EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Secure short-packet communications in power beacon-assisted IoT networks over Nakagami-*m* fading channels

Dechuan Chen[1], Jin Li[1], Jianwei Hu[2*], Xingang Zhang[1], Shuai Zhang[1] and Dong Wang[1]

*Correspondence:
hujianwei1990@yeah.net

[1] College of Physics and Electronic Engineering, Nanyang Normal University, Nanyang 473061, China
[2] National Key Laboratory for Complex Systems Simulation, Beijing 100101, China

Abstract

In this work, we investigate short-packet communications in power beacon (PB)-assisted Internet-of-Things (IoT) networks, where an energy-constrained actuator first harvests energy from a dedicated PB, and then transmits confidential signals to a desired controller in the presence of an eavesdropper. We derive a closed-form lower bound approximation expression for the average achievable effective secrecy rate (AESR) over Nakagami-*m* fading channels. To gain more insights, we also present the asymptotic average AESR in the high signal-to-noise ratio (SNR) regime. Specifically, analytical results indicate that an average AESR floor appears with the increase of SNR. Moreover, a low complexity one-dimensional search method is employed to maximize the average AESR by optimizing the energy harvesting length. Monte-Carlo simulations are provided to corroborate our analysis.

Keywords: Short-packet communications, PB, Physical layer security, Average AESR

1 Introduction

Energy harvesting from radio-frequency signals has recently been introduced as a promising solution to extend the lifetime of low-power Internet-of-Things (IoT) devices [1–3]. For instance, in smart city applications, IoT sensors embedded in infrastructure can be powered by harvesting energy from ambient radio-frequency signals, ensuring continuous operation and reducing maintenance costs. Generally, wireless energy harvesting networks based on radio-frequency signals are categorized into three fundamental architectures: (1) simultaneous wireless information and power transfer (SWIPT) networks, where both wireless energy and information signals share the same waveform from a source [4]; (2) hybrid access point (HAP)-assisted networks, where energy-constrained devices receive energy signals transmitted by an HAP and subsequently use the harvested energy to transmit information signals back to the HAP [5]; and (3) power beacon (PB)-assisted networks, in which a dedicated and cost-effective PB is solely responsible for powering energy-constrained devices [6]. Specifically, low-cost energy-constrained devices in IoT networks charged by a dedicated PB is a hot design topic, since it is not

necessary to require backhaul links and can support for longer communication distances [7].

Due to the openness of the wireless medium, security is also a critical issue for IoT networks [8]. Traditional cryptographic techniques, which focus on securing data at higher layers of the communication protocol stack, have long been used for data protection. However, these methods face challenges when applied to IoT networks [9, 10]. On one hand, IoT devices often have limited computational capabilities, memory, and power constraints. Traditional encryption algorithms may be too computationally intensive for these devices, leading to increased latency and reduced performance. On the other hand, the restricted communication resources of IoT devices make it challenging to support the overhead associated with traditional encryption and decryption processes. Fortunately, physical-layer security presents a more appealing alternative to cryptographic techniques [11–13]. This is due to its elimination of the requirement for secret keys, as secrecy is achieved through leveraging the unique characteristics of the physical channel.

Recently, physical-layer security has drawn ever-increasing attention in PB-assisted IoT applications [14]. In [15], a hybrid PB scheme for secure communication was introduced, aimed at enhancing secrecy throughput by concurrently managing source transmit power, time allocation, and redundancy rate. Closed-form expressions for achievable secrecy outage probability was derived in [16] under several different jamming schemes, illustrating that having full channel state information (CSI) at a PB enables significant secrecy diversity gain through the utilization of a simple zero-forcing scheme. In particular, two adaptive secure transmission schemes, which dynamically determine whether to harvest energy or transmit confidential information based on the energy status and channel quality, were proposed in [17] to enhance the security of PB-assisted IoT networks. In [18], a PB first charge an energy-constrained user, and then act as a friendly jammer by transmitting jamming signals to degrade the eavesdropper channel.

The above studies on PB-assisted IoT networks assumed infinite blocklength transmission. However, the data flows of IoT networks are typically using short-packet for transmission to reduce the communication delay [19–21]. For example, temperature and humidity sensors in smart home automation frequently transmit small packets of data to the central control unit, enabling rapid response and efficient energy management within the household. Then, the Shannon capacity expression, where the blocklength tends to infinite, is not applicable for system design with short-packet feature. Considering physical-layer security with finite blocklength, [22] derived the maximal secrecy rate for general wiretap channels. In [23], a closed-form approximation for the average achievable effective secrecy rate (AESR) was obtained to measure the secrecy performance. The authors in [24] addressed a power control problem for secure short-packet communications using an unsupervised deep learning approach. Subsequently, [25] introduced the concept of average information leakage to evaluate the performance of short-packet communications, and maximized the average secrecy throughput through both adaptive and non-adaptive strategies. Although a few works [22–28] studied short-packet communications in the context of physical-layer security, they all did not consider the problem of energy constrained of IoT networks. Only in a recent work [29], the packet error rate and the packet length were jointly optimized to maximize the total

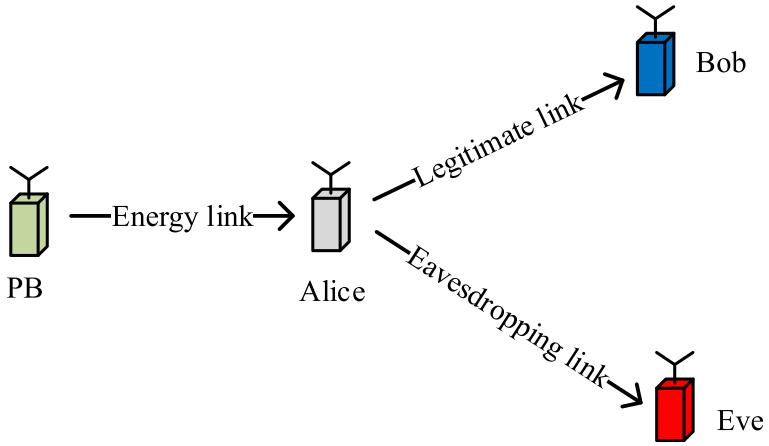

Fig. 1 Illustration of a secure PB-assisted IoT communication network

secrecy throughput of PB-assisted IoT networks. However, to the best of the authors' knowledge, the average AESR of PB-assisted IoT networks has not been studied yet. Moreover, the impact of channel fading severity on the secure short-packet communications remains unexplored.

Motivated by the above background, we investigate the secure short-packet communications in a PB-assisted IoT network, which consists of a dedicated PB, an energy-constrained actuator, a desired controller, and an eavesdropper. Considering the time-switching protocol, the energy-constrained actuator first harvests energy from the PB, and then uses the harvested energy to send sensitive information to the desired controller. Our contributions are threefold: first, we derive the approximation and asymptotic closed-form expressions for the average AESR over Nakagami-m channels, which indicate that an average AESR floor appears with the increase of SNR. Second, a low complexity one-dimensional search method is employed to maximize the average AESR by optimizing the energy harvesting length. Third, simulation results corroborate our analysis and offer valuable design guidelines for secure short-packet communications in PB-assisted IoT networks.

The remainder of this paper is organized as follows. In Sect. 2, we provide a description of PB-assisted IoT networks employing the time-switching protocol. In Sect. 3, we present the derivation of closed-form expressions for both average AESR and asymptotic average AESR, along with the determination of the optimal energy harvesting length to maximize the average AESR. Finally, numerical results and conclusions are, respectively, given in Sects. 4 and 5.

2 Methods/experimental

In this work, we consider secure short-packet communications in a PB-assisted IoT network as shown in Fig. 1, where an energy-constrained actuator (Alice) attempts to transmit sensitive information to a desired controller (Bob) in the presence of an eavesdropper (Eve). It is assumed that Alice is powered by a dedicated PB, without any external energy supply [17, 18, 29]. We assume that all the channels in the considered system are modeled as independent quasi-static Nakagami-m fading, which means that the channel coefficients

remain static during a coherence slot and vary independently from one coherence slot to the next [30]. A practical passive eavesdropping scenario is considered, where only the statistical CSI of Eve is available. Moreover, each node is equipped with a single antenna and operate in half duplex mode.

The transmission period of each packet contains the following two phases: energy harvesting phase and information transmission phase. In the energy harvesting phase, Alice utilizes L_e channel uses to harvest energy. In the information transmission phase, Alice sends confidential message of B bits to Bob through L_d channel uses. It is worth noting that the transmitter is equipped with a low-power circuit to match the low transmission power required for short-packet communications, as mentioned in [31]. In scenarios where the harvested power operates within a low-power regime without experiencing power saturation, the nonlinear energy harvesting model exhibits linear characteristics [32]. Therefore, in this work, we employ the linear energy harvesting model to simplify the subsequent analysis. The energy harvested at Alice can be expressed as $E_{\mathrm{h}} = \eta L_e T_s P \left|h_{\mathrm{pa}}\right|^2$, where P is the transmit power of PB, h_{pa} is the channel coefficient between PB and Alice with fading severity parameter m_p and average fading power Ω_p, $0 < \eta < 1$ is the energy conversion efficiency, and T_s is the time duration of one channel use. The details of energy harvesting process can be found in [33]. We assume that the harvested energy is completely used for signal transmission from Alice to Bob [17, 18, 29]. This is justifiable when the transmission distances are not too short, such that the energy utilized for transmission becomes the primary source of energy consumption. Therefore, the received SNRs at Bob and Eve can be, respectively, expressed as

$$\gamma_b = \omega \left|h_{\mathrm{pa}}\right|^2 \left|h_{\mathrm{ab}}\right|^2, \tag{1}$$

and

$$\gamma_e = \omega \left|h_{\mathrm{pa}}\right|^2 \left|h_{\mathrm{ae}}\right|^2, \tag{2}$$

where $\omega = \frac{P\eta L_e}{L_d N_0}$, N_0 is the noise variance at each receiver, h_{ab} is the channel coefficient between Alice and Bob with fading severity parameter m_b and average fading power Ω_b, h_{ae} is the channel coefficient between Alice and Eve with fading severity parameter m_e and average fading power Ω_e.

According to [22], for the PB-assisted IoT network with short-packet transmission, the achievable secrecy rate under the target decoding error probability ϵ and the information leakage probability δ is closely approximated by

$$R_s = \left[\log_2\left(\frac{1+\gamma_b}{1+\gamma_e}\right) - \sqrt{\frac{V_d}{L_d}}\frac{Q^{-1}(\epsilon)}{\ln 2} - \sqrt{\frac{V_e}{L_d}}\frac{Q^{-1}(\delta)}{\ln 2}\right]^+, \tag{3}$$

where $V_i = 1 - (1+\gamma_i)^{-2}$, $i \in \{b, e\}$, is the channel dispersion, $Q^{-1}(\cdot)$ is the inverse Q-function $Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} \mathrm{d}t$, and $[u]^+ = \max(u, 0)$.

3 Secrecy performance analysis

In this section, we investigate the secrecy performance of the PB-assisted IoT network with short-packet transmission in terms of average AESR. Before delving into the detailed analysis, we first present the statistical characteristics of legitimate channel and eavesdropping channel.

3.1 Preliminaries

Based on (1), the probability density function (PDF) and cumulative distribution function (CDF) of γ_b are given by

$$f_{\gamma_b}(x) = G_1 x^{c_1-1} K_{2c_2}\left(\sqrt{\frac{4m_b m_p x}{\Omega_b \Omega_p \omega}}\right), \tag{4}$$

and

$$\begin{aligned} F_{\gamma_b}(x) = 1 - \sum_{i=0}^{m_p-1} \left(\frac{m_b}{\Omega_b}\right)^{m_b} \left(\frac{m_p}{\Omega_p \omega}\right)^{i} \left(\frac{m_p \Omega_b}{\Omega_p \omega m_b}\right)^{\frac{m_b-i}{2}} \frac{2}{i!\Gamma(m_b)} \\ \times x^{\frac{m_b+i}{2}} K_{m_b-i}\left(\sqrt{\frac{4m_p m_b x}{\Omega_p \Omega_b \omega}}\right), \end{aligned} \tag{5}$$

where $G_1 = \left(\frac{m_b}{\Omega_b}\right)^{m_b} \left(\frac{m_p}{\Omega_p}\right)^{m_p} \left(\frac{m_p \Omega_b}{\Omega_p m_b}\right)^{c_2} \frac{2\omega^{-c_1}}{\Gamma(m_b)\Gamma(m_p)}$, $c_1 = \frac{m_b+m_p}{2}$, $c_2 = \frac{m_b-m_p}{2}$, $i! = i \times (i-1) \times \cdots \times 1$, $0! = 1$, $\Gamma(\cdot)$ is the gamma function, and $K_\nu(\cdot)$ is the ν^{th}-order modified Bessel function of the second kind.

Proof The proof can be found in Appendix A.

Making an appropriate substitution of the parameters, i.e., $m_b \to m_e$, and $\Omega_b \to \Omega_e$, we can obtain the exact PDF and CDF of γ_e as

$$f_{\gamma_e}(x) = G_2 x^{c_3-1} K_{2c_4}\left(\sqrt{\frac{4m_e m_p x}{\Omega_e \Omega_p \omega}}\right), \tag{6}$$

and

$$\begin{aligned} F_{\gamma_e}(x) = 1 - \sum_{i=0}^{m_p-1} \left(\frac{m_e}{\Omega_e}\right)^{m_b} \left(\frac{m_p}{\Omega_p \omega}\right)^{i} \left(\frac{m_p \Omega_e}{\Omega_p \omega m_e}\right)^{\frac{m_b-i}{2}} \frac{2}{i!\Gamma(m_e)} \\ \times x^{\frac{m_e+i}{2}} K_{m_e-i}\left(\sqrt{\frac{4m_p m_e x}{\Omega_p \Omega_e \omega}}\right), \end{aligned} \tag{7}$$

where $G_2 = \left(\frac{m_e}{\Omega_e}\right)^{m_e} \left(\frac{m_p}{\Omega_p}\right)^{m_p} \left(\frac{m_p \Omega_e}{\Omega_p m_e}\right)^{c_2} \frac{2\omega^{-c_3}}{\Gamma(m_e)\Gamma(m_p)}$, $c_3 = \frac{m_e+m_p}{2}$, and $c_4 = \frac{m_e-m_p}{2}$.

3.2 Average AESR

The average AESR is defined as the average number of information bits can be transmitted per channel use under given reliability and information leakage constraints. Mathematically, the average AESR of the PB-assisted IoT network can be formulated as

$$\begin{aligned}\bar{R}_s &= \frac{L_d}{L}\mathbb{E}_{\gamma_b,\gamma_e}(R_s)\\ &\overset{(\tilde{a})}{\geq} \frac{L_d}{L}\left[\mathbb{E}_{\gamma_b}\left(\log_2(1+\gamma_b)\right) - \frac{Q^{-1}(\epsilon)}{\ln 2\sqrt{L_d}}\mathbb{E}_{\gamma_b}\left(\sqrt{V_b}\right)\right.\\ &\qquad \left. -\mathbb{E}_{\gamma_e}\left(\log_2(1+\gamma_e)\right) - \frac{Q^{-1}(\delta)}{\ln 2\sqrt{L_d}}\mathbb{E}_{\gamma_e}\left(\sqrt{V_e}\right)\right]^+\\ &\triangleq \frac{L_d}{L}[\Phi_b(\gamma_b) - \Psi_b(\gamma_b,\epsilon) - \Phi_e(\gamma_e) - \Phi_e(\gamma_e,\delta)]^+,\end{aligned} \tag{8}$$

where $L = L_e + L_d$, $\mathbb{E}(\cdot)$ is the expectation, and $(\tilde{a})$ is obtained by using the fact that $\mathbb{E}(\max(U,V)) \geq \max(\mathbb{E}(U),\mathbb{E}(V))$.

Substituting (4) into (8), the integral term $\Phi_b(\gamma_b)$ can be derived as

$$\begin{aligned}\Phi_b(\gamma_b) &= \frac{1}{\ln 2}\int_0^\infty \ln(1+x) f_{\gamma_b}(x)\mathrm{d}x\\ &\overset{(a)}{=} \frac{G_1}{\ln 2}\int_0^\infty x^{c_1-1} G_{2,2}^{1,2}\left(x\middle|\begin{matrix}1,1\\1,0\end{matrix}\right) K_{2c_2}\left(\sqrt{\frac{4m_b m_p x}{\Omega_b\Omega_p\omega}}\right)\mathrm{d}x\\ &\overset{(b)}{=} \frac{G_1}{\ln 2}\left(\frac{\Omega_b\Omega_p\omega}{m_b m_p}\right)^{c_1}\int_0^\infty y^{c_1-1} G_{2,2}^{1,2}\left(\frac{\Omega_b\Omega_p\omega y}{m_b m_p}\middle|\begin{matrix}1,1\\1,0\end{matrix}\right) K_{2c_2}\left(2\sqrt{y}\right)\mathrm{d}y\\ &\overset{(c)}{=} \frac{G_1}{2\ln 2}\left(\frac{\Omega_b\Omega_p\omega}{m_b m_p}\right)^{c_1} G_{4,2}^{1,4}\left(\frac{\Omega_b\Omega_p\omega}{m_b m_p}\middle|\begin{matrix}1-c_1-c_2, 1-c_1+c_2, 1, 1\\1, 0\end{matrix}\right),\end{aligned} \tag{9}$$

where (a) is based on the fact that $\ln(1+x) = G_{2,2}^{1,2}\left(x\middle|\begin{matrix}1,1\\1,0\end{matrix}\right)$, (b) is obtained via using $y = \frac{m_p m_b x}{\Omega_p\Omega_b\omega}$, (c) is derived from [34, 7.821.3], and $G(\cdot|\cdot)$ is the Meijer's G-function.

In order to derive a closed-form expression of the integral term $\Psi_b(\gamma_b,\epsilon)$ in (8), we introduce a sufficiently large parameter M_1 to ensure $V_b \approx 1$, when $\gamma_b > M_1$, and then $\Psi_b(\gamma_b,\epsilon)$ is accordingly approximated as

$$\Psi_b(\gamma_b,\epsilon) \approx \frac{Q^{-1}(\epsilon)}{\ln 2\sqrt{L_d}}\left(\underbrace{\int_0^{M_1}\sqrt{1-(1+x)^{-2}} f_{\gamma_b}(x)\mathrm{d}x}_{\Psi_{b,1}(\gamma_b)} + \underbrace{\int_{M_1}^\infty f_{\gamma_b}(x)\mathrm{d}x}_{\Psi_{b,2}(\gamma_b)}\right). \tag{10}$$

On the one hand, using the Gaussian–Chebyshev quadrature method [35, 36], the integral term $\Psi_{b,1}(\gamma_b)$ can be approximated as

$$\begin{aligned}\Psi_{b,1}(\gamma_b) \approx &\sum_{n=1}^N \frac{\pi M_1}{2N} f_{\gamma_b}\left(\frac{M_1}{2}(1+t_n)\right)\\ &\times\sqrt{\left(1-t_n^2\right)\left(1-\left(1+\frac{M_1}{2}(1+t_n)\right)^{-2}\right)},\end{aligned} \tag{11}$$

where N is a parameter for the complexity accuracy tradeoff, and $t_n = \cos\left(\frac{2n-1}{2N}\pi\right)$. On the other hand, the integral term $\Psi_{b,2}(\gamma_b)$ can be derived as

$$\Psi_{b,2}(\gamma_b) = F_{\gamma_b}(x)\Big|_{M_1}^{\infty} = 1 - F_{\gamma_b}(M_1). \tag{12}$$

Substituting (11) and (12) into (10), we have a closed-form approximation of $\Psi_b(\gamma_b, \epsilon)$, which is given by

$$\begin{aligned}\Psi_b(\gamma_b, \epsilon) \approx \frac{Q^{-1}(\epsilon)}{\ln 2\sqrt{L_d}} \Bigg(1 - F_{\gamma_b}(M_1) + \sum_{n=1}^{N} \frac{\pi M_1}{2N} f_{\gamma_b}\left(\frac{M_1}{2}(1+t_n)\right) \\ \times \sqrt{\left(1-t_n^2\right)\left(1 - \left(1 + \frac{M_1}{2}(1+t_n)\right)^{-2}\right)} \Bigg).\end{aligned} \tag{13}$$

Then, by following similar procedures as in $\Phi_b(\gamma_b)$ and $\Psi_b(\gamma_b, \epsilon)$, we can obtain closed-form approximation expressions of $\Phi_e(\gamma_e)$ and $\Psi_e(\gamma_e, \delta)$ as

$$\Phi_e(\gamma_e) = \frac{G_2}{2\ln 2}\left(\frac{\Omega_e \Omega_p \omega}{m_e m_p}\right)^{c_3} G_{4,2}^{1,4}\left(\frac{\Omega_e \Omega_p \omega}{m_e m_p}\middle| \begin{matrix} 1 - c_3 - c_4, 1 - c_3 + c_4, 1, 1 \\ 1, 0 \end{matrix}\right), \tag{14}$$

and

$$\begin{aligned}\Psi_e(\gamma_e, \delta) \approx \frac{Q^{-1}(\delta)}{\ln 2\sqrt{L_d}} \Bigg(1 - F_{\gamma_e}(M_2) + \sum_{n=1}^{N} \frac{\pi M_2}{2N} f_{\gamma_e}\left(\frac{M_2}{2}(1+t_n)\right) \\ \times \sqrt{\left(1-t_n^2\right)\left(1 - \left(1 + \frac{M_2}{2}(1+t_n)\right)^{-2}\right)} \Bigg),\end{aligned} \tag{15}$$

where M_2 is a sufficiently large parameter to ensure $V_e \approx 1$, when $\gamma_e > M_2$.

Accordingly, we can derive the approximation lower bound expression for the average AESR of the PB-assisted IoT network with short-packet transmission as

$$\begin{aligned}\bar{R}_s = \Bigg[\frac{L_d}{L} \Bigg(\frac{G_1}{2\ln 2}\left(\frac{\Omega_b \Omega_p \omega}{m_b m_p}\right)^{c_1} G_{4,2}^{1,4}\left(\frac{\Omega_b \Omega_p \omega}{m_b m_p}\middle| \begin{matrix} 1 - c_1 - c_2, 1 - c_1 + c_2, 1, 1 \\ 1, 0 \end{matrix}\right) \\ - \frac{Q^{-1}(\epsilon)}{\ln 2\sqrt{L_d}} \Bigg(1 - F_{\gamma_b}(M_1) + \sum_{n=1}^{N} \frac{\pi M_1}{2N} f_{\gamma_b}\left(\frac{M_1}{2}(1+t_n)\right) \\ \times \sqrt{\left(1-t_n^2\right)\left(1 - \left(1 + \frac{M_1}{2}(1+t_n)\right)^{-2}\right)} \Bigg) \\ - \frac{G_2}{2\ln 2}\left(\frac{\Omega_e \Omega_p \omega}{m_e m_p}\right)^{c_3} G_{4,2}^{1,4}\left(\frac{\Omega_e \Omega_p \omega}{m_e m_p}\middle| \begin{matrix} 1 - c_3 - c_4, 1 - c_3 + c_4, 1, 1 \\ 1, 0 \end{matrix}\right) \\ - \frac{Q^{-1}(\delta)}{\ln 2\sqrt{L_d}} \Bigg(1 - F_{\gamma_e}(M_2) + \sum_{n=1}^{N} \frac{\pi M_2}{2N} f_{\gamma_e}\left(\frac{M_2}{2}(1+t_n)\right) \\ \times \sqrt{\left(1-t_n^2\right)\left(1 - \left(1 + \frac{M_2}{2}(1+t_n)\right)^{-2}\right)} \Bigg) \Bigg) \Bigg]^{+}.\end{aligned} \tag{16}$$

3.3 Asymptotic analysis

In this section, we turn our attention to the high SNR regime, and derive the asymptotic expression for average AESR to achieve more insights. In the high SNR regime, there exists $1+\gamma_x \approx \gamma_x$, and $V_x \approx 1$, and the achievable secrecy rate of the PB-assisted IoT network with short-packet transmission in (3) is given by

$$R_s^{\infty} = \left[\log_2\left(\frac{|h_{ab}|^2}{|h_{ae}|^2}\right) - \frac{Q^{-1}(\epsilon)}{\ln 2\sqrt{L_d}} - \frac{Q^{-1}(\delta)}{\ln 2\sqrt{L_d}}\right]^+. \tag{17}$$

Therefore, the asymptotic average AESR in the high SNR regime can be expressed as

$$\begin{aligned}\bar{R}_s^{\infty} &\geq \frac{L_d}{L}\left[\mathbb{E}_{|h_{ab}|^2}\left(\log_2|h_{ab}|^2\right) - \mathbb{E}_{|h_{ae}|^2}\left(\log_2|h_{ae}|^2\right) - \frac{Q^{-1}(\epsilon)}{\ln 2\sqrt{L_d}} - \frac{Q^{-1}(\delta)}{\ln 2\sqrt{L_d}}\right]^+ \\ &= \frac{L_d}{L}\left[\left(\frac{m_b}{\Omega_b}\right)^{m_b}\frac{1}{\ln 2\Gamma(m_b)}\int_0^{\infty} x^{m_b-1}e^{-\frac{m_b x}{\Omega_b}}\ln x\mathrm{d}x - \frac{Q^{-1}(\epsilon)}{\ln 2\sqrt{L_d}}\right. \\ &\quad \left. -\left(\frac{m_e}{\Omega_e}\right)^{m_e}\frac{1}{\ln 2\Gamma(m_e)}\int_0^{\infty} x^{m_e-1}e^{-\frac{m_e x}{\Omega_e}}\ln x\mathrm{d}x - \frac{Q^{-1}(\delta)}{\ln 2\sqrt{L_d}}\right]^+ \\ &\overset{(d)}{=} \frac{L_d}{L}\left[\frac{\psi(m_b) - \ln m_b + \ln\Omega_b - \psi(m_e) + \ln m_e - \ln\Omega_e}{\ln 2} - \frac{Q^{-1}(\epsilon)}{\ln 2\sqrt{L_d}} - \frac{Q^{-1}(\delta)}{\ln 2\sqrt{L_d}}\right]^+,\end{aligned} \tag{18}$$

where (d) is derived from [34, 4.352.1], and $\psi(\cdot)$ is the psi function. Specifically, when $m_b = m_e = 1$, the expression in (18) reduces to the Rayleigh fading scenario as

$$\bar{R}_s^{\infty} = \frac{L_d}{L}\left[\frac{\ln\Omega_b - \ln\Omega_e}{\ln 2} - \frac{Q^{-1}(\epsilon)}{\ln 2\sqrt{L_d}} - \frac{Q^{-1}(\delta)}{\ln 2\sqrt{L_d}}\right]^+. \tag{19}$$

From (18), we can see that the asymptotic average AESR mainly depends on L_e, L_d, ϵ, δ, m_b, Ω_b, m_e, and Ω_e, and is independent of m_p and Ω_p. Moreover, there is an average AESR floor in the high SNR regime, indicating that the average AESR does not decrease as the SNR further increases. This occurs because as the SNR of the legitimate node approaches infinity, the SNR of the eavesdropping node also approaches infinity.

3.4 Optimal transmission design

Under the given constraints of reliability and information leakage, the maximization of average AESR can be achieved by optimizing the length of energy harvesting. Specifically, the problem of maximizing average AESR can be formulated as follows:

$$\begin{aligned}&\max_{L_e} \quad \bar{R}_s \\ &s.t. \quad L_e \in \{1, 2, \cdots, L-1\}.\end{aligned} \tag{20}$$

Due to the complexity of the average AESR expression, it is difficult to obtain an explicit solution for the optimal energy harvesting length. However, the Golden Search method, which is a low complexity one-dimensional search method shown as Algorithm 1, can be employed to obtain the optimal energy harvesting length.

Algorithm 1 Golden Search Iterative Algorithm for average AESR maximization

Initialization: $L_{e,L}^1 = 1$, $L_{e,U}^1 = L - 1$, and the iteration number $k = 1$;
Calculate $\upsilon_1 = L_{e,L}^1 + 0.382\left(L_{e,U}^1 - L_{e,L}^1\right)$ and $\mu_1 = L_{e,L}^1 + 0.618\left(L_{e,U}^1 - L_{e,L}^1\right)$;
while $\mu_k - \upsilon_k \leq 0.5$ **do**
    Calculate the average AESR $\bar{R}_s(\upsilon_k)$ and $\bar{R}_s(\mu_k)$;
    if $\bar{R}_s(\upsilon_k) \geq \bar{R}_s(\mu_k)$ **then**
        Update $L_{e,L}^{k+1} = L_{e,L}^k$, $L_{e,U}^{k+1} = \mu_k$, $\mu_{k+1} = \upsilon_k$, $\upsilon_{k+1} = L_{e,L}^{k+1} + 0.382\left(L_{e,U}^{k+1} - L_{e,L}^{k+1}\right)$, $\bar{R}_s(\mu_{k+1}) = \bar{R}_s(\upsilon_k)$, calculate $\bar{R}_s(\upsilon_{k+1})$, and set $k = k+1$;
    else
        Update $L_{e,L}^{k+1} = \upsilon_k$, $L_{e,U}^{k+1} = L_{e,U}^k$, $\upsilon_{k+1} = \mu_k$, $\mu_{k+1} = L_{e,L}^{k+1} + 0.618\left(L_{e,U}^{k+1} - L_{e,L}^{k+1}\right)$, $\bar{R}_s(\upsilon_{k+1}) = \bar{R}_s(\mu_k)$, calculate $\bar{R}_s(\mu_{k+1})$, and set $k = k+1$;
    end if
end while
Let $L_e^{opt1} = \left\lfloor \frac{\mu_k + \upsilon_k}{2} \right\rfloor$ and $L_e^{opt2} = \left\lceil \frac{\mu_k + \upsilon_k}{2} \right\rceil$;
if $\bar{R}_s\left(L_e^{opt1}\right) \leq \bar{R}_s\left(L_e^{opt2}\right)$ **then**
    $L_e^{opt} = L_e^{opt2}$;
else
    $L_e^{opt} = L_e^{opt1}$;
end if
Obtain the optimal energy harvesting length L_e^{opt}.

4 Results and discussion

In this section, we present the simulation results of the PB-assisted IoT network with short-packet transmission. All channels undergo the Nakagami-m fading, which is a generalized fading model and fits well in IoT scenarios [27]. According to [37], the channel use in short-packet communications is usually set in the range of 100–1000. Therefore, we set $L_d = 300$. Unless specified otherwise, we assume that $\epsilon = 10^{-3}$, $\delta = 10^{-7}$, $\eta = 0.8$, $M_1 = M_2 = 30$, $N = 200$, $L_e = 100$, $\Omega_b = 12$ dB, $\Omega_e = 0$ dB, $\Omega_p = 0$ dB, $m_b = 2$, $m_e = 2$, and $m_p = 2$. Moreover, let $\lambda = P/N_0$ denote the transmit SNR.

Figure 2 plots the average AESR versus the energy harvesting length L_e with different values of λ. We first observe that the Monte-Carlo simulation results match well with the approximation expression of average AESR, which demonstrates the correctness of analytical results. We second observe that the average AESR increases as L_e increases from 0 to some optimal L_e (80 for $\lambda = 10$ dB) but later, it starts decreasing as L_e increases from its optimal value. This phenomenon is explained as follows: when L_e is too small, there is less time for energy harvesting such that less transmission power is available for Alice, which will lead to poor average AESR. When L_e is too large, more power is available for Alice such that it increases the amount of information leakage, which results in the degradation of average AESR. In addition, we observe that the optimal L_e decreases as λ increases. This is because, in order to maintain a fixed secrecy rate, the energy harvesting length L_e should be decreased when a larger λ is employed.

Figure 3 plots the average AESR versus the transmit SNR λ with different values of fading severity parameters, where $\Omega_b = 5$ dB. We first observe an increase in the average AESR as λ increases, which eventually saturates in the high SNR regime. Consequently,

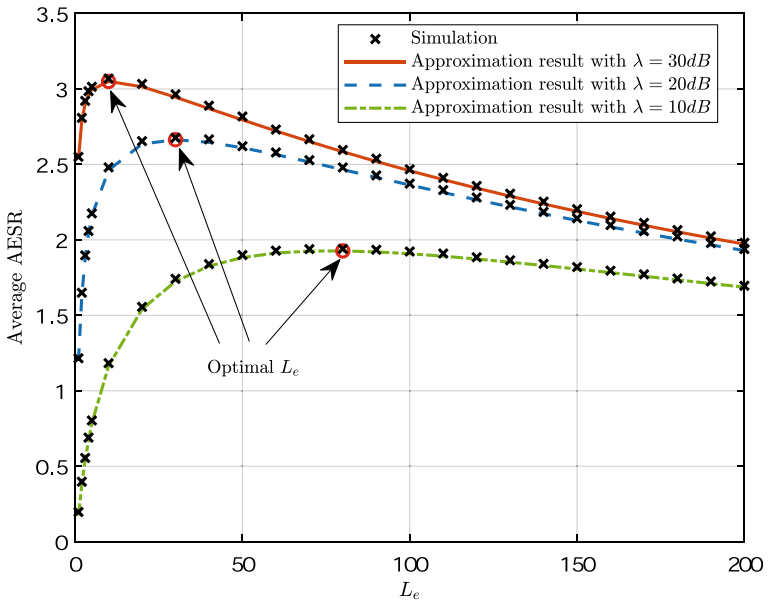

Fig. 2 Average AESR versus the energy harvesting length L_e with different values of λ

continuously boosting the SNR may not always enhance the performance of the PB-assisted IoT network when transmitting short packets. We second observe that the floor can be improved with higher values of fading severity parameters. The reason behind this is that higher values of fading severity parameters indicate improved propagation conditions. Furthermore, we observe that the floor is unaffected by the channel between the PB and Alice, since the channel quality of the legitimate and eavesdropping links ultimately becomes the limiting factor for average AESR.

Figure 4 plots the average AESR versus the energy conversion efficiency η with different values of λ. It is observed that with $\lambda = 10$ dB, the average AESR consistently

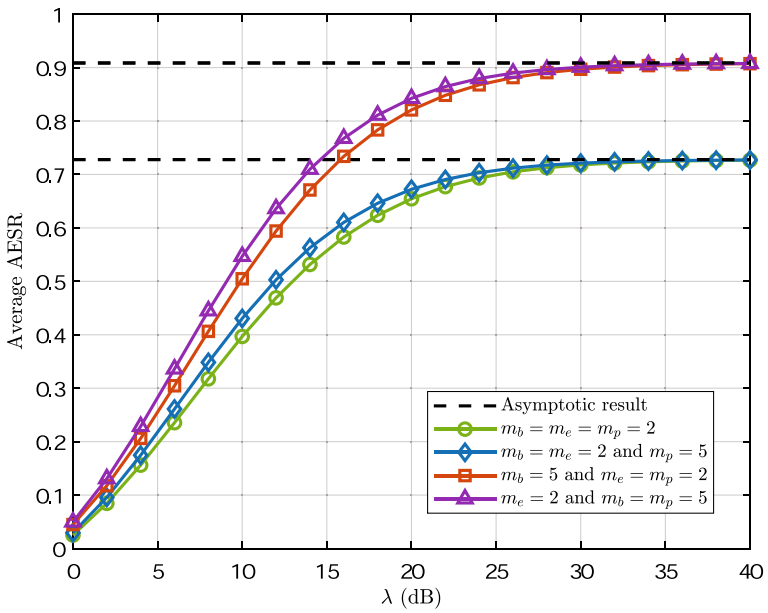

Fig. 3 Average AESR versus the transmit SNR λ with different values of fading severity parameters

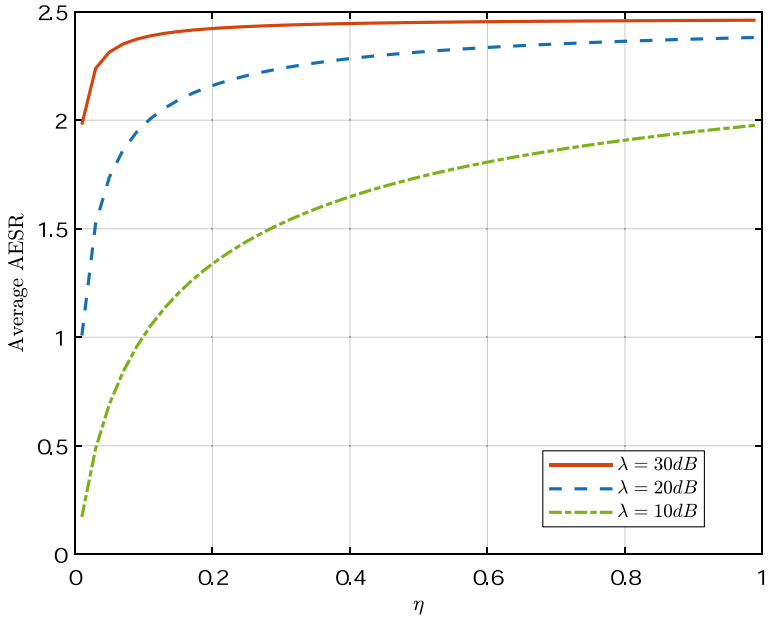

Fig. 4 Average AESR versus the energy conversion efficiency η with different values of λ

increases as the energy conversion efficiency improves. In contrast, with $\lambda = 30$ dB, the average AESR exhibits a more significant increase for lower values of energy harvesting efficiency, while remaining relatively constant for higher values of energy harvesting efficiency. Therefore, it is clarified that enhancing average AESR through energy conversion efficiency is more pronounced in the low SNR region. This is attributed to the fact that enhancing the energy conversion efficiency enables Alice to obtain a greater amount of energy for transmitting information, particularly in the low SNR region.

Figure 5 plots the average AESR and conventional ergodic secrecy rate (ESR) versus the information transmission length L_d with different values of λ, where $L_e = 30$. The conventional ESR $\bar{R}_s^{\text{ESR}} \triangleq \frac{L_d}{L}[\Phi_b(\gamma_b) - \Phi_e(\gamma_e)]^+$ is a metric that quantifies the average number of confidential information bits that can be transmitted per channel use in a scenario where the codeword blocklength tends to infinity. It is important to note that the average AESR, which takes into account the short-packet feature, is consistently lower than the conventional ESR assuming an infinite blocklength. This signifies that the conventional ESR tends to overestimate the practical secrecy performance of the PB-assisted IoT network when finite-length coding is applied. To mitigate this negative impact, one approach is to relax the latency constraint. However, we observe that loosing the latency constraint does not always contribute to an improvement in the average AESR, as it leads to a decrease in the transmit power of Alice.

Figure 6 plots the average AESR under different energy harvesting schemes versus the transmission latency L, where $\lambda = 20$ dB. We present the following energy harvesting schemes to ensure comparable results: (1) fixed-ratio energy harvesting length scheme with the energy harvesting length $L_e = 0.5L$ being fixed; (2) fixed energy harvesting length scheme with the energy harvesting length $L_e = 40$ being fixed. It is evident that the average AESR achieved with the optimal energy harvesting length surpasses the performance of

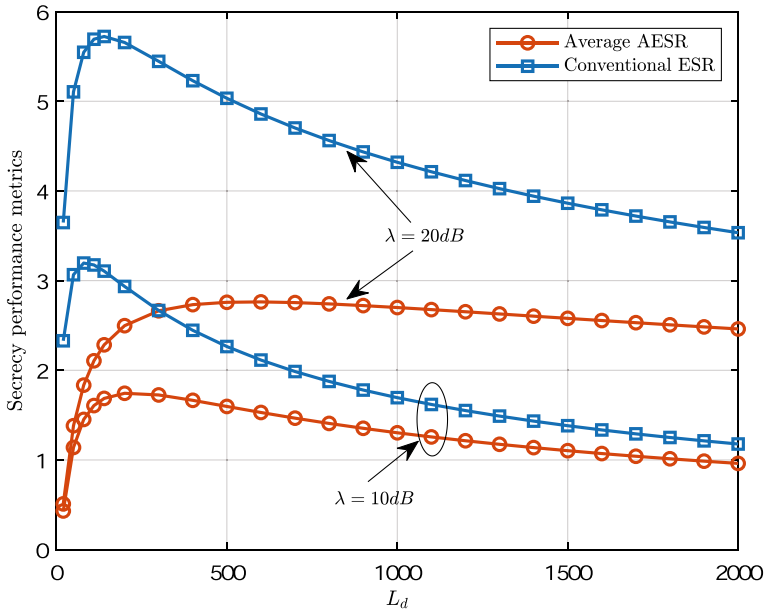

Fig. 5 Average AESR and conventional ESR versus the information transmission length L_d with different values of λ

the two benchmark schemes mentioned earlier, indicating a substantial enhancement in the PB-assisted IoT network's performance through the optimization of the energy harvesting length.

5 Conclusions

In this work, we presented a comprehensive secrecy performance analysis for PB-assisted IoT networks with short-packet transmission. Both approximation and asymptotic expressions of average AESR were provided over Nakagami-m fading channel. Specifically, an

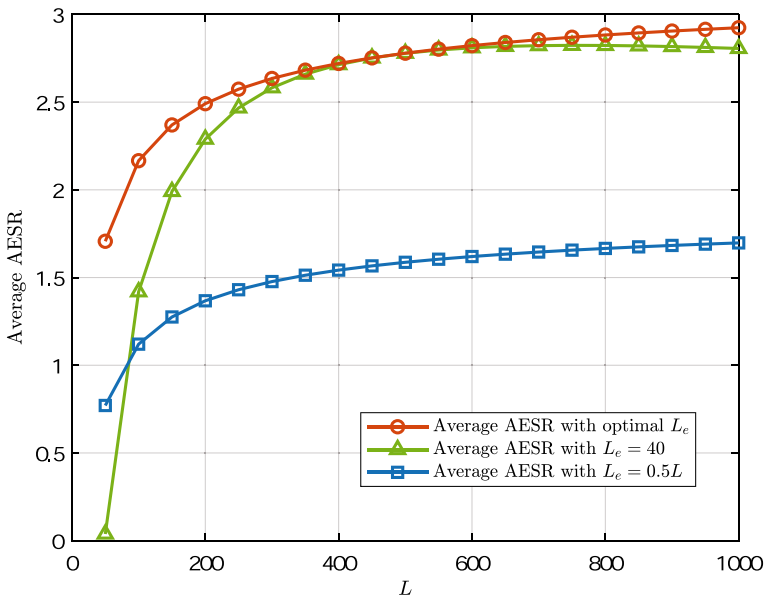

Fig. 6 Average AESR under different energy harvesting schemes versus the transmission latency L

average AESR floor appears with the increase of SNR, indicating that continuously boosting the SNR may not always enhance the performance of the PB-assisted IoT network when transmitting short packets. Moreover, a low complexity one-dimensional search method was used to obtain the optimal energy harvesting length for maximizing the average AESR. The simulations results corroborated our analysis and brought some meaningful insights as well.

Appendix A

Without loss of generality, let us denote $X_1 = \left|h_{\mathrm{ab}}\right|^2$, and $Y_1 = \left|h_{\mathrm{pa}}\right|^2$. Then, the PDFs of X, and Y can be given, respectively, by

$$f_{X_1}(x_1) = \left(\frac{m_b}{\Omega_b}\right)^{m_b} \frac{x_1^{m_b-1}}{\Gamma(m_b)} e^{-\frac{m_b x_1}{\Omega_b}}, \tag{21}$$

and

$$f_{Y_1}(y_1) = \left(\frac{m_p}{\Omega_p}\right)^{m_b} \frac{y_1^{m_p-1}}{\Gamma(m_p)} e^{-\frac{m_p y_1}{\Omega_p}}. \tag{22}$$

According to [38], the PDF of random variable $Z = XY$ can be formulated as

$$\begin{aligned} f_Z(z) &= \int_0^\infty \frac{1}{x_1} f_{X_1}(x_1) f_{Y_1}\left(\frac{z}{x_1}\right) \mathrm{d}x_1 \\ &= \left(\frac{m_b}{\Omega_b}\right)^{m_b} \left(\frac{m_p}{\Omega_p}\right)^{m_p} \frac{z^{m_p-1}}{\Gamma(m_b)\Gamma(m_p)} \\ &\quad \times \int_0^\infty x_1^{m_b-m_p-1} e^{-\frac{m_b x_1}{\Omega_b} - \frac{m_p z}{\Omega_p x_1}} \mathrm{d}x_1 \\ &\overset{(f)}{=} \left(\frac{m_b}{\Omega_b}\right)^{m_b} \left(\frac{m_p}{\Omega_p}\right)^{m_p} \left(\frac{m_p \Omega_b}{\Omega_p m_b}\right)^{c_2} \\ &\quad \times \frac{2 z^{c_1-1}}{\Gamma(m_b)\Gamma(m_p)} K_{2c_2}\left(\sqrt{\frac{4 m_b m_p z}{\Omega_b \Omega_p}}\right), \end{aligned} \tag{23}$$

where (f) is derived from [34, 3.471.9]. Subsequently, we can derived the PDF of γ_b as

$$\begin{aligned} f_{\gamma_b}(x) &= \frac{1}{\omega} f_Z\left(\frac{x}{\omega}\right) \\ &= G_1 x^{c_1-1} K_{2c_2}\left(\sqrt{\frac{4 m_b m_p x}{\Omega_b \Omega_p \omega}}\right). \end{aligned} \tag{24}$$

According to (1), the CDF of γ_b can be formulated as

$$F_{\gamma_b}(x) = \int_0^\infty F_{Y_1}\left(\frac{x}{\omega x_1}\right) f_{X_1}(x_1) \mathrm{d}x_1, \tag{25}$$

where the CDF of X_1 is given by

$$F_{Y_1}(y_1) = 1 - \sum_{i=0}^{m_p-1} \left(\frac{m_p y_1}{\Omega_p}\right)^i \frac{1}{i!} e^{-\frac{m_p y_1}{\Omega_p}}. \tag{26}$$

Substituting (26) in (25), performing mathematical operations and using [34, 3.471.9], we can obtain

$$\begin{aligned} F_{\gamma_b}(x) = 1 - \sum_{i=0}^{m_p-1} \left(\frac{m_b}{\Omega_b}\right)^{m_b} \left(\frac{m_p}{\Omega_p \omega}\right)^i \left(\frac{m_p \Omega_p}{\Omega_p \omega m_b}\right)^{\frac{m_b-i}{2}} \frac{2}{i!\Gamma(m_b)} \\ \times x^{\frac{m_b+i}{2}} K_{m_b-i}\left(\sqrt{\frac{4 m_p m_b x}{\Omega_p \Omega_b \omega}}\right). \end{aligned} \tag{27}$$

Abbreviations

AESR	Achievable effective secrecy rate
CDF	Cumulative distribution function
CSI	Channel state information
ESR	Ergodic secrecy rate
HAP	Hybrid access point
IoT	Internet-of-Things
PB	Power beacon
PDF	Probability density function
SNR	Signal-to-noise ratio
SWIPT	Simultaneous wireless information and power transfer

Author contributions

DC and JL wrote the paper. JH and XZ performed the simulations. SZ and DW reviewed the manuscript. All authors read and approved the manuscript.

Funding

This work was supported in part by the Doctoral Research Start-up Funding of Nanyang Normal University under Grant no. 2022ZX017, in part by the Cultivating Fund Project for the National Natural Science Foundation of China of Nanyang Normal University under Grant no. 2022PY024, in part by the Key Scientific Research Projects of Colleges and Universities in Henan Province of China under Grant nos. 23A520038, 23A510001, 24A520031, and 24A520032, in part by the Key Scientific and Technological Research Projects in Henan Province under Grant nos. 232102210121, 232102220101, and 242102320068, in part by the Henan Provincial Natural Science Foundation Project under Grant no. 232300421355, in part by the Young Backbone Teachers of Nanyang Normal University under Grant no. 2023-QNGG-7, and in part by Henan Engineering Research Center of Rare Earth Alloys.

Availability of data and materials

Data will be made available on reasonable request from the corresponding author.

Declarations

Competing interests

The authors declare that they have no conflict of interest.

Received: 26 June 2024 Accepted: 1 October 2024
Published online: 10 October 2024

References

1. D. Ma, G. Lan, M. Hassan, W. Hu and S.K. Das, Sensing, computing, and communications for energy harvesting IoTs: a survey. IEEE Commun. Surv. Tutor. **22**(2), 1222-1250 (Secondquarter 2020)
2. O.L.A. López, H. Alves, R.D. Souza, S. Montejo-Sánchez, E.M.G. Fernández, M. Latva-Aho, Massive wireless energy transfer: enabling sustainable IoT toward 6G era. IEEE Internet Things J. **8**(11), 8816–8835 (2021)
3. Z. Fang, J. Wang, Y. Ren, Z. Han, H.V. Poor, L. Hanzo, Age of information in energy harvesting aided massive multiple access networks. IEEE J. Sel. Areas Commun. **40**(5), 1441–1456 (2022)
4. K. Agrawal, S. Prakriya, M.F. Flanagan, TS-based SWIPT in full-duplex relayed NOMA with intelligent relay battery management. IEEE Trans. Commun. **71**(9), 5137–5151 (2023)

5. J. Chen, L. Zhang, Y.-C. Liang, X. Kang, R. Zhang, Resource allocation for wireless-powered IoT networks with short packet communication. IEEE Trans. Wirel. Commun. **18**(2), 1447–1461 (2019)
6. J. Yang, X. Wu, K.P. Peppas, P.T. Mathiopoulos, Capacity analysis of power beacon-assisted energy harvesting MIMO system over κ−μ shadowed fading channels. IEEE Trans. Veh. Technol. **70**(11), 11869–11880 (2021)
7. G. Li, D. Mishra, H. Jiang, Resource allocation in power-beacon-assisted IoT networks with nonorthogonal multiple access. IEEE Internet Things J. **8**(18), 14385–14398 (2021)
8. E. Illi et al., Physical layer security for authentication, confidentiality, and malicious node detection: a paradigm shift in securing IoT networks. IEEE Commun. Surv. Tutor. **26**(1), 347–388 (2024)
9. J. Hu, N. Yang, Y. Cai, Secure downlink transmission in the Internet of Things: How many antennas are needed? IEEE J. Sel. Areas Commun. **36**(7), 1622–1634 (2018)
10. M.S.J. Solaija, H. Salman, H. Arslan, Towards a unified framework for physical layer security in 5G and beyond networks. IEEE Open J. Veh. Technol. **3**, 321–343 (2022)
11. X. Sun, W. Yang, Y. Cai, Secure and reliable transmission in mmWave NOMA relay networks with SWIPT. IEEE Syst. J. **16**(3), 4861–4872 (2022)
12. X. Jiang, P. Li, Y. Zou, B. Li, R. Wang, Physical layer security for cognitive multiuser networks with hardware impairments and channel estimation errors. IEEE Trans. Commun. **70**(9), 6164–6180 (2022)
13. H. Du et al., Rethinking wireless communication security in semantic Internet of Things. IEEE Wirel. Commun. **30**(3), 36–43 (2023)
14. X. Lu, N. Cong Luong, D.T. Hoang, D. Niyato, Y. Xiao, P. Wang, Secure wirelessly powered networks at the physical layer: challenges, countermeasures, and road ahead. Proc. IEEE **110**(1), 193–209 (2022)
15. L. Tang, Q. Li, Wireless power transfer and cooperative jamming for secrecy throughput maximization. IEEE Wirel. Commun. Lett. **5**(5), 556–559 (2016)
16. X. Jiang, C. Zhong, Z. Zhang, G.K. Karagiannidis, Power beacon assisted wiretap channels with jamming. IEEE Trans. Wireless Commun. **15**(12), 8353–8367 (2016)
17. Y. Wang, W. Yang, T. Zhang, Y. Chen, X. Shang, Q. Wang, Adaptive secure transmission for wireless powered communication networks. China Commun. **18**(3), 155–173 (2021)
18. M. Wu, Q. Song, L. Guo, I. Lee, Energy-efficient secure computation offloading in wireless powered mobile edge computing systems. IEEE Trans. Veh. Technol. **72**(5), 6907–6912 (2023)
19. G. Durisi, T. Koch, P. Popovski, Toward massive, ultrareliable, and low-latency wireless communication with short packets. Proc. IEEE **104**(9), 1711–1726 (2016)
20. Z. Xiang, W. Yang, Y. Cai, Z. Ding, Y. Song, Y. Zou, NOMA-assisted secure short-packet communications in IoT. IEEE Wirel. Commun. **27**(4), 8–15 (2020)
21. R. Ma, W. Yang, X. Guan, X. Lu, Y. Song, D. Chen, Covert mmWave communications with finite blocklength against spatially random wardens. IEEE Internet of Things J. **11**(2), 3402–3416 (2024)
22. W. Yang, R.F. Schaefer, H.V. Poor, Wiretap channels: nonasymptotic fundamental limits. IEEE Trans. Inf. Theory **65**(7), 4069–4093 (2019)
23. Y. Xie, P. Ren, Optimizing training and transmission overheads for secure URLLC against randomly distributed eavesdroppers. IEEE Trans. Veh. Technol. **71**(11), 11921–11935 (2022)
24. C. Li, C. She, N. Yang, T.Q.S. Quek, Secure transmission rate of short packets with queueing delay requirement. IEEE Trans. Wirel. Commun. **21**(1), 203–218 (2022)
25. M.T. Mamaghani, X. Zhou, N. Yang, A.L. Swindlehurst, H.V. Poor, Performance analysis of finite blocklength transmissions over wiretap fading channels: an average information leakage perspective. IEEE Trans. Wirel. Commun. accepted to appear. https://doi.org/10.1109/TWC.2024.3400601.
26. C. Feng, H.M. Wang, H.V. Poor, Reliable and secure short-packet communications. IEEE Trans. Wireless Commun. **21**(3), 1913–1926 (2022)
27. Z. Xiang, W. Yang, Y. Cai, J. Xiong, Z. Ding, Y. Song, Secure transmission in a NOMA-assisted IoT network with diversified communication requirements. IEEE Internet Things J. **7**(11), 11157–11169 (2020)
28. D. Chen, J. Li, J. Hu, X. Zhang, S. Zhang, Secure short-packet communications using a full-duplex receiver. Int. J. Intell. Netw. **4**, 349–354 (2023)
29. D. Xu, H. Zhao, H. Zhu, Resource allocation for secure short packet communications in wireless powered IoT networks. IEEE Trans. Veh. Technol. **72**(8), 11000–11005 (2023)
30. C. Xia, Z. Xiang, J. Meng, H. Liu, G. Pan, Reliable transmission of short packets in cognitive radio inspired NOMA network. IEEE Syst. J. **17**(4), 6148–6158 (2023)
31. T.A. Khan, R.W. Heath, P. Popovski, Wirelessly powered communication networks with short packets. IEEE Trans. Commun. **65**(12), 5529–5543 (2017)
32. E. Boshkovska, D.W.K. Ng, N. Zlatanov, R. Schober, Practical non-linear energy harvesting model and resource allocation for SWIPT systems. IEEE Commun. Lett. **19**(12), 2082–2085 (2015)
33. X. Zhou, R. Zhang, C.K. Ho, Wireless information and power transfer: architecture design and rate-energy tradeoff. IEEE Trans. Commun. **61**(11), 4754–4767 (2013)
34. I.S. Gradshteyn, I.M. Ryzhik, *Table of Integrals, Series and Products*, 7th edn. (Academic, New York, NY, USA, 2007)
35. D. Chen, J. Li, J. Hu, X. Zhang, S. Zhang, D. Wang, Interference-assisted energy harvesting short packet communications with hardware impairments. Int. J. Intell. Netw. **5**, 231–240 (2024)
36. M. Abramowitz, I.A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, 9th edn. (US Govt. Print, Washington, USA, 1972)
37. H. Wang, Q. Yang, Z. Ding, H.V. Poor, Secure short-packet communications for mission-critical IoT applications. IEEE Trans. Wirel. Commun. **18**(5), 2565–2578 (2019)
38. A. Papoulis, S. Pillai, *Probability, Random Variables, and Stochastic Processes*, 4th edn. (McGraw-Hill, 2002)

Publisher's Note