

Computational Analysis of Secrecy Outage in Energy-Harvesting Multi-Backscatter IoT Networks

Sang Q. NGUYEN¹, Minh-Han H. DO², Lam-Dong HUYNH^{2,1}, Tan N. NGUYEN^{3,*}

¹ Faculty of Telecommunications 2, Posts and Telecommunications Institute of Technology, Ho Chi Minh City, Vietnam

² Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam

³ Advanced Intelligent Technology Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam

*Corresponding author: nguyennhattan@tdtu.edu.vn

Submitted June 19, 2026 / Accepted September 1, 2026 / Online first September 30, 2026

Abstract. This paper studies the secrecy outage performance (SOP) of an energy-harvesting multi-backscatter-device (BD) network in the presence of a passive eavesdropper. A dedicated radio-frequency source illuminates multiple BDs employing power splitting (PS), and the BD with the strongest source-to-BD channel is opportunistically selected for confidential backscatter transmission. Unlike conventional secure backscatter communication models that assume an always-active BD, we explicitly impose a practical circuit-activation constraint requiring the selected BD to harvest sufficient energy before transmission. Consequently, the selected source-to-BD channel jointly determines circuit availability and the strengths of the legitimate and wiretap cascaded links. A tractable analytical framework for the SOP is developed by accounting for activation failure, secrecy-rate outage, opportunistic selection, PS, and Rayleigh fading. Since the activation constraint yields a non-zero lower integration bound, we derive a finite-sum approximation using the binomial expansion and Gaussian–Chebyshev quadrature. We further obtain a high-signal-to-noise-ratio expression that reveals a non-zero secrecy outage floor caused by the proportional scaling of the legitimate and eavesdropping links. Monte Carlo simulations validate the analysis and show that increasing the number of candidate BDs improves secrecy performance, particularly in energy-limited regimes, but with diminishing returns. The results also reveal the trade-off between circuit activation and backscattered-signal strength and quantify the effects of the activation threshold, PS coefficient, and channel conditions on secrecy performance.

Keywords

Energy harvesting, backscatter communication, physical layer security, secrecy outage probability, power splitting

1. Introduction

1.1 Background

The rapid proliferation of the Internet of Things (IoT) is fundamentally reshaping modern wireless communications, with its transformative impact already envisioned in the Cisco Annual Internet Report (2018–2023) [1]. This unprecedented growth is expected to continue in future sixth-generation (6G) networks, where ultra-low latency, massive connectivity, and ubiquitous intelligence will support billions of interconnected devices [2–4]. To enable such large-scale deployments, future IoT networks must simultaneously achieve ultra-low power consumption, high energy efficiency, and sustainable long-term operation [5], [6]. Nevertheless, conventional IoT devices generally rely on active radio-frequency (RF) transceivers and finite-capacity batteries. To alleviate the resulting lifetime and maintenance constraints, energy harvesting (EH) has been extensively investigated as a means of enabling self-sustainable low-power wireless devices, particularly through RF energy harvesting and other ambient energy sources [7–9]. In particular, active RF front-ends require power-hungry components such as RF power amplifiers [10–12], resulting in limited operational lifetime and frequent battery replacement or recharging. These maintenance requirements become increasingly costly and impractical in large-scale IoT deployments, especially for devices deployed in remote, inaccessible, or hazardous environments. Consequently, developing self-sustainable and energy-efficient communication paradigms has become one of the most critical challenges for future IoT and 6G ecosystems.

1.2 Related Works

Backscatter communication (BackCom) has attracted considerable research interest as an energy-efficient transmission paradigm for next-generation IoT networks [13–16]. Instead of generating a dedicated RF waveform through an ac-

tive transmitter, a backscatter device (BD) conveys information by modulating its antenna impedance and reflecting an incident RF signal. This transmission mechanism substantially reduces RF circuit complexity and energy consumption, making BackCom particularly attractive for battery-limited and potentially battery-free IoT applications. Furthermore, continuous advances in BackCom have broadened its application scope across several critical domains, including smart urban infrastructure [17], precision agriculture [18], and healthcare monitoring [19]. Recent studies have further enhanced BackCom networks through the integration of reconfigurable intelligent surfaces, non-orthogonal multiple access (NOMA), interference-aware resource allocation, and learning-based tag-selection techniques [20–24]. Collectively, these developments demonstrate the potential of BackCom to improve coverage, spectral and energy efficiency, multi-user connectivity, and secure transmission.

Despite its ultra-low-power transmission mechanism, a practical BD still requires sufficient energy to support sensing, control, impedance switching, and other circuit operations. EH has therefore become an important enabling technique for sustaining long-term BackCom operation [4,25,26]. EH-enabled wireless systems can obtain energy from dedicated wireless power transmitters or ambient sources such as solar, wind, and electromagnetic radiation [27–29]. Among RF-powered architectures, simultaneous wireless information and power transfer (SWIPT) [30–32] and wireless-powered communication networks (WPCNs) [33], [34] represent two widely investigated paradigms. In SWIPT systems, a common RF transmission supports both information decoding and EH through receiver architectures such as time switching, power splitting (PS), antenna switching, or spatial switching. By contrast, WPCNs typically separate downlink wireless energy transfer from uplink information transmission, using dedicated power stations, power beacons, or hybrid access points to energize the network devices before data transmission. RF-EH is particularly attractive for dense IoT deployments because it is compatible with existing wireless infrastructures and can support autonomous low-power operation [35]. In an EH-enabled BackCom system employing PS, one portion of the incident RF power is allocated to EH, while the remaining portion is used for signal reflection, thereby creating an inherent trade-off between the energy available for circuit activation and the strength of the backscattered information signal.

In addition to energy limitations, the broadcast nature of wireless propagation exposes IoT and BackCom transmissions to potential eavesdropping. Such vulnerabilities may arise across heterogeneous IoT deployments, including low-power wide-area networks and UAV-assisted aerial communication networks [36–39]. Although conventional cryptographic mechanisms can provide confidentiality, their computational complexity and key-management requirements may be burdensome for lightweight BDs. Physical-layer security (PLS) has therefore emerged as a complementary solution that exploits the inherent randomness of wireless

channels, including fading, noise, interference, and path loss, to protect confidential transmission without relying solely on computationally intensive encryption [40–42]. These considerations motivate the investigation of secure BackCom systems under practical EH and hardware constraints.

1.3 Research Gap and Motivation

Existing BackCom studies related to the considered problem can be broadly divided into performance-oriented and security-oriented research directions. The first direction primarily focuses on reliability, detection performance, throughput, and spectral efficiency [43–45]. A partial NOMA-assisted BackCom system for device-to-device networks was investigated in [43], where the outage probability (OP) was derived under Rayleigh fading and different resource-allocation settings. Symbol detection in a multi-channel multi-tag ambient BackCom network under in-phase/quadrature imbalance was studied in [44], including the derivation of the bit error rate and a near-optimal detection threshold. In [45], a backscatter-assisted wireless-powered communication network comprising multiple energy-constrained nodes and a multi-antenna power source was considered. Notably, a device-sensitivity threshold was incorporated into the outage formulation such that communication fails when the incident RF power is insufficient to activate the node. Nevertheless, these studies mainly addressed reliability, detection, or throughput and did not consider passive eavesdropping or secrecy outage performance (SOP). The second research direction incorporates physical-layer security (PLS) into ambient BackCom systems [46–48]. A cognitive ambient BackCom network in the presence of an unlicensed eavesdropper was investigated in [46], where analytical and asymptotic expressions for the outage and intercept probabilities were derived. The outage and intercept performance of a relay-free two-way ambient BackCom system under independent Rayleigh fading was analyzed in [47]. More recently, an EH-enabled ambient BackCom system was considered in [48], where a multi-antenna power beacon supplies energy to the source while simultaneously generating friendly jamming against the eavesdropper. Exact and asymptotic expressions for the outage and intercept probabilities of the source and backscatter signals were derived. Despite these contributions, the secure BackCom systems in [46–48] considered a single BD and did not explicitly model a harvested-energy or circuit-activation threshold governing BD operation. For clarity, the main differences between the proposed work and the most closely related studies are summarized in Tab. 1.

As summarized in Tab. 1, the existing studies address only subsets of the key characteristics considered in this work. The works in [43] and [44] focus on outage or detection performance without jointly considering EH, eavesdropping, and circuit activation. Although [45] incorporates EH, multiple energy-constrained nodes, and a device-sensitivity threshold, secrecy performance is not investigated. Conversely, the secure BackCom frameworks in [46] and [47] account for

Ref.	System Model	EH	Multi-BD	PLS	Activation	Closed-form	Performance metric
[43]	Partial NOMA BackCom	×	×	×	×	✓	OP
[44]	Ambient BackCom	×	✓	×	×	✓	BER
[45]	Wireless-powered BackCom	✓	✓	×	✓	✓	OP, throughput
[46]	Cognitive Ambient BackCom	×	×	✓	×	✓	OP, IP
[47]	Two-way Ambient BackCom	×	×	✓	×	✓	OP, IP
[48]	EH-enabled Ambient BackCom	✓	×	✓	×	✓	OP, IP
This work	EH-enabled multi-BD BackCom	✓	✓	✓	✓	✓	SOP

Abbreviations: BER: bit-error rate; IP: intercept probability.

Tab. 1. Comparison of the proposed work with representative BackCom studies.

eavesdropping but consider a single BD without explicitly incorporating EH or circuit activation. Although [48] jointly considers EH and eavesdropping, it likewise assumes a single BD and does not impose an explicit harvested-energy threshold for BD operation. Therefore, the secrecy performance of an activation-constrained multi-BD BackCom network with opportunistic selection and passive eavesdropping remains insufficiently characterized.

In practice, an energy-harvesting BD can operate only when the available harvested energy is sufficient to activate its sensing, control, and impedance-switching circuits. The common source-to-BD channel therefore determines not only the energy available for circuit operation but also the strengths of the legitimate and eavesdropping backscatter links. Moreover, the activation constraint truncates the feasible operating region of the selected BD, requiring the SOP formulation to jointly account for circuit-activation failure and secrecy-rate outage. Consequently, analytical results developed for always-active or single-BD secure BackCom systems cannot be directly applied to the considered network. To provide meaningful performance comparisons, two idealized benchmark schemes are also considered in the numerical analysis. The first removes only the circuit-activation constraint while retaining the energy-harvesting architecture, whereas the second assumes an externally powered and always-active BD. These benchmarks allow the secrecy-performance loss caused by circuit activation to be distinguished from that resulting from allocating part of the incident RF power to EH.

Against this background, this paper investigates the SOP of an energy-harvesting multi-BD BackCom network in the presence of a passive eavesdropper under non-line-of-sight (NLoS) Rayleigh fading. Unlike the existing studies, the proposed framework jointly accounts for opportunistic multi-BD selection, power splitting (PS), circuit activation, and passive eavesdropping. In particular, it combines the activation-aware modeling considered in [45] with the security-oriented BackCom setting studied in [46–48], while incorporating opportunistic selection among multiple BDs. The main contributions of this work are summarized as follows:

- We first establish an activation-aware secrecy framework for an energy-harvesting multi-BD BackCom network with opportunistic BD selection and passive eavesdropping. The BD with the strongest source-

to-BD channel is selected for confidential backscatter transmission and is permitted to operate only when its harvested energy satisfies a predefined circuit-activation requirement. We explicitly account for the dual role of the selected source-to-BD channel, which determines both the energy available for circuit operation and the strengths of the legitimate and wiretap cascaded backscatter links. This formulation enables the SOP to capture both circuit-activation failure and secrecy-rate outage within a unified analytical framework.

- We then derive the order-statistical distribution of the selected source-to-BD channel and use it to formulate the activation-constrained SOP. We show that the circuit-activation condition truncates the feasible operating region of the selected channel, resulting in an integral with a non-zero lower bound for which conventional identities defined over $[0, \infty)$ cannot be directly applied. To overcome this analytical difficulty, we develop a computationally efficient finite-sum approximation based on Gaussian–Chebyshev quadrature (GCQ). We further derive a high-signal-to-noise-ratio (SNR) characterization showing that the activation-failure probability vanishes as the transmit power increases, whereas the SOP approaches a non-zero floor because the legitimate and eavesdropping backscatter links scale proportionally under the considered architecture.
- We finally introduce two physically interpretable benchmark schemes to separately quantify the secrecy-performance losses caused by circuit activation and the allocation of incident RF power to EH. We validate the analytical, approximate, and asymptotic results through Monte Carlo simulations and use the resulting comparisons to reveal the fundamental PS trade-off between circuit availability and backscattered-signal strength. We also quantify the performance improvement and diminishing returns obtained by increasing the number of candidate BDs and characterize the effects of the activation requirement and the relative qualities of the legitimate and eavesdropping channels on the SOP.

The remainder of this paper is organized as follows. Section 2 presents the considered secure energy-harvesting multi-BD BackCom system and its signal model. Section 3 characterizes the relevant channel distributions and derives

the GCQ-based SOP approximation and high-SNR results. Section 4 validates the analysis through Monte Carlo simulations and discusses the effects of key system parameters and the considered benchmark cases. Finally, Section 5 concludes the paper and outlines potential directions for future research.

2. System Model

We consider a secure energy-harvesting BackCom network consisting of a dedicated RF source (S), a cluster of N BDs, denoted by BD_k for $k = 1, \dots, N$, a legitimate destination (D), and a passive eavesdropper (E), as illustrated in Fig. 1. The RF source is equipped with a continuous-wave generator and continuously broadcasts an unmodulated carrier signal with a constant transmit power P_S . To enhance the harvested energy and increase the probability of successful circuit activation, an opportunistic suboptimal backscatter selection (SBS) scheme is adopted. Specifically, a central controller selects the BD with the strongest source-to-BD channel gain, i.e., the largest instantaneous $|h_{\text{SB},k}|^2$, for information transmission. It is worth noting that this selection criterion relies solely on the source-to-BD channel and therefore is sub-optimal from the secrecy perspective, since the instantaneous BD-to-destination and BD-to-eavesdropper channel conditions are not involved in the selection process. Owing to the broadcast nature of wireless propagation, the backscattered signal intended for the legitimate destination can also be overheard by the passive eavesdropper, giving rise to potential secrecy outages.

All wireless links are assumed to experience independent and identically distributed (i.i.d.) quasi-static Rayleigh flat fading. Let $h_{\text{SB},k}$ denote the baseband equivalent channel coefficient from S to the k th BD, where $h_{\text{SB},k} \sim \mathcal{CN}(0, \lambda_{\text{SB}}^{-1})$. Accordingly, the corresponding channel power gain $|h_{\text{SB},k}|^2$ is exponentially distributed with rate parameter λ_{SB} , and mean $\mathbb{E}\{|h_{\text{SB},k}|^2\} = 1/\lambda_{\text{SB}}$. Under the proposed opportunistic BD-selection policy, we define the effective source-to-selected-BD channel power gain as:

$$|h_{\text{SB}}|^2 = \max_{k \in \{1, \dots, N\}} |h_{\text{SB},k}|^2. \quad (1)$$

Similarly, $h_{\text{BD}} \sim \mathcal{CN}(0, \lambda_{\text{BD}}^{-1})$ and $h_{\text{BE}} \sim \mathcal{CN}(0, \lambda_{\text{BE}}^{-1})$. Hence, $|h_{\text{BD}}|^2$ and $|h_{\text{BE}}|^2$ are exponentially distributed with rate parameters λ_{BD} and λ_{BE} , respectively.

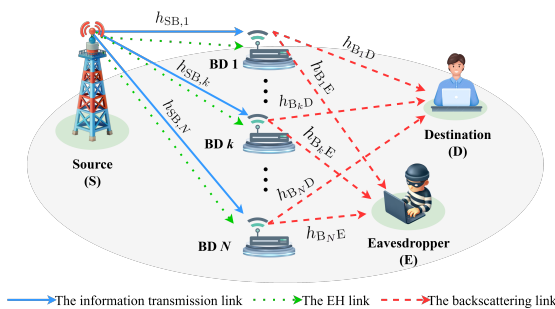


Fig. 1. System model of the secure BackCom system.

At the selected BD, a PS architecture is adopted to coordinate the EH and information backscattering processes. Let $\beta \in (0, 1)$ represent the PS factor. During a given transmission block of duration T , a fraction $(1 - \beta)$ of the incident RF signal power is directed to the EH circuitry, while the remaining portion β is reflected toward the destination D to carry the BD's confidential information. Following the linear EH model adopted in [49], we adopt the following harvested-energy expression for the selected BD:

$$E_h = (1 - \beta)P_S|h_{\text{SB}}|^2T. \quad (2)$$

Based on (2), the selected BD is activated only when

$$E_h \geq E_{\text{th}} \iff (1 - \beta)P_S|h_{\text{SB}}|^2T \geq E_{\text{th}} \quad (3)$$

which can be equivalently expressed as

$$\gamma_{\text{SB}} \geq \xi = \frac{E_{\text{th}}}{(1 - \beta)P_S T} = \frac{\Phi_{\text{th}}}{(1 - \beta)\Psi} \quad (4)$$

where $\gamma_{\text{SB}} \triangleq |h_{\text{SB}}|^2$ denotes the channel power gain of the S-BD link. Here, ξ represents the equivalent channel gain threshold required for circuit activation, $\Psi \triangleq P_S/N_0$, and $\Phi_{\text{th}} \triangleq E_{\text{th}}/(N_0T)$, with N_0 denoting the noise power spectral density.

Based on the standard baseband BackCom signal model in [50], we adapt the received-signal expressions to the considered PS-based architecture. The signal received at the legitimate destination is

$$y_D = \sqrt{P_S\beta} h_{\text{SB}} h_{\text{BD}} x_S c_B + n_D \quad (5)$$

where x_S denotes the source signal, c_B is the reflection coefficient of the BD satisfying $|c_B|^2 = 1$, and $n_D \sim \mathcal{CN}(0, N_0)$ is the additive white Gaussian noise (AWGN) at D .

Similarly, the signal received at the eavesdropper is

$$y_E = \sqrt{P_S\beta} h_{\text{SB}} h_{\text{BE}} x_S c_B + n_E \quad (6)$$

where $n_E \sim \mathcal{CN}(0, N_0)$ denotes the AWGN at E .

From (5) and (6), we derive the instantaneous SNRs at D and E as

$$\gamma_D = \Psi\beta|h_{\text{SB}}|^2|h_{\text{BD}}|^2, \quad (7)$$

and

$$\gamma_E = \Psi\beta|h_{\text{SB}}|^2|h_{\text{BE}}|^2. \quad (8)$$

3. Performance Analysis

3.1 Statistical Characterization of the Channels

To maximize the EH and backscattering efficiency, the selection combining (SC) scheme is employed at the source-to-BD link. Specifically, the BD with the strongest channel from the source is selected, i.e., $|h_{\text{SB}}|^2 = \max_{k=1, \dots, N} |h_{\text{SB},k}|^2$. Let $\gamma_{\text{BD}} \triangleq |h_{\text{BD}}|^2$, and $\gamma_{\text{BE}} \triangleq |h_{\text{BE}}|^2$ denote the channel power gains of the BD-D, and BD-E links,

respectively. The cumulative distribution function (CDF) of the selected channel γ_{SB} is given by:

$$\begin{aligned} F_{\gamma_{\text{SB}}}(x) &= \Pr\left(\max_k \{|h_{\text{SB}_k}|^2\} < x\right) \\ &= \prod_{k=1}^N \Pr(|h_{\text{SB}_k}|^2 < x) \\ &= (1 - \exp(-\lambda_{\text{SB}}x))^N \end{aligned} \quad (9)$$

where λ_{SB} is the rate parameter of the exponential distribution for the S-BD link. By applying the binomial theorem $(a + b)^N = \sum_{n=0}^N \binom{N}{n} a^{N-n} b^n$, with $a = 1$ and $b = -\exp(-\lambda_{\text{SB}}x)$, the CDF in (9) can be expanded as [51]:

$$F_{\gamma_{\text{SB}}}(x) = 1 + \sum_{n=1}^N \binom{N}{n} (-1)^n \exp(-n\lambda_{\text{SB}}x). \quad (10)$$

The probability density function (PDF) of γ_{SB} is obtained by taking the derivative of (10) with respect to x :

$$f_{\gamma_{\text{SB}}}(x) = \frac{\partial F_{\gamma_{\text{SB}}}(x)}{\partial x} = \sum_{n=1}^N \binom{N}{n} (-1)^{n+1} n \lambda_{\text{SB}} \exp(-n\lambda_{\text{SB}}x). \quad (11)$$

3.2 Secrecy Outage Probability Analysis

Following the standard definition of secrecy capacity in [52], we have $C_{\text{sec}} = [C_{\text{D}} - C_{\text{E}}]^+$, where $C_{\text{D}} = \log_2(1 + \gamma_{\text{D}})$ and $C_{\text{E}} = \log_2(1 + \gamma_{\text{E}})$. By additionally accounting for circuit-activation failure, the SOP of the proposed system can be formulated as follows.

Due to the EH constraint, if the harvested energy is insufficient (i.e., $(1 - \beta)P_{\text{S}}\gamma_{\text{SB}}T < E_{\text{th}}$), the BD remains inactive, and no information is transmitted. In this scenario, the secrecy capacity is zero, which leads to a secrecy outage event if the target secrecy rate $C_{\text{th}} > 0$. Therefore, the SOP is formulated as the probability that the secrecy capacity falls below the threshold C_{th} or the BD fails to activate:

$$\begin{aligned} \text{SOP} &= \Pr(C_{\text{sec}} < C_{\text{th}}, \gamma_{\text{SB}} \geq \xi) + \Pr(\gamma_{\text{SB}} < \xi) \\ &= \Pr\left(\frac{1 + \gamma_{\text{D}}}{1 + \gamma_{\text{E}}} < 2^{C_{\text{th}}}, \gamma_{\text{SB}} \geq \xi\right) + \Pr(\gamma_{\text{SB}} < \xi). \end{aligned} \quad (12)$$

Let $\gamma_{\text{th}} = 2^{C_{\text{th}}}$ and $\tilde{\gamma}_{\text{th}} = \gamma_{\text{th}} - 1$. The SOP can be rewritten as

$$\begin{aligned} \text{SOP} &= \Pr\left(\frac{1 + \gamma_{\text{D}}}{1 + \gamma_{\text{E}}} < \gamma_{\text{th}}, \gamma_{\text{SB}} \geq \xi\right) + \Pr(\gamma_{\text{SB}} < \xi) \\ &= \Pr(1 + \gamma_{\text{D}} < \gamma_{\text{th}} + \gamma_{\text{th}}\gamma_{\text{E}}, \gamma_{\text{SB}} \geq \xi) + \Pr(\gamma_{\text{SB}} < \xi) \\ &= \underbrace{\Pr(\gamma_{\text{D}} < \tilde{\gamma}_{\text{th}} + \gamma_{\text{th}}\gamma_{\text{E}}, \gamma_{\text{SB}} \geq \xi)}_{\mathcal{P}_1} + \underbrace{\Pr(\gamma_{\text{SB}} < \xi)}_{\mathcal{P}_2}. \end{aligned} \quad (13)$$

Substituting (7) and (8) into $\mathcal{P}_1$ in (13), we obtain

$$\mathcal{P}_1 = \int_{\xi}^{\infty} \Pr\left(\gamma_{\text{BD}} < \frac{\tilde{\gamma}_{\text{th}}}{\Psi\beta x} + \gamma_{\text{th}}\gamma_{\text{BE}}\right) f_{\gamma_{\text{SB}}}(x) dx. \quad (14)$$

Conditioning on $\gamma_{\text{SB}} = x$ and $\gamma_{\text{BE}} = z$, the secrecy-outage event in (14) occurs when $\gamma_{\text{BD}} < \frac{\tilde{\gamma}_{\text{th}}}{\Psi\beta x} + \gamma_{\text{th}}z$. Since γ_{BD} and γ_{BE} are independent exponentially distributed random variables with $F_{\gamma_{\text{BD}}}(u) = 1 - \exp(-\lambda_{\text{BD}}u)$ and $f_{\gamma_{\text{BE}}}(z) = \lambda_{\text{BE}} \exp(-\lambda_{\text{BE}}z)$, respectively, averaging the conditional OP over γ_{BE} yields

$$\begin{aligned} \mathcal{I}(x) &= \int_0^{\infty} F_{\gamma_{\text{BD}}}\left(\frac{\tilde{\gamma}_{\text{th}}}{\Psi\beta x} + \gamma_{\text{th}}z\right) f_{\gamma_{\text{BE}}}(z) dz \\ &= \int_0^{\infty} \left[1 - \exp\left(-\lambda_{\text{BD}}\left(\frac{\tilde{\gamma}_{\text{th}}}{\Psi\beta x} + \gamma_{\text{th}}z\right)\right)\right] \lambda_{\text{BE}} \exp(-\lambda_{\text{BE}}z) dz \\ &= 1 - \lambda_{\text{BE}} \exp\left(-\frac{\lambda_{\text{BD}}\tilde{\gamma}_{\text{th}}}{\Psi\beta x}\right) \int_0^{\infty} \exp[-(\lambda_{\text{BE}} + \lambda_{\text{BD}}\gamma_{\text{th}})z] dz \\ &= 1 - \frac{\lambda_{\text{BE}}}{\lambda_{\text{BD}}\gamma_{\text{th}} + \lambda_{\text{BE}}} \exp\left(-\frac{\lambda_{\text{BD}}\tilde{\gamma}_{\text{th}}}{\Psi\beta x}\right). \end{aligned} \quad (15)$$

Substituting (15) back into (14) and combining with $\mathcal{P}_2 = \int_0^{\xi} f_{\gamma_{\text{SB}}}(x) dx$, the total SOP is expressed as:

$$\begin{aligned} \text{SOP} &= \int_{\xi}^{\infty} \left(1 - \frac{\lambda_{\text{BE}}}{\lambda_{\text{BD}}\gamma_{\text{th}} + \lambda_{\text{BE}}} \exp\left(-\lambda_{\text{BD}}\frac{\tilde{\gamma}_{\text{th}}}{\Psi\beta x}\right)\right) f_{\gamma_{\text{SB}}}(x) dx \\ &\quad + \Pr(X < \xi) \\ &= \int_{\xi}^{\infty} f_{\gamma_{\text{SB}}}(x) dx \\ &\quad - \frac{\lambda_{\text{BE}}}{\lambda_{\text{BD}}\gamma_{\text{th}} + \lambda_{\text{BE}}} \int_{\xi}^{\infty} \exp\left(-\lambda_{\text{BD}}\frac{\tilde{\gamma}_{\text{th}}}{\Psi\beta x}\right) f_{\gamma_{\text{SB}}}(x) dx \\ &\quad + \int_0^{\xi} f_{\gamma_{\text{SB}}}(x) dx \\ &= \left(\int_{\xi}^{\infty} f_{\gamma_{\text{SB}}}(x) dx + \int_0^{\xi} f_{\gamma_{\text{SB}}}(x) dx\right) \\ &\quad - \frac{\lambda_{\text{BE}}}{\lambda_{\text{BD}}\gamma_{\text{th}} + \lambda_{\text{BE}}} \sum_{n=1}^N \binom{N}{n} (-1)^{n+1} n \lambda_{\text{SB}} \\ &\quad \times \int_{\xi}^{\infty} \exp\left(-\lambda_{\text{BD}}\frac{\tilde{\gamma}_{\text{th}}}{\Psi\beta x}\right) \exp(-n\lambda_{\text{SB}}x) dx \\ &= 1 - \frac{\lambda_{\text{BE}}}{\lambda_{\text{BD}}\gamma_{\text{th}} + \lambda_{\text{BE}}} \sum_{n=1}^N \binom{N}{n} (-1)^{n+1} n \lambda_{\text{SB}} \\ &\quad \times \int_{\xi}^{\infty} \exp\left(-\lambda_{\text{BD}}\frac{\tilde{\gamma}_{\text{th}}}{\Psi\beta x}\right) \exp(-n\lambda_{\text{SB}}x) dx. \end{aligned} \quad (16)$$

To facilitate the analysis, we first evaluate the second term ($\mathcal{I}_2$). Specifically, we define:

$$\mathcal{I}_2 = \int_{\xi}^{\infty} \exp\left(-\lambda_{BD} \frac{\tilde{\gamma}_{th}}{\Psi\beta x} - n\lambda_{SB}x\right) dx. \quad (17)$$

The integral $\mathcal{I}_2$ in (17) contains an integrand of the form $\exp(-A/x - Bx)$ over the interval $[\xi, \infty)$, where $\xi > 0$. Although the corresponding complete integral over $[0, \infty)$ can be represented in terms of a modified Bessel function [53], the non-zero lower bound introduced by the circuit-activation constraint prevents the direct application of that identity. Therefore, a tractable approximation is obtained using the GCQ method.

To map the semi-infinite interval $[\xi, \infty)$ onto the finite interval $[-1, 1]$, we introduce the transformation $x = \xi + \tan\left(\frac{(\tau+1)\pi}{4}\right)$, $-1 \leq \tau \leq 1$, whose Jacobian is $dx = \frac{\pi}{4} \sec^2\left(\frac{(\tau+1)\pi}{4}\right) d\tau$.

Consequently, $\mathcal{I}_2$ can be rewritten as

$$\mathcal{I}_2 = \frac{\pi}{4} \int_{-1}^1 \left\{ \exp\left(-\frac{\lambda_{BD}\tilde{\gamma}_{th}}{\Psi\beta x(\tau)} - n\lambda_{SB}x(\tau)\right) \times \sec^2\left(\frac{(\tau+1)\pi}{4}\right) \right\} d\tau \quad (18)$$

where $x(\tau) = \xi + \tan\left(\frac{(\tau+1)\pi}{4}\right)$.

To apply the first-kind GCQ rule, the above integral is expressed in the weighted form $\int_{-1}^1 f(\tau) d\tau = \int_{-1}^1 \frac{\sqrt{1-\tau^2}f(\tau)}{\sqrt{1-\tau^2}} d\tau$. Using $\int_{-1}^1 \frac{g(\tau)}{\sqrt{1-\tau^2}} d\tau \approx \frac{\pi}{M} \sum_{m=1}^M g(\tau_m)$ where $\tau_m = \cos\left(\frac{2m-1}{2M}\pi\right)$ as [54], we obtain

$$\mathcal{I}_2 \approx \frac{\pi^2}{4M} \sum_{m=1}^M W_m \exp\left(-\frac{\lambda_{BD}\tilde{\gamma}_{th}}{\Psi\beta x_m} - n\lambda_{SB}x_m\right) \quad (19)$$

where

$$x_m = \xi + \tan\left(\frac{(\tau_m+1)\pi}{4}\right), W_m = \sqrt{1-\tau_m^2} \sec^2\left(\frac{(\tau_m+1)\pi}{4}\right).$$

Here, M denotes the number of quadrature nodes and controls the trade-off between computational complexity and approximation accuracy. Substituting (19) into (16) yields the tractable GCQ-based approximation of the SOP stated in Proposition 1.

Proposition 1. *Based on the preceding derivation, the SOP of the proposed backscatter system can be approximated by*

$$\begin{aligned} \text{SOP} \approx & 1 - \frac{\lambda_{BE}}{\lambda_{BD}\gamma_{th} + \lambda_{BE}} \sum_{n=1}^N \binom{N}{n} (-1)^{n+1} n\lambda_{SB} \\ & \times \left[\frac{\pi^2}{4M} \sum_{m=1}^M W_m \exp\left(-\frac{\lambda_{BD}\tilde{\gamma}_{th}}{\Psi\beta x_m} - n\lambda_{SB}x_m\right) \right] \end{aligned} \quad (20)$$

where M is the number of quadrature nodes, and the definitions of W_m, x_m follow the standard GCQ rules as described previously.

The proof follows directly from substituting the integral representation in the exact SOP expression with its GCQ summation form.

3.3 Asymptotic Analysis

To gain further insight into the high-SNR behavior of the considered system, we derive the asymptotic expression of the SOP when $\Psi \rightarrow \infty$.

From (13), the term $\mathcal{P}_1$ can be rewritten as

$$\begin{aligned} \mathcal{P}_1 &= \Pr(\Psi\beta\gamma_{SB}\gamma_{BD} < \tilde{\gamma}_{th} + \gamma_{th}\Psi\beta\gamma_{SB}\gamma_{BE}, \gamma_{SB} \geq \xi) \\ &= \int_{\xi}^{\infty} \int_0^{\infty} F_{\gamma_{BD}}\left(\gamma_{th}y + \frac{\tilde{\gamma}_{th}}{\Psi\beta x}\right) f_{\gamma_{BE}}(y) f_{\gamma_{SB}}(x) dy dx \end{aligned} \quad (21)$$

where $F_{\gamma_{BD}}(z) = 1 - \exp(-\lambda_{BD}z)$ and $f_{\gamma_{BE}}(y) = \lambda_{BE} \exp(-\lambda_{BE}y)$.

Substituting these distributions into the above expression and solving the inner integral over y , we obtain

$$\mathcal{P}_1 = \int_{\xi}^{\infty} \left[1 - \frac{\lambda_{BE}}{\lambda_{BE} + \gamma_{th}\lambda_{BD}} \exp\left(-\frac{\lambda_{BD}\tilde{\gamma}_{th}}{\Psi\beta x}\right) \right] f_{\gamma_{SB}}(x) dx. \quad (22)$$

Therefore, the SOP can be expressed as

$$\text{SOP} = 1 - \frac{\lambda_{BE}}{\lambda_{BE} + \gamma_{th}\lambda_{BD}} \int_{\xi}^{\infty} \exp\left(-\frac{\lambda_{BD}\tilde{\gamma}_{th}}{\Psi\beta x}\right) f_{\gamma_{SB}}(x) dx. \quad (23)$$

Using the standard first-order Taylor expansion in [55], the exponential term can be approximated in the high-SNR regime as

$$\exp\left(-\frac{\lambda_{BD}\tilde{\gamma}_{th}}{\Psi\beta x}\right) \approx 1 - \frac{\lambda_{BD}\tilde{\gamma}_{th}}{\Psi\beta x}. \quad (24)$$

Substituting this standard approximation into the authors' SOP expression in (23), we obtain

$$\begin{aligned} \text{SOP}^{\infty} &\approx 1 - \frac{\lambda_{BE}}{\lambda_{BE} + \gamma_{th}\lambda_{BD}} \int_{\xi}^{\infty} \left(1 - \frac{\lambda_{BD}\tilde{\gamma}_{th}}{\Psi\beta x} \right) f_{\gamma_{SB}}(x) dx \\ &= 1 - \frac{\lambda_{BE}}{\lambda_{BE} + \gamma_{th}\lambda_{BD}} (1 - F_{\gamma_{SB}}(\xi)) \\ &\quad + \frac{\lambda_{BE}\lambda_{BD}\tilde{\gamma}_{th}}{(\lambda_{BE} + \gamma_{th}\lambda_{BD})\Psi\beta} \int_{\xi}^{\infty} \frac{f_{\gamma_{SB}}(x)}{x} dx. \end{aligned} \quad (25)$$

Using the PDF of γ_{SB} , we further obtain

$$\int_{\xi}^{\infty} \frac{f_{\gamma_{SB}}(x)}{x} dx = \sum_{n=1}^N \binom{N}{n} (-1)^{n+1} n\lambda_{SB} E_1(n\lambda_{SB}\xi) \quad (26)$$

where $E_1(\cdot)$ denotes the standard exponential integral function [55], defined by

$$E_1(z) = \int_z^{\infty} \frac{\exp(-t)}{t} dt. \quad (27)$$

Hence, the asymptotic SOP is finally given by

$$\begin{aligned} \text{SOP}^{\infty} &\approx 1 - \frac{\lambda_{\text{BE}}}{\lambda_{\text{BE}} + \gamma_{\text{th}}\lambda_{\text{BD}}} (1 - F_{\gamma_{\text{SB}}}(\xi)) \\ &+ \frac{\lambda_{\text{BE}}\lambda_{\text{BD}}\tilde{\gamma}_{\text{th}}}{(\lambda_{\text{BE}} + \gamma_{\text{th}}\lambda_{\text{BD}})\Psi\beta} \times \sum_{n=1}^N \binom{N}{n} (-1)^{n+1} n \lambda_{\text{SB}} E_1(n\lambda_{\text{SB}}\xi). \end{aligned} \quad (28)$$

Moreover, it is worth noting that the equivalent activation threshold $\xi = \frac{\Phi_{\text{th}}}{(1-\beta)\Psi}$ is inversely proportional to the transmit SNR. Therefore, as $\Psi \rightarrow \infty$, we have $\xi \rightarrow 0$. Consequently, the activation-OP

$$\mathcal{P}_2 = \Pr(\gamma_{\text{SB}} < \xi) = F_{\gamma_{\text{SB}}}(\xi) \rightarrow 0 \quad (29)$$

which indicates that the selected BD is almost surely activated in the high-SNR regime. Hence, the activation constraint becomes asymptotically inactive, and the secrecy outage is dominated solely by the successful-activation event represented by $\mathcal{P}_1$.

Furthermore, since $F_{\gamma_{\text{SB}}}(\xi) \rightarrow 0$ and the second term in (28) is proportional to $1/\Psi$, which also vanishes as $\Psi \rightarrow \infty$, the asymptotic SOP converges to the following non-zero secrecy outage floor:

$$\text{SOP}^{\infty} = \frac{\gamma_{\text{th}}\lambda_{\text{BD}}}{\lambda_{\text{BE}} + \gamma_{\text{th}}\lambda_{\text{BD}}}. \quad (30)$$

This result indicates that increasing the transmit SNR cannot completely eliminate secrecy outage, since both the legitimate and eavesdropping links scale proportionally with Ψ_{SB} .

4. Numerical Results and Discussion

In this section, numerical results are presented to validate the derived analytical expressions and investigate the effects of the key system parameters on the secrecy performance. All numerical evaluations were implemented in MATLAB, and no physical hardware testbed was employed because this study is based on mathematical analysis and Monte Carlo simulations. All Monte Carlo results are averaged over 10^6 independent channel realizations, and $M = 100$ quadrature nodes are consistently employed in the GCQ-based evaluation. Unless otherwise specified, the common simulation parameters are summarized in Tab. 2.

Parameter	Symbol	Value
Number of BDs	N	1,2,4
PS coefficient	β	0.5
Target secrecy rate	C_{th}	{0.25, 0.5, 1} bps/Hz
Number of GCQ samples	M	100
Channel parameter (S to BD)	λ_{SB}	{0.5, 1, 2}
Channel parameter (BD to D)	λ_{BD}	{0.5, 1}
Channel parameter (BD to E)	λ_{BE}	{1, 1.5}
EH activation threshold	Φ_{th}	{-5, 0, 1, 2} dB

Tab. 2. Simulation parameters.

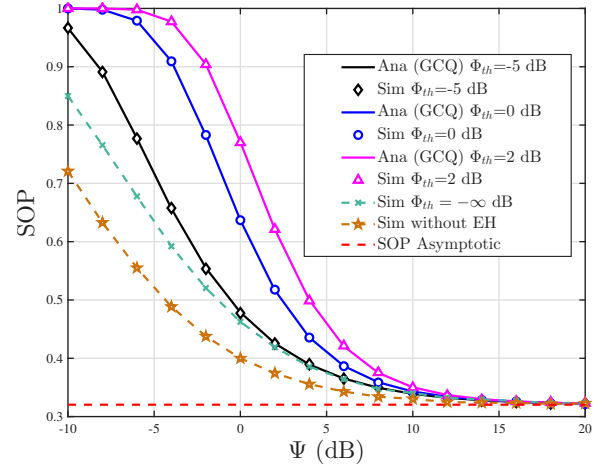


Fig. 2. SOP versus the transmit SNR Ψ for different finite energy-activation thresholds, the $E_{\text{th}} = 0$, and the ideal without-EH benchmark.

The baseline parameter values are selected to represent favorable, moderate, and adverse operating conditions while enabling the individual effect of each parameter to be clearly isolated. Parameters varied in a particular experiment are explicitly stated in the corresponding figure discussion. Across all considered cases, the analytical curves and Monte Carlo simulation markers are generated independently and closely agree with each other. Although they appear to overlap at the plotting resolution, the remaining numerical discrepancies are negligible, indicating that both the GCQ-based evaluation and the Monte Carlo simulations have sufficiently converged and thereby confirming the accuracy of the proposed analytical framework.

Figure 2 illustrates the SOP versus the transmit SNR Ψ for different normalized circuit-activation thresholds, $\Phi_{\text{th}} \in \{-5, 0, 2\}$ dB, together with two benchmark schemes, namely the $E_{\text{th}} = 0$ case and the ideal without-EH case. The considered SNR range from -10 to 20 dB spans the energy-limited, transition, and high-SNR operating regions, while the selected threshold values represent relatively low, moderate, and stringent activation requirements for passive BDs. As expected, the SOP decreases monotonically with increasing Ψ because a higher transmit SNR not only enhances the received backscatter signal quality but also increases the probability that the harvested energy exceeds the circuit-activation threshold. In contrast, increasing Φ_{th} degrades the secrecy performance by making circuit activation more difficult, thereby increasing the probability that the selected BD remains inactive. Consequently, the case $\Phi_{\text{th}} = 2$ dB exhibits the highest SOP, whereas $\Phi_{\text{th}} = -5$ dB achieves the best secrecy performance among the practical finite-threshold scenarios. The two benchmark schemes further reveal the impact of practical energy constraints. Specifically, the $E_{\text{th}} = 0$ benchmark removes only the circuit-activation requirement while preserving the EH process, corresponding to the commonly adopted assumption that the selected BD is always active. Therefore, the performance gap between this benchmark and the proposed finite-threshold cases directly quantifies the secrecy degradation caused by the activation-energy

constraint. In contrast, the ideal without-EH benchmark eliminates both the EH process and the associated power allocation for EH, thereby providing an upper performance bound and yielding the lowest SOP over almost the entire SNR range. These comparisons clearly demonstrate that both the activation-energy requirement and the EH process contribute to secrecy-performance degradation, with the activation constraint having a particularly noticeable impact in the low- and moderate-SNR regions. As the transmit SNR continues to increase, the SOP curves gradually converge toward the same non-zero secrecy outage floor predicted by (30). This behavior arises because both the legitimate and eavesdropping SNRs scale proportionally with the transmit power in the high-SNR regime, causing the influence of noise and activation constraints to become negligible. Consequently, further increasing the transmit power beyond the onset of the secrecy floor provides only marginal secrecy improvement, whereas reducing the activation threshold or improving the harvested energy efficiency is considerably more beneficial in the practical low- and moderate-SNR operating regions.

Following the transmit-SNR and activation-threshold analysis in Fig. 2, Figure 3 further investigates the impact of the PS coefficient β on the SOP for $\Psi \in \{5, 10, 15\}$ dB. The PS coefficient is varied from 0.05 to 0.95, while the limiting values are excluded since $\beta = 0$ corresponds to no backscatter transmission and $\beta = 1$ allocates all the incident RF power to information reflection, leaving no energy available for circuit activation. The selected SNR values represent low, moderate, and relatively high operating conditions, thereby enabling the dependence of the optimal PS coefficient on the available transmit power to be clearly observed. It can be seen that all curves exhibit a pronounced U-shaped behavior, revealing the inherent trade-off between EH and backscatter information transmission. Specifically, when β is small, a larger portion of the incident RF power is allocated to EH, resulting in a high circuit-activation probability. However, the reflected information signal becomes relatively weak, which degrades the received SNR at the legitimate destination and leads to a relatively high SOP. As β increases, more power is allocated to backscatter transmission, strengthening the reflected signal and improving the secrecy performance. Nevertheless, beyond a certain point, further increasing β significantly reduces the harvested energy, making the activation requirement more difficult to satisfy. Consequently, the probability of activation failure increases, causing the SOP to rise again. This competition between activation reliability and backscatter signal quality gives rise to the observed U-shaped curves and demonstrates the existence of an optimal PS coefficient. Moreover, increasing the transmit SNR consistently reduces the SOP over the entire range of β and shifts the optimal PS coefficient toward a larger value. This behavior can be explained by the fact that a stronger incident RF signal enables the BD to harvest sufficient energy even when a larger fraction of the received power is allocated to backscatter transmission. Therefore, at higher SNRs, more power can be devoted to information reflection without violating the circuit-activation constraint.

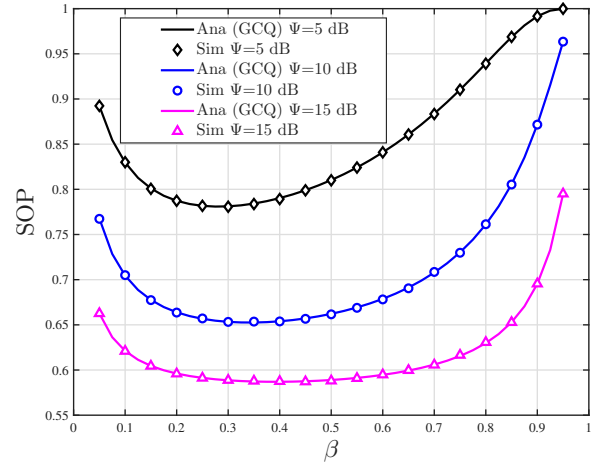


Fig. 3. SOP versus the PS coefficient β for different transmit SNRs Ψ .

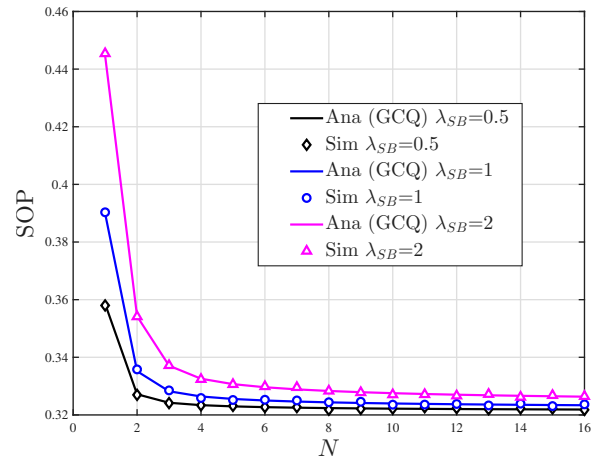


Fig. 4. SOP versus the number of BDs N for different channel parameters λ_{SB} .

These observations suggest that the PS coefficient should be adaptively optimized according to the operating SNR in order to effectively balance EH and confidential backscatter transmission while minimizing the SOP.

Having established the EH-backscatter power-allocation trade-off in Fig. 3, Figure 4 investigates the secrecy gain provided by opportunistic multi-BD selection by varying the number of candidate BDs from $N = 1$ to $N = 16$ for $\lambda_{SB} \in \{0.5, 1, 2\}$. Since the average source-to-BD channel power gain is inversely proportional to λ_{SB} , these values represent favorable, moderate, and adverse source-to-BD propagation conditions, respectively. For every considered λ_{SB} , the SOP decreases as N increases because a larger candidate set improves the probability of selecting a BD with a strong incident channel, which simultaneously enhances its activation probability and effective backscatter transmission. For a fixed N , increasing λ_{SB} produces a higher SOP because the average RF power available for both EH and reflection becomes smaller. The reduction in SOP is particularly pronounced when the number of candidate BDs increases from a small value, whereas the curves gradually flatten as N becomes larger. The range $1 \leq N \leq 16$ is therefore selected to reveal both the initial selection-diversity gain and

its subsequent saturation. These results show that deploying additional candidate BDs can effectively mitigate moderate source-to-BD channel degradation. However, the marginal secrecy improvement becomes limited beyond a certain network size, indicating that, in practical implementations, the additional selection gain should be weighed against the increased coordination and channel-estimation requirements associated with a larger candidate set.

After examining the effects of the source-to-BD link and the number of candidate devices in Fig. 4, Figure 5 evaluates the influence of the legitimate BD-to-destination channel by varying λ_{BD} from 0.5 to 3 for $N \in \{1, 2, 4\}$. The considered channel-parameter range represents propagation conditions from a relatively strong legitimate link to a substantially weakened one, while the selected values of N correspond to single-BD transmission and moderate multi-BD selection diversity. The SOP increases monotonically with λ_{BD} because a larger rate parameter corresponds to a smaller average legitimate channel gain, thereby reducing the received SNR at the destination and making the target secrecy rate more difficult to satisfy. Increasing N shifts all curves downward because a larger candidate set increases the probability of selecting a BD with a stronger source-to-BD channel, thereby improving activation reliability and providing a finite-SNR selection gain. Nevertheless, the separation among the curves becomes insufficient to compensate for severe degradation of the BD-to-destination link when λ_{BD} is large. Therefore, opportunistic multi-BD selection improves secrecy performance but cannot replace the need for a sufficiently reliable legitimate channel, which remains a dominant factor in achieving a low SOP.

Complementing the legitimate-link analysis in Fig. 5, Figure 6 investigates the effect of the eavesdropping channel by varying λ_{BE} from 0.5 to 3 for $N \in \{1, 2, 4\}$. This interval covers conditions ranging from a relatively strong eavesdropping link to a considerably attenuated one because the average BD-to-eavesdropper channel gain is inversely proportional to λ_{BE} . In contrast to the trend observed for λ_{BD} , the SOP decreases monotonically as λ_{BE} increases. A larger λ_{BE} weakens the average wiretap channel, thereby reducing the received SNR and interception capability of the eavesdropper. Increasing N further lowers the SOP over the considered range because a larger candidate set improves the selected source-to-BD channel and consequently increases the BD activation probability. Meanwhile, the statistical distribution of the BD-to-eavesdropper channel remains unchanged. The performance improvement provided by multi-BD selection remains visible even when the eavesdropping link is relatively strong, although the absolute SOP is ultimately determined by the quality difference between the legitimate and wiretap channels. These results demonstrate that opportunistic BD selection and attenuation of the eavesdropping link provide complementary secrecy benefits, suggesting that practical deployments should jointly exploit selection diversity and propagation conditions that reduce the eavesdropper's received signal strength.

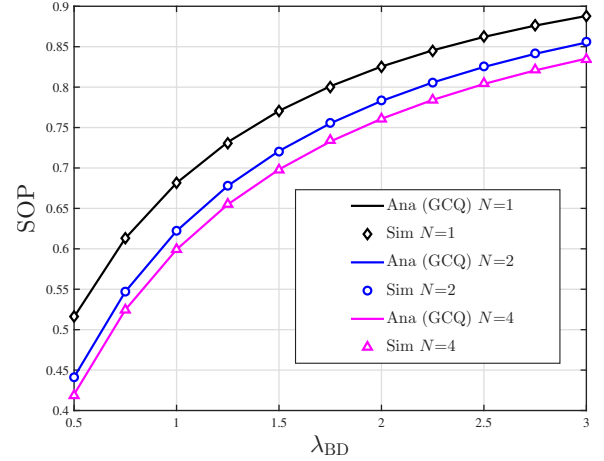


Fig. 5. SOP versus the legitimate channel parameter λ_{BD} for different numbers of BDs N .

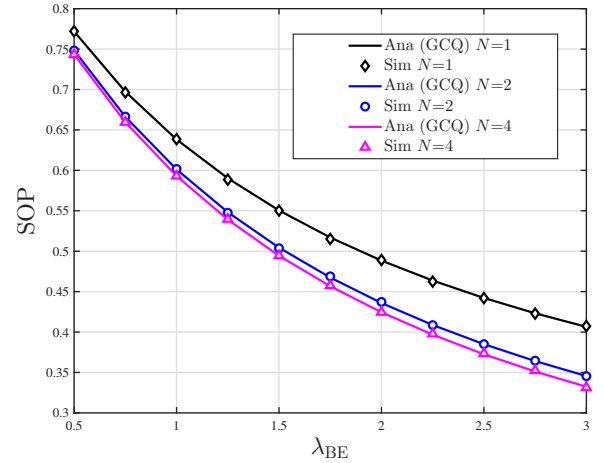


Fig. 6. SOP versus the eavesdropper's channel parameter λ_{BE} for varying numbers of BDs N .

5. Conclusion

In this paper, we investigated the SOP of an energy-harvesting multi-BD BackCom system in the presence of a passive eavesdropper under practical circuit-activation constraints. Unlike most existing studies that assume an always-active BD, the proposed framework explicitly incorporates the energy-harvesting activation condition together with the instantaneous secrecy-rate requirement into the SOP analysis. By exploiting the statistical characteristics of the selected backscatter channel and employing the GCQ technique, a tractable closed-form approximation for the SOP was derived. Furthermore, a high-SNR asymptotic expression was obtained, revealing a non-zero secrecy outage floor and providing valuable insights into the limiting secrecy performance of the considered system. The derived analytical results were verified by extensive Monte Carlo simulations over a wide range of system parameters. The numerical results demonstrated the impacts of the transmit SNR, circuit-activation threshold, PS coefficient, and opportunistic multi-BD selection on the secrecy performance. In particular, a lower activation threshold significantly improves the

SOP in the low- and moderate-SNR regions, while the PS coefficient exhibits an inherent trade-off between EH and confidential backscatter transmission, leading to an optimal operating point. Moreover, although increasing the transmit SNR enhances secrecy performance, the SOP eventually converges to a non-zero floor because both the legitimate and eavesdropping links scale proportionally with the transmit power. These findings provide useful design guidelines for practical energy-constrained secure BackCom-enabled IoT networks. Although the proposed analytical framework provides valuable insights, it is developed under several simplifying assumptions, including a single passive eavesdropper, an idealized RF energy-harvesting model, and Rayleigh fading channels. Future work will extend the proposed framework to more practical scenarios involving multiple eavesdroppers (both colluding and non-colluding), nonlinear RF energy-harvesting models that capture rectifier sensitivity and saturation effects, imperfect channel state information for BD selection, and more general fading environments such as Nakagami- m and Rician channels.

Data Availability

The MATLAB source code used to generate the numerical results presented in this paper is publicly available at: <https://github.com/dohoangminhhan2005/matlab-code-paper-2026>.

Acknowledgments

This research is supported by Posts and Telecommunications Institute of Technology (PTIT).

References

- [1] CISCO. *Cisco Annual Internet Report (2018–2023)*. White Paper, San Jose (CA, USA): Cisco, 2020.
- [2] KAUSHIK, A., SINGH, R., DAYARATHNA, S., et al. Toward integrated sensing and communications for 6G: Key enabling technologies, standardization, and challenges. *IEEE Communications Standards Magazine*, 2024, vol. 8, no. 2, p. 52–59. DOI: 10.1109/MCOMSTD.0007.2300043
- [3] ALMOMANI, A., AL-TURJMAN, F. Challenges and opportunities in integrated 6G and IoT paradigms: An overview. In *International Conference on Artificial Intelligence in Everything (AIE)*. Nicosia (Cyprus), 2022, p. 140–145. DOI: 10.1109/AIE57029.2022.00033
- [4] DUY, T. T., NHAT, N. L., HANH, T., et al. On the performance of the coverage probability of LoRa networks with non-linear energy harvesting. In *Proceedings of the International Conference on Advanced Technologies for Communications (ATC)*. Ho Chi Minh City (Vietnam), 2024, p. 722–726. DOI: 10.1109/ATC63255.2024.10908157
- [5] ROSABAL, O. M., ALCARAZ LOPEZ, O. L., ALVES, H., et al. Sustainable RF wireless energy transfer for massive IoT: Enablers and challenges. *IEEE Access*, 2023, vol. 11, p. 133979–133992. DOI: 10.1109/ACCESS.2023.3337214
- [6] NGUYEN, T. P., VO, D. T., VU, Q.-S., et al. RIS-aided multi-antenna IoT systems: Performance evaluation under MRC combining. *Advances in Electrical and Electronic Engineering*, 2025, vol. 23, no. 3, p. 227–236. DOI: 10.15598/aece.v23i3.250801
- [7] LU, X., WANG, P., NIYATO, D., et al. Wireless networks with RF energy harvesting: A contemporary survey. *IEEE Communications Surveys & Tutorials*, 2015, vol. 17, no. 2, p. 757–789. DOI: 10.1109/COMST.2014.2368999
- [8] VINKO, D. Applicability of Dickson charge pump in energy harvesting systems: Experimental validation of energy harvesting charge pump model. *Radioengineering*, 2018, vol. 27, no. 2, p. 510–518. DOI: 10.13164/re.2018.0510
- [9] LEON AVILA, B. Y., GARCIA VAZQUEZ, C. A., PEREZ BALUJA, O., et al. Energy harvesting techniques for wireless sensor networks: A systematic literature review. *Energy Strategy Reviews*, 2025, vol. 57, p. 1–23. DOI: 10.1016/j.esr.2024.101617
- [10] VAN HUYNH, N., HOANG, D. T., LU, X., et al. Ambient backscatter communications: A contemporary survey. *IEEE Communications Surveys & Tutorials*, 2018, vol. 20, no. 4, p. 2889–2922. DOI: 10.1109/COMST.2018.2841964
- [11] ATANASKOVIC, A., DJORIC, A., MALES ILIC, N., et al. Linearization of the fifth generation power amplifiers by injection of the second order digitally processed signals. *Radioengineering*, 2024, vol. 33, no. 3, p. 339–348. DOI: 10.13164/re.2024.0339
- [12] VARLAMOV, O. V., GROMORUSHKIN, V. N. High efficiency power amplifier for IoT applications: RF path. In *Systems of Signals Generating and Processing in the Field of on Board Communications*. Moscow (Russia), 2020, p. 1–5. DOI: 10.1109/IEEECONF48371.2020.9078651
- [13] SONG, C., DING, Y., EID, A., et al. Advances in wirelessly powered backscatter communications: From antenna/RF circuitry design to printed flexible electronics. *Proceedings of the IEEE*, 2022, vol. 110, no. 1, p. 171–192. DOI: 10.1109/JPROC.2021.3125285
- [14] CORREIA, R., BOAVENTURA, A., CARVALHO, N. B. Quadrature amplitude backscatter modulator for passive wireless sensors in IoT applications. *IEEE Transactions on Microwave Theory and Techniques*, 2017, vol. 65, no. 4, p. 1103–1110. DOI: 10.1109/TMTT.2017.2661262
- [15] DUAN, R., WANG, X., YIGITLER, H., et al. Ambient backscatter communications for future ultra-low-power machine type communications: Challenges, solutions, opportunities, and future research trends. *IEEE Communications Magazine*, 2020, vol. 58, no. 2, p. 42–47. DOI: 10.1109/MCOM.001.1900464
- [16] TORRES, R., CORREIA, R., CARVALHO, N. B., et al. Backscatter communications. *IEEE Journal of Microwaves*, 2021, vol. 1, no. 4, p. 864–878. DOI: 10.1109/JMW.2021.3110058
- [17] WANG, X., KOU, X., LI, H., et al. AllSpark: Enabling long-range backscatter for vehicle-to-infrastructure communication. *IEEE Internet of Things Journal*, 2022, vol. 9, no. 24, p. 25525–25537. DOI: 10.1109/JIOT.2022.3197596
- [18] LIN, K., ALCARAZ LOPEZ, O. L., ALVES, H., et al. Throughput optimization in backscatter-assisted wireless-powered underground sensor networks for smart agriculture. *Internet of Things*, 2022, vol. 20, p. 1–13. DOI: 10.1016/j.iot.2022.100637
- [19] JAMEEL, F., DUAN, R., CHANG, Z., et al. Applications of backscatter communications for healthcare networks. *IEEE Network*, 2019, vol. 33, no. 6, p. 50–57. DOI: 10.1109/MNET.001.1900109
- [20] ALTUWAIRGI, K. H., KHEL, A. M. T., HAMDI, K. A. Energy detection for reflecting surfaces-aided ambient backscatter communications. *IEEE Transactions on Green Communications and Networking*, 2024, vol. 8, no. 1, p. 279–290. DOI: 10.1109/TGCN.2023.3321525

- [21] DING, Z., POOR, H. V. Advantages of NOMA for multi-user BackCom networks. *IEEE Communications Letters*, 2021, vol. 25, no. 10, p. 3408–3412. DOI: 10.1109/LCOMM.2021.3100337
- [22] ASIF, M., IHSAN, A., KHAN, W. U., et al. Energy-efficient beam-forming and resource optimization for AmbSC-assisted cooperative NOMA IoT networks. *IEEE Internet of Things Journal*, 2023, vol. 10, no. 14, p. 12434–12448. DOI: 10.1109/JIOT.2023.3247021
- [23] KHAN, Y., TRIPATHI, S., DUBEY, A., et al. Deep learning-based secure tag selection in BackCom network with RIS-induced interference. *IEEE Journal of Radio Frequency Identification*, 2025, vol. 9, p. 797–806. DOI: 10.1109/JRFID.2025.3611299
- [24] KHAN, W. U., LAGUNAS, E., ALI, Z., et al. Deep reinforcement learning for backscatter communications: Augmenting intelligence in future Internet of Things. *IEEE Internet of Things Magazine*, 2024, vol. 7, no. 5, p. 72–78. DOI: 10.1109/IOTM.001.2400003
- [25] HUNG, T., MINH, B., NGUYEN, T., et al. Power beacon-assisted energy harvesting symbiotic radio networks: Outage performance. *PLOS ONE*, 2025, vol. 20, no. 2, p. 1–16. DOI: 10.1371/journal.pone.0313981
- [26] DASKALAKIS, S. N., ASSIMONIS, S. D., BLETSAS, A. Sensitive and efficient RF harvesting supply for batteryless backscatter sensor networks. *IEEE Transactions on Microwave Theory and Techniques*, 2016, vol. 64, no. 4, p. 1327–1338. DOI: 10.1109/TMTT.2016.2533619
- [27] YANG, H., SHAO, N., WANG, J., et al. Experimental analysis of hybrid multiple-layer piezoelectric-solar energy harvester for self-powered wireless sensing. *Sustainable Energy Technologies and Assessments*, 2025, vol. 73, p. 1–11. DOI: 10.1016/j.seta.2024.104157
- [28] SU, B., GUO, T., ALAM, M. M. A review of wind energy harvesting technology: Civil engineering resource, theory, optimization, and application. *Applied Energy*, 2025, vol. 389, p. 1–35. DOI: 10.1016/j.apenergy.2025.125771
- [29] MURAMATSU, D., AMANO, K. Ambient electromagnetic wave energy harvesting using human body antenna for wearable sensors. *Sensors*, 2025, vol. 25, no. 15, p. 1–18. DOI: 10.3390/s25154689
- [30] QARAGOEZ, Y., POLLIN, S., SCHREURS, D. Frequency division duplex-multitone approach for backscatter aided SWIPT. In *Wireless Power Week (WPW)*. Bordeaux (France), 2022, p. 213–217. DOI: 10.1109/WPW54272.2022.9853856
- [31] KRIKIDIS, I., TIMOTHEOU, S., NIKOLAOU, S., et al. Simultaneous wireless information and power transfer in modern communication systems. *IEEE Communications Magazine*, 2014, vol. 52, no. 11, p. 104–110. DOI: 10.1109/MCOM.2014.6957150
- [32] TIN, P. T., NGUYEN, T. N., TRAN, D. H., et al. Performance enhancement for full-duplex relaying with time switching-based SWIPT in wireless sensors networks. *Sensors*, 2021, vol. 21, no. 11, p. 1–16. DOI: 10.3390/s211113847
- [33] BOSHKOVSKA, E., NG, D. W. K., ZLATANOV, N., et al. Robust resource allocation for MIMO wireless powered communication networks based on a non-linear EH model. *IEEE Transactions on Communications*, 2017, vol. 65, no. 5, p. 1984–1999. DOI: 10.1109/TCOMM.2017.2664860
- [34] MA, Y., CHEN, H., LIN, Z., et al. Distributed and optimal resource allocation for power beacon-assisted wireless-powered communications. *IEEE Transactions on Communications*, 2015, vol. 63, no. 10, p. 3569–3583. DOI: 10.1109/TCOMM.2015.2468215
- [35] KAUR, A., HEMA, N. RF-energy harvester and its applications in IoT: A review. In *Second International Conference on Informatics (ICI)*. Noida (India), 2023, p. 1–5. DOI: 10.1109/ICI60088.2023.10421418
- [36] RAO, B., HU, J., AL-NAHARI, A., et al. On the physical layer security of UAV-aided backscatter communications. *IEEE Wireless Communications Letters*, 2024, vol. 13, no. 2, p. 274–278. DOI: 10.1109/LWC.2023.3324914
- [37] VILES, E. C., SILVESTRE, E. R. R., MAYDANA, E. B. C., et al. Performance assessment of a low-power wide-area wireless network based on LoRa technology using IoT devices in different Bolivia areas. In *IEEE Eighth Ecuador Technical Chapters Meeting (ETCM)*. Cuenca (Ecuador), 2024, p. 1–4. DOI: 10.1109/ETCM63562.2024.10746217
- [38] FOTOUHI, A., QIANG, H., DING, M., et al. Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges. *IEEE Communications Surveys & Tutorials*, 2019, vol. 21, no. 4, p. 3417–3442. DOI: 10.1109/COMST.2019.2906228
- [39] SUN, X., NG, D. W. K., DING, Z., et al. Physical layer security in UAV systems: Challenges and opportunities. *IEEE Wireless Communications*, 2019, vol. 26, no. 5, p. 40–47. DOI: 10.1109/MWC.001.1900028
- [40] MINH, B. V., NGUYEN, T. N., TU, L. T. Physical layer security in wireless sensors networks: Secrecy outage probability analysis. *Journal of Information and Telecommunication*, 2025, vol. 9, no. 1, p. 1–23. DOI: 10.1080/24751839.2024.2352961
- [41] WANG, N., WANG, P., ALIPOUR-FANID, A., et al. Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities. *IEEE Internet of Things Journal*, 2019, vol. 6, no. 5, p. 8169–8181. DOI: 10.1109/JIOT.2019.2927379
- [42] ILLI, E., QARAQ, M., ALTHUNIBAT, S., et al. Physical layer security for authentication, confidentiality, and malicious node detection: A paradigm shift in securing IoT networks. *IEEE Communications Surveys & Tutorials*, 2024, vol. 26, no. 1, p. 347–388. DOI: 10.1109/COMST.2023.3327327
- [43] PHAM, T. H. T., NGUYEN, N. T. T., NGUYEN, Q. S., et al. Performance analysis in D2D partial NOMA-assisted backscatter communication. *Advances in Electrical and Electronic Engineering*, 2025, vol. 23, no. 3, p. 250–262. DOI: 10.15598/aeec.v23i3.250314
- [44] LI, Y., LU, G., YE, Y., et al. Symbol detection in multi-channel multi-tag ambient backscatter communication under IQ imbalance. *IEEE Transactions on Cognitive Communications and Networking*, 2026, vol. 12, p. 3777–3789. DOI: 10.1109/TCCN.2025.3632405
- [45] DEEPAN, N., REBEKKA, B. Backscatter-assisted wireless powered communication networks with multiple antennas. In *International Conference on Wireless Communications Signal Processing and Networking (WiSPNET)*. Chennai (India), 2020, p. 135–138. DOI: 10.1109/WiSPNET48689.2020.9198357
- [46] LI, X., ZHENG, Y., KHAN, W. U., et al. Physical layer security of cognitive ambient backscatter communications for green Internet-of-Things. *IEEE Transactions on Green Communications and Networking*, 2021, vol. 5, no. 3, p. 1066–1076. DOI: 10.1109/TGCN.2021.3062060
- [47] WANG, H., JIANG, J., HUANG, G., et al. Physical layer security of two-way ambient backscatter communication systems. *Wireless Communications and Mobile Computing*, 2022, vol. 2022, p. 1–10. DOI: 10.1155/2022/5445676
- [48] NGUYEN, T. N., KIM, H. Y., TRAN, P. T., et al. On the performance of secured ambient backscatter communications to protect digital content and copyrights. *IEEE Access*, 2025, vol. 13, p. 195385–195400. DOI: 10.1109/ACCESS.2025.3632851
- [49] CLERCKX, B., ZHANG, R., SCHÖBER, R., et al. Fundamentals of wireless information and power transfer: From RF energy harvester models to signal and system designs. *IEEE Journal on Selected Areas in Communications*, 2019, vol. 37, no. 1, p. 4–33. DOI: 10.1109/JSAC.2018.2872615

- [50] ZHANG, Y., GAO, F., FAN, L., et al. Secure communications for multi-tag backscatter systems. *IEEE Wireless Communications Letters*, 2019, vol. 8, no. 4, p. 1146–1149. DOI: 10.1109/LWC.2019.2909199
- [51] VO, D. T., HA THI-PHAM, T., TRAN, M., et al. Short packet communication in IoT networks: Performance analysis. *Journal of Information and Telecommunication*, 2026, vol. 10, no. 2, p. 199–212. DOI: 10.1080/24751839.2025.2487353
- [52] BHARGAV, N., COTTON, S. L., SIMMONS, D. E. Secrecy capacity analysis over κ - μ fading channels: Theory and applications. *IEEE Transactions on Communications*, 2016, vol. 64, no. 7, p. 3011–3024. DOI: 10.1109/TCOMM.2016.2565580
- [53] DING, Z., KRIKIDIS, I., SHARIF, B., et al. Wireless information and power transfer in cooperative networks with spatially random relays. *IEEE Transactions on Wireless Communications*, 2014, vol. 13, no. 8, p. 4440–4453. DOI: 10.1109/TWC.2014.2314114
- [54] DHUNGANA, Y., TELLAMBURA, C. Rational Gauss-Chebyshev quadratures for wireless performance analysis. *IEEE Wireless Communications Letters*, 2013, vol. 2, no. 2, p. 215–218. DOI: 10.1109/WCL.2013.012513.120837
- [55] OLVER, F. W. J., OLDE DAALHUIS, A. B., LOZIER, D. W., et al. *NIST Digital Library of Mathematical Functions*. Release 1.2.5 of 2025-12-15. [Online] Cited 2026-07-25. Available at: <https://dlmf.nist.gov/>

About the Authors ...

Sang Q. NGUYEN received the B.E. degree in Electrical Engineering from Ho Chi Minh City University of Transport, Vietnam, in 2010, the M.E. degree in Telecommunications Engineering from Ho Chi Minh City University of Technology, Vietnam, in 2013, and the Ph.D. degree in Electrical Engineering from the University of Ulsan, South Korea, in 2017. From 2017 to 2021, he was a Lecturer with Duy Tan University, Vietnam. Since May 2021, he has been a Lecturer with Ho Chi Minh City University of Transport. In September 2024, he joined the Post and Telecommunications Institute of Technology, Ho Chi Minh City, as a Lecturer. He was a Research Fellow with Queen's University Belfast, U.K., where he contributed to advancements in wireless communications. His research interests include cooperative communications, cognitive radio networks, physical layer security, NOMA, short-packet communications, and backscatter communications. His work primarily focuses on secure and energy-efficient communication solutions for next-generation wireless networks. Email: sangnq@ptit.edu.vn.

Minh-Han H. DO was born in Da Nang City, Vietnam, in 2005. She is currently pursuing the B.Eng. degree in Electronics and Telecommunications Engineering (High-Quality Program) with the Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam. She has received academic scholarships from Ton Duc Thang University for excellent academic achievement. Her current research interests include cooperative communications, cognitive radio, signal processing, satellite communications, UAVs, wireless power transfer, and physical layer security. Her research focuses on the performance analysis and optimization of emerging wireless communication networks. Email: dohoangminhhan.st@tdtu.edu.vn.

Lam-Dong HUYNH was born in Ho Chi Minh City, Vietnam, in 1987. He received the B.E. degree in Electronics and Telecommunications Engineering from Ho Chi Minh City University of Technology and Education, in 2010, and the M.E. degree in Electronic Engineering from the same university, in 2013. He is currently pursuing the Ph.D. degree at Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam, and serving as a Lecturer with the Posts and Telecommunications Institute of Technology, Ho Chi Minh City, Vietnam. His major research interests include cooperative communications, cognitive radio, signal processing, satellite communication, UAV, and physical layer security. Email: huynhlam-dong.st@tdtu.edu.vn.

Tan N. NGUYEN (Corresponding author) was born in Nha Trang City, Vietnam, in 1986. He received the B.S. degree in Electronics from Ho Chi Minh University of Natural Sciences, in 2008, the M.S. degree in Telecommunications Engineering from Vietnam National University, in 2012, and the Ph.D. degree in Communications Technologies from the Faculty of Electrical Engineering and Computer Science, VSB—Technical University of Ostrava, Czech Republic, in 2019. He joined the Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Vietnam, in 2013, and since then has been lecturing. He was appointed as an Associate Professor in electronics, in 2024. His major research interests include cooperative communications, cognitive radio, signal processing, satellite communication, UAV, and physical layer security. He started as the Editor-in-Chief of *Advances in Electrical and Electronic Engineering (AEEE) journal*, in 2023. Email: nguyennhattan@tdtu.edu.vn.