint PDF of w_1 and w_2. By substituting (5) into (3), we can have,

$$f(w_1, w_2) = \sum_{k=0}^{\infty} \rho_0 w_1^k w_2^k e^{-\rho_1 w_1} e^{-\rho_2 w_2}, \tag{25}$$

where ρ_0, ρ_1, and ρ_2 are constants, given by,

$$\rho_0 = \frac{\lambda^k}{(1-\lambda)(2k+1)(ab)^{k+1}(k!)^2}, \tag{26}$$

$$\rho_1 = \frac{1}{(1-\lambda)a}, \quad \rho_2 = \frac{1}{(1-\lambda)b}. \tag{27}$$

From the above equations, we can obtain the following expressions for I_1 and I_2,

$$I_1 = \sum_{k=0}^{\infty} k! b\zeta_r^{k+1} - 2\beta\left(b\zeta_r^{1-k}\right) K_{k+1}\left(2\beta\sqrt{b\zeta_r}\right), \tag{28}$$

$$I_2 = \sum_{k=0}^{\infty} \lambda^k(1-\lambda)\zeta_s\zeta_e\left(\frac{1}{\zeta_s\zeta_e + b\zeta_r}\right), \tag{29}$$

where $\beta = \rho_1(\zeta_s - 1)$. From the analytical I_1 and I_2, we can finally obtain the analytical expression of SOP for the considered multi-tag backscatter communication system,

$$\begin{aligned} P_{\text{out}} = \Bigg\{ \sum_{k=0}^{\infty} \frac{\lambda^k(1-\lambda)}{(c\zeta_s\zeta_e + b\zeta_r)} \Bigg[c\zeta_s\zeta_e + b\zeta_r - 2\beta_1 \left(\frac{b\zeta_r}{2}\right)^{k+1/2} \\ \times K_{k+1}\left(2\sqrt{\beta_1 (b\zeta_r)^{-1}}/k!\right)\Bigg]\Bigg\}^N. \end{aligned} \tag{30}$$

The above analytical expression of SOP can be used to evaluate the security performance of the considered multi-tag backscatter communication system. However, this expression involves an infinite series, making it difficult to obtain practical insights on the system optimization. To simplify the analysis and gain a clearer understanding of the system security performance, we derive the asymptotic SOP as the average SNR at the receiver approaches infinity. Note that the function $K_1(\cdot)$ can be approximated as,

$$K_1(x) \sim \frac{1}{x} + \frac{x}{2}\ln\left(\frac{x}{2}\right), \tag{31}$$

as $x \to 0$. Substituting this approximation into (30), we can derive a closed-form expression for the SOP as ζ_e increases, given by,

$$P_{\text{out}}^{\infty} = \left[\frac{c\zeta_s\zeta_e + \beta\ln(b\zeta_r/\beta)}{b\zeta_r}\right]^N, \tag{32}$$

When ζ_e is small, the term $c\zeta_s\zeta_e$ in (32) can be neglected, simplifying the expression for the asymptotic SOP, yielding,

$$P_{\text{out}}^{\infty} = \left[\frac{\ln(b\zeta_r/\beta)}{b\zeta_r/\beta}\right]^N, \tag{33}$$

where $b_{\beta r} = b\zeta_r(1-\lambda)/(\zeta_s - 1)$. From (32) and (33), we observe that as the correlation λ between the forward and backscatter links increases, the asymptotic SOP worsens. This implies that a higher correlation between these links reduces the communication security performance, making the system more vulnerable to interference. In particular, when the correlation is strong, the forward and backscatter channels become less independent, diminishing the system secrecy. In RFID systems, the channel fading parameters a and b are crucial factors that influence the secrecy performance. Increasing these parameters can enhance the overall secrecy by improving the system capability to separate communication links. Additionally, as the number of tags N increases, the system diversity order of secure transmission improves, further boosting system security.

4. Simulations Results and Discussions

In this paper, we perform some simulations for the considered multi-tag backscatter communication system where a reader exchanges information with multiple distributed tags, while an eavesdropper attempts to capture the transmitted signals. The channel gains are modeled using Rayleigh fading distributions. The paper utilizes both monostatic and bistatic RFID configurations, with the correlation coefficient λ between the forward and backscatter links being a key parameter. The number of tags varies from 1 to 3. Additionally, the main-to-eavesdropper ratio (MER) varies from -5dB to 30dB, and the correlation coefficient λ varies from 0.2 to 0.8. These simulations settings are used to validate the theoretical analysis by comparing the system SOP for different system configurations.

Fig. 2 illustrates the SOP performance of the considered multi-tag backscatter communication system versus the main-to-eavesdropper ratio (MER), with different numbers of tags ($N = 1, 2, 3$) and $\lambda = 0.2$. From this figure, we can find that the system secrecy outage probability decreases as the MER increases, indicating that higher MERs lead to a more secure communication environment. For instance, at an MER of 10 dB, the SOP for $N = 1$ is approximately 10^{-2}, while for $N = 3$, it drops to around 10^{-3}, demonstrating the benefit of increasing the number of tags. Additionally, as the number of tags increases, the system capability to withstand interference improves, resulting in a lower SOP. This effect is due to the increased system diversity, which provides more options for selecting tags that optimize

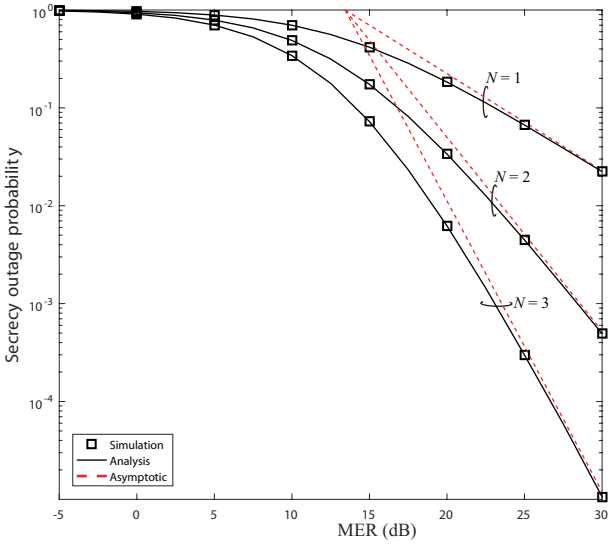

Figure 2. Secrecy outage probability versus MER with $\lambda = 0.2$.

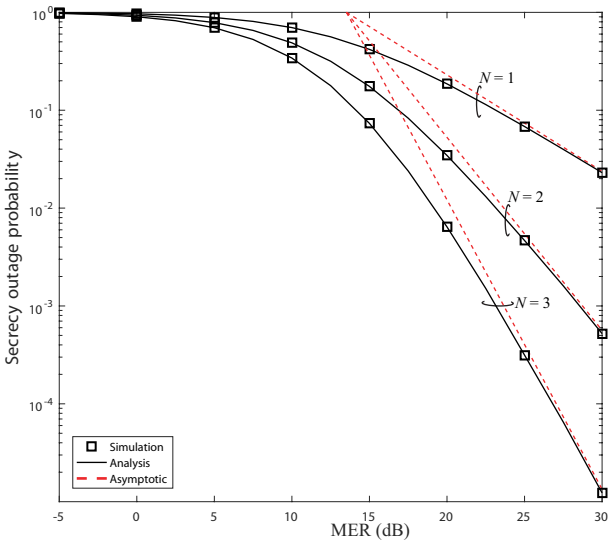

Figure 3. Secrecy outage probability versus MER with $\lambda = 0.5$.

the secrecy capacity. Moreover, the comparison between the simulation results, theoretical analysis, and asymptotic analysis reveals a strong alignment, confirming the accuracy of the proposed theoretical analysis. In further, the line slope of the asymptotic result changes with N, showing that the system's secrecy diversity order increases linearly with N.

Fig. 3 shows the SOP of the considered multi-tag backscatter communication system versus the MER for different values of the number of tags N (i.e., $N = 1, 2, 3$), with a correlation $\lambda = 0.5$. From Fig. 3, one can find that as N increases, the SOP decreases. For instance, at an MER of 10 dB, the SOP for $N = 1$ is approximately 10^{-2}, while for $N = 3$, it decreases to around 10^{-3}, demonstrating the

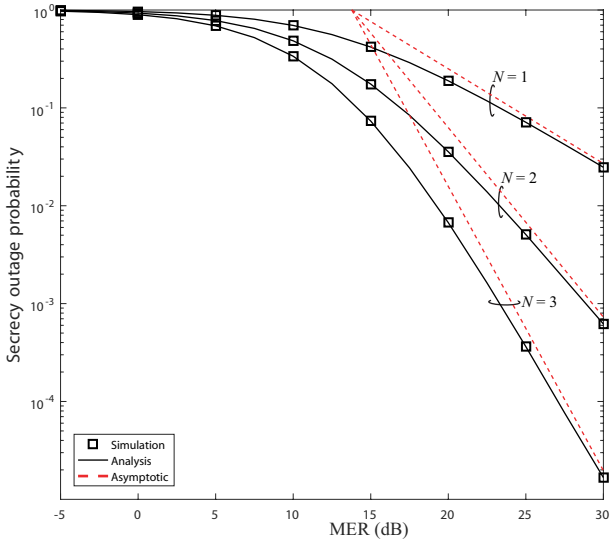

Figure 4. Secrecy outage probability versus MER with $\lambda = 0.8$.

advantage of increasing the number of tags. This effect is due to the increased diversity, as more tags provide more options for selecting the one with the best channel conditions, optimizing the secrecy capacity and improving the system's capability to withstand interference. The comparison between simulated, analytical, and asymptotic results reveals strong agreement, validating the theoretical analysis. The asymptotic analysis further shows that the slope of the SOP curve changes with N, indicating that the system's secrecy diversity order increases linearly with N. As the number of tags increases, the system becomes more resilient to eavesdropping, and the secrecy performance improves significantly. This emphasizes the critical role of N in enhancing system security. Specifically, at an MER of 10 dB, the SOP values for $N = 1$ and $N = 3$ are approximately $P_{\text{out}}(N = 1) \approx 10^{-2}$ and $P_{\text{out}}(N = 3) \approx 10^{-3}$, respectively, clearly illustrating the significant reduction in SOP with the increase in N, which enhances the overall security of the communication system.

Fig. 4 illustrates the system SOP of the considered multi-tag backscatter communication with respect to, where N varies from 1 to 3, and the correlation coefficient λ is set to 0.8. From Fig. 4, we can find that the system SOP decreases significantly as the number of tags N increases. Specifically, at an MER of 10 dB, the SOP for $N = 1$ is approximately 10^{-2}, while for $N = 3$, the SOP drops to around 10^{-3}. This demonstrates the impact of increasing N on improving the system's security by enhancing the diversity of the system, providing more options to select the optimal tag for communication. Moreover, the slope of the SOP curve changes with N, which is consistent with the theoretical analysis that the secrecy diversity order increases linearly with N. As the number of tags grows, the system's ability to withstand interference improves, leading to a more secure communication environment. This indicates the crucial role of N in reducing the SOP and improving the overall security of the multi-tag backscatter communication system. Specifically, at an MER of 10 dB, the SOP for $N = 1$ and $N = 3$ are approximately $\text{Pout}(N = 1) \approx 10^{-2}$ and $\text{Pout}(N = 3) \approx 10^{-3}$, respectively, clearly showing the significant reduction in SOP with the increase in N, thus enhancing the overall security of the communication system.

5. Conclusions

This paper examined the security performance of the considered multi-tag backscatter system, focusing on SOP as a critical metric for evaluating system security. An optimal tag selection scheme was proposed, which maximized the system secrecy capacity by selecting the tag with the best channel links between the reader and the eavesdropper, based on CSI. Theoretical analyses were carried out to derive SOP expressions and study the asymptotic behavior as the SNR increased. These analyses were validated through simulations, which confirmed t hat t he proposed analysis accurately predicted the system security performance. In particular, increasing the number of tags significantly i mproved s ystem s ecurity by enhancing diversity order, which provides more robust options for tag selection, thereby reducing the likelihood of eavesdropping. Additionally, the correlation between the forward and backscatter links was found to have a notable impact on secrecy performance, where a higher correlation between these links resulted in a less secure system, indicating the importance of managing link correlations for optimal security. Overall, the findings p rovided valuable insights for the design and optimization of secure backscatter communication systems, offering a solid foundation for future IoT applications.

References

[1] S. S. Saab, D. Shen, M. Orabi, D. Kors, and R. H. Jaafar, "Iterative learning control: Practical implementation and automation," *IEEE Trans. Ind. Electron.*, vol. 69, no. 2, pp. 1858–1866, 2022.

[2] T. Klopot, P. Skupin, P. Grelewicz, and J. Czeczot, "Practical plc-based implementation of adaptive dynamic matrix controller for energy-efficient control of heat sources," *IEEE Trans. Ind. Electron.*, vol. 68, no. 5, pp. 4269–4278, 2021.

[3] K. Yang, D. Liu, S. Baldi, and C. Lv, "On practical implementations of connected vehicles: The issue of

acceleration feedback," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 12, pp. 21 035–21 046, 2024.

[4] Y. Wu, D. Xu, D. W. K. Ng, R. Schober, and W. H. Gerstacker, "Globally optimal resource allocation design for discrete phase shift irs-assisted multiuser networks with perfect and imperfect CSI," *IEEE Trans. Wirel. Commun.*, vol. 24, no. 2, pp. 1306–1324, 2025.

[5] S. Kurma, K. Singh, P. K. Sharma, C. Li, and T. A. Tsiftsis, "On the performance analysis of full-duplex cell-free massive MIMO with user mobility and imperfect CSI," *IEEE Trans. Commun.*, vol. 73, no. 5, pp. 3683–3701, 2025.

[6] M. A. Ajay, K. Agrawal, S. K. Singh, K. Singh, S. Prakriya, and C. Li, "Performance of battery-assisted EH full-duplex NOMA network with FBL driven mode switching under imperfect CSI and SIC," *IEEE Trans. Commun.*, vol. 73, no. 6, pp. 4486–4502, 2025.

[7] C. Li, Y. Yang, J. Song, X. Zhang, and Q. Xu, "A short-term power load visualization forecasting method based on 2DVMD and ConvLSTM," *Southern Power System Technology*, vol. 19, no. 2, pp. 1–9, 2025.

[8] C. Ye, J. Chen, X. Ma, and Z. Hu, "Anti-UAV target detection algorithm for substation based on improved YOLOv5," *Southern Power System Technology*, vol. 18, no. 2, pp. 89–97, 2024.

[9] X. Liu, H. Zhang, K. Long, A. Nallanathan, and V. C. M. Leung, "Distributed unsupervised learning for interference management in integrated sensing and communication systems," *IEEE Trans. Wirel. Commun.*, vol. 22, no. 12, pp. 9301–9312, 2023.

[10] A. Rahmati, S. Hosseinalipour, Y. Yapici, X. He, I. Güvenç, H. Dai, and A. Bhuyan, "Dynamic interference management for uav-assisted wireless networks," *IEEE Trans. Wirel. Commun.*, vol. 21, no. 4, pp. 2637–2653, 2022.

[11] J. Huang, C. Yang, S. Zhang, F. Yang, O. Alfarraj, V. Frascolla, S. Mumtaz, and K. Yu, "Reinforcement learning based resource management for 6g-enabled miot with hypergraph interference model," *IEEE Trans. Commun.*, vol. 72, no. 7, pp. 4179–4192, 2024.

[12] X. Zhang, J. Li, J. Wu, G. Chen, Y. Meng, H. Zhu, and X. Zhang, "Binary-level formal verification based automatic security ensurement for PLC in industrial iot," *IEEE Trans. Dependable Secur. Comput.*, vol. 22, no. 3, pp. 2211–2226, 2025.

[13] F. Li, J. Wang, W. Xie, N. Tong, and D. Wang, "X-RAFT: improve RAFT consensus to make blockchain better secure edgeai-human-iot data," *IEEE Trans. Emerg. Top. Comput.*, vol. 13, no. 1, pp. 22–33, 2025.

[14] M. Liang, K. Liu, R. Gao, and Y. Li, "Integrating gpu-accelerated for fast large-scale vessel trajectories visualization in maritime iot systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 26, no. 3, pp. 4048–4065, 2025.

[15] M. Liu, H. Peng, P. Zhang, M. Zeng, Z. Zhu, A. A. Boulogeorgos, K. Dev, and X. Li, "Ris-segmented symbiotic covert cooperative backscatter communication systems," *IEEE Trans. Veh. Technol.*, vol. 74, no. 1, pp. 1708–1712, 2025.

[16] J. Chen, Q. Guan, Y. Rong, D. Li, W. Chen, and H. Yu, "High order time shift keying modulation for ambient backscatter communications," *IEEE Trans. Commun.*, vol. 73, no. 6, pp. 3792–3803, 2025.

[17] Q. Zhang, Z. Wang, C. Zhou, S. Wang, D. Zhou, S. Jiang, L. Cai, and Y. Li, "A packaging scheme enabling resonant frequency tuning and magnetic shielding for electromagnetic vibration energy harvesters toward industrial applications," *IEEE Trans. Instrum. Meas.*, vol. 74, pp. 1–10, 2025.

[18] K. Huang, W. Cao, Y. Liu, D. Wu, C. Yang, and W. Gui, "A weighted deep learning-based predictive control for multimode nonlinear system with industrial applications," *IEEE Trans Autom. Sci. Eng.*, vol. 22, pp. 10 814–10 826, 2025.

[19] K. Huang, X. Ying, D. Wu, C. Yang, and W. Gui, "A generalized integrated fuzzy-mpc with optimal input excitation for complex systems with industrial applications," *IEEE Trans. Fuzzy Syst.*, vol. 33, no. 5, pp. 1415–1428, 2025.

[20] Y. Zhang, Y. Ko, R. F. Woods, and A. Marshall, "Defining spatial secrecy outage probability for exposure region-based beamforming," *IEEE Trans. Wirel. Commun.*, vol. 16, no. 2, pp. 900–912, 2017.

[21] J. D. V. Sánchez, L. F. Urquiza-Aguiar, H. R. C. Mora, N. V. O. Garzón, and D. P. M. Osorio, "Fluid antenna system: Secrecy outage probability analysis," *IEEE Trans. Veh. Technol.*, vol. 73, no. 8, pp. 11 458–11 469, 2024.

[22] B. Li, Y. Zou, J. Zhou, F. Wang, W. Cao, and Y. Yao, "Secrecy outage probability analysis of friendly jammer selection aided multiuser scheduling for wireless networks," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3482–3495, 2019.

[23] R. K. Mallik, "Multiplexing with multi-level ASK and noncoherent MIMO in rayleigh fading," *IEEE Trans. Commun.*, vol. 72, no. 10, pp. 6162–6177, 2024.

[24] J. Gao, Y. Wu, G. Caire, W. Yang, H. V. Poor, and W. Zhang, "Unsourced random access in MIMO quasi-static rayleigh fading channels: Finite blocklength and scaling law analyses," *IEEE Trans. Inf. Theory*, vol. 71, no. 6, pp. 4342–4373, 2025.

[25] R. K. Mallik and R. D. Murch, "Rayleigh fading channel capacity for coherent signaling with asymmetric constellations," *IEEE Trans. Commun.*, vol. 70, no. 4, pp. 2342–2357, 2022.

[26] X. He, R. Zhou, Q. Fan, X. Xiao, Y. Yu, and Z. Yan, "Preparing student teachers for professional development: Mentoring generative artificial intelligence (AI) learners in mathematical problem solving," *IEEE Trans. Learn. Technol.*, vol. 18, pp. 458–469, 2025.

[27] A. Cuenca, H. Moncayo, and G. Gavilanez, "Artificial-intelligence-assisted geomagnetic navigation framework," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 61, no. 2, pp. 2477–2490, 2025.

[28] J. C. Ku and S. L. Chen, "The deployment and implementation of cloud platform for remote automatic correction of artificial intelligence models," *IEEE Trans. Ind. Informatics*, vol. 21, no. 4, pp. 3466–3474, 2025.