Physical-Layer Security for Ambient Backscattering Internet-of-Things

Basem M. ElHalawany, Ahmad A. Aziz El-Banna, and Kaishun Wu

Abstract The pursuit of tiny computing and sensor devices become a big challenge in the Internet of Things (IoT) era. The process of powering such small-size wireless nodes becomes more difficult as the battery adds extra weight, size, and cost. Additionally, batteries replacement is impractical for the expected massive IoT connectivity especially in inaccessible environments, while recharging is very difficult in multiple scenarios. Ambient backscatter communication (AmBC) solves this problem by leveraging existing radio-frequency transmissions for wirelessly powering battery-free nodes. Due to the limited computational power of such nodes, high-complexity security and authentication protocols are infeasible. Consequently, it is imperative to exploit low-complexity techniques such as physical-layer security (PLS). PLS is a key-less security technique that relies on the randomness of the communication channel between the transceiver nodes for securing the transmitted message. In this work, we consider the PLS of an ambient backscattering IoT (AmBC-IoT) system. In AmBC-IoT system, backscattering IoT devices (BDs) form a symbiotic system, in which the access point (i.e., radio frequency source) supports not only the conventional legacy receiver but also the IoT transmission. Specifically, we derive closed-form expressions for the secrecy outage probability and the ergodic secrecy rate under passive eavesdropping. Additionally, we provide

B. M. ElHalawany · A. A. Aziz El-Banna · K. Wu
Guangdong Laboratory of Artificial Intelligence and Digital Economy (SZ),
Shenzhen University, Shenzhen 518060, China
e-mail: basem.mamdoh@szu.edu.cn

A. A. Aziz El-Banna
e-mail: ahmad.elbanna@feng.bu.edu.eg

B. M. ElHalawany · A. A. Aziz El-Banna
Benha University, Benha, Egypt

K. Wu (✉)
PCL Research Center of Networks and Communications, Peng Cheng Laboratory,
Shenzhen, China
e-mail: wu@szu.edu.cn

F. Jameel and S. A. Hassan (eds.), *Wireless-Powered Backscatter Communications for Internet of Things*, Internet of Things,
https://doi.org/10.1007/978-3-030-46201-7_2

asymptotic analysis for both metrics to gain insights on the effect of different parameters on the performance. The accuracy of the analytical results has been validated by extensive simulations.

1 Introduction

The Internet of Things (IoT) is a major player of the fifth generation (5G) and beyond 5G (B5G) mobile communication networks. IoT is expected to interconnect a massive number of devices for many application areas including smart networks, vehicular networks, environmental monitoring and control [2]. Those interconnected IoT devices varies in design, size, power consumption, and hardware limitations, however, the pursuit of tiny sensor devices is a big trend in the IoT era. The vision to have small-size wireless devices faces many challenges including hardware, computing, battery replacement, and battery size limitations. Consequently, many concepts have been investigated to solve those challenges such as the wireless RF energy harvesting technology, which allows a wireless device to harvest energy from the RF transmissions of another source to charge its battery to avoid depletion and the need of regular replacement. The harvested energy could be used for powering the transceiver circuitry, thus allowing the node to communicate with other entities in the network.

However, this wireless-powered communication technology provides an option for solving battery-replacement, it does not solve the size problem since the wireless node must have its own battery and oscillator circuitry needed for transmission, which usually hinders the process of designing tiny nodes. Another early concept has been investigated to jointly solve the power and size challenges is the RF identification (RFID) communication, which require a dedicated device/source, i.e. the reader, to provide RF power to a tiny battery-less passive, i.e. with no oscillator circuitry, devices known as RFID tags. The basic concept of this RFID systems is the backscattering principle, which allow backscattering devices (BDs) to transmit information by reflecting and modulating incident RF signals by controlling their antennas' reflection coefficients via adapting impedance mismatch and harvesting a fraction of the energy for circuit operations [16]. However, in this traditional backscattering communication systems (BC), also known as bistatic backscatter configuration, the communication process is always initiated by the dedicated reader which limits the widespread use of BC-IoT.

Another step forward in the pursuit of designing tiny wireless nodes is the ambient backscatter communication (AmBC) technology. The idea behind AmBC is to harvest power from the surrounding RF sources such as the cellular base stations, digital television (DTV) transmitters, wireless fidelity (Wi-Fi) access points, and FM radio signals, etc to power the circuits, and to symbiotically modulate the backscattering devices (BDs) messages over the RF source signal [8, 16, 19]. In other words, AmBC technology exploits the surrounding RF signals as both energy resources and signal resources for reflection [7], which in turns reduces the communication system implementation and maintenance costs. Notice that the BDs' signals that are modulated over the ambient signal has a much lower data rate which facilitate their separation at the receivers by averaging or successive interference cancellation (SIC). The backscattering receiver, i.e., reader, in this case can decode and recover the messages without the need to provide wireless power to the tags. Nguyen et al. [12] have focused on finding the optimal energy detector at the receiver side and estimating the corresponding bit error rate for AmBC.

Another interesting point is that the interference caused by the ambient backscatter signal to other legacy wireless device is unnoticeable unless they in close proximity [10] as demonstrated in a real experiment in [10].

Although AmBC has presented itself as a promising candidate for self-sustainable IoT communication systems because of its energy-saving and tiny size features, it leads to another security challenge. Due to the limited computational power of such tiny nodes, high-complexity security and authentication protocols are likely to be infeasible. Consequently, it is vital to design alternative non-computational/ cryptographic based security techniques to protect the confidentiality of messages in AmBC systems. Physical-layer security (PLS) and physical-layer authentication (PLS) are two major security paradigms that rely on the physical properties of the wireless communication channels between two communicating nodes under different scenarios including cooperative relay network, vehicular-to-everything networks, non-orthogonal multiple access, millimeter waves and massive MIMO, etc [4–6].

PLS is a key-less security technique that allow hiding messages from potential eavesdroppers without a shared secret key by relying on the randomness of the communication channel between the transceiver nodes. Consequently, PLS denotes the study of techniques and algorithms that aim at improving the security of networks by exploiting the properties of the physical layer such as noise and fading. In [18], Wyner has laid the foundations of PLS assuming a much noisier eavesdropper's channel with respect to the legitimate receiver. In other words, PLS exploits the difference in quality between legitimate transceiver pair channel and the transmitter-eavesdroppers channel to securely transmit a message from a source to an intended legitimate receiver, which leads to a positive secrecy rate only if the legitimate receiver channel is better than the channel to any eavesdropper. Several research work have been dedicated for investigating the PLS of traditional and ambient backscattering communication (BC and AmBC) [7, 15, 17, 20, 21]. In [7], the authors have proposed a machine learning based antenna design scheme for reducing the side lobs in order to improve the PLS of traditional BC. In [20], a noise-injection precoding strategy is proposed to safe-guard the security in MIMO and MISO BC. In [15], the author proposed a relay selection strategy using artificial noise at the selected relay node for maximizing the positive secrecy rate at the reader. In [21], the authors have proposed a time-division based protocol to enhance the security of data transmission between the multiple tags and the reader in AmBC system.

Despite the significant aforementioned contributions up to now, there is still a gap regarding the theoretical tools for inspecting the performance analysis of different types of backscattering communication. In this chapter, with the objective of evaluating the security performance, closed-form analytical expressions for the secrecy outage probability (SOP) and ergodic secrecy rate (ESR) of an ambient backscatter IoT communications system in the presence of a passive eavesdropper. Furthermore, to gain more insights for the system design, we obtain asymptotic closed-form expressions for the SOP and ESR over Rayleigh fading channels.

2 System Model

We consider a communication scenario where a group of battery-less IoT tags is exploiting the transmission of an ambient radio-frequency source to its legacy receiver by reflecting and modulating incident RF signals to transmit their own messages. The considered ambient backscattering IoT system (AmBC-IoTs) consists of a radio-frequency source (S), N distributed IoT tags, and a reader (R), where the tags transmit their messages on a time-division basis, such that the nth IoT tag transmits for a duration T_n. We investigate the secrecy performance of this AmBC-IoT system in the presence of a passive eavesdropper (E) that overhear the tags' transmissions as shown in Fig. 1. All nodes are equipped with a single antenna, while the channels coefficients are assumed to be independent, identically distributed quasi static with Rayleigh distribution, $\mathcal{CN}(0, \Omega_x)$, where $\Omega_x = PL_o\, d^{-\alpha}$ is the mean power of channel x, PL_o is the path loss constant, d is the transmission distance, and α is the path-loss exponent. We denote f_n, h_n, g_n, f_o, and f_e the channel gains from S to the nth tag, nth tag to the reader, nth tag to the eavesdropper, S to reader, and S to eavesdropper, respectively for $n \in [1, N]$ with mean powers Ω_{fn}, Ω_{hn}, Ω_{gn}, Ω_{fo}, and Ω_{fe}, respectively.

The received signals at the reader (R) and the eavesdropper from the nth tag and the RF source at the nth time slot can be expressed as follow

$$y_R^n(t) = f_o x_o(t) + \sqrt{\beta} f_n h_n x_o(t) c_n(t) + \omega_n(t) \tag{1}$$

$$y_E^n(t) = f_e x_o(t) + \sqrt{\beta} f_n g_n x_o(t) c_n(t) + \omega_e(t), \tag{2}$$

where $x_o(t)$ is the message to the legacy user with $E\left[|x_o(t)|^2\right] = p_o$, β is the reflection coefficient with $0 < \beta < 1$, $c_n(t)$ is the backscatter device (BD) message where $E\left[|c_n(t)|^2\right] = 1$, and $\omega_n(t)$ and $\omega_e(t)$ is the additive white Gaussian noises (AWGN) at both the reader and the eavesdropper, respectively, with zero mean and variance σ^2.

Similar to [9, 11], we assume that SIC is used at both nodes (R and E) to cancel the strong signal of the ambient transmission, consequently the signal-to-interference plus noise ratios (SINRs) at both nodes are given respectively as follows

$$\gamma_{nR} = \rho\, |f_n|^2\, |h_n|^2 \tag{3}$$

$$\gamma_{nE} = \rho\, |f_n|^2\, |g_n|^2\,, \tag{4}$$

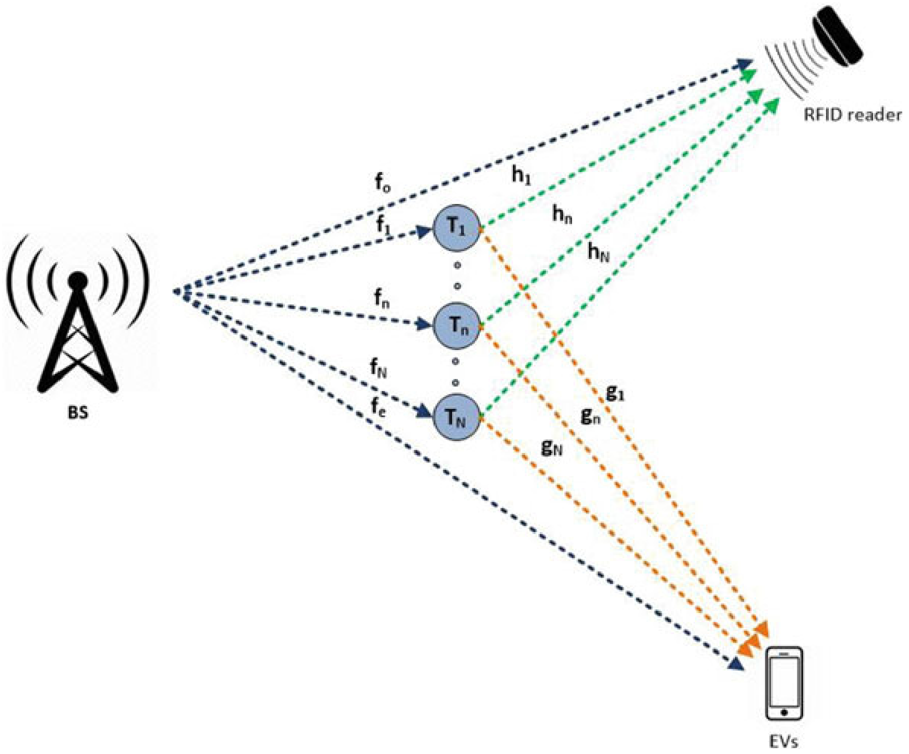

Fig. 1 A typical multi-tag ambient backscatter system under passive eavesdropping

where $\rho = \frac{p_o}{\sigma^2}$ is the transmit SNR of the ambient source. In the next two sections, we derive the SOP and the ergodic secrecy rate of the nth tag.

3 Secrecy Outage Probability (SOP)

The SOP is defined as the probability that the secrecy capacity (C_s^n) achieved by the tag is less than certain threshold value (R_s), where C_s^n is defined as the difference between the achievable capacity of the tag and the eavesdropper, i.e, $C_s^n = C_n - C_e$, where $C_n = T_n \log_2(1 + \gamma_{nR})$ and $C_e = T_n \log_2(1 + \gamma_{nE})$. Consequently, the SOP can be mathematically formulated as follows

$$\begin{aligned} P_s^n &= Pr\left(T_n \, log_2\left(\frac{1+\gamma_{nR}}{1+\gamma_{nE}}\right) < R_s\right) \\ &= Pr\left(\frac{1+\gamma_{nR}}{1+\gamma_{nE}} < \pi_n\right), \end{aligned} \tag{5}$$

where $\pi_n = 2^{R_s/T_n}$. By substituting (3) and (4), the SOP can be reformulated as

$$\begin{aligned} P_s^n &= Pr\left(|f_n|^2\left(|h_n|^2 - \pi_n\,|g_n|^2\right) < \frac{\pi_n - 1}{\rho\beta}\right) \\ &= Pr\left(|f_n|^2\,Y < \frac{\pi_n - 1}{\rho\beta}\right) \\ &= \int_0^\infty F_Y\left(\frac{\pi_n - 1}{\rho\beta\,x}\right) f_{|f_n|^2}(x)dx, \end{aligned} \tag{6}$$

where $Y = |h_n|^2 - \pi_n\,|g_n|^2$, and $f_{|f_n|^2}(x)$ is the probability density function (PDF) of the exponentially distributed random variable $|f_n|^2$ and $F_Y(.)$ is the cumulative distribution function (CDF) of the random variable Y. In order to find the SOP in (6), we need to find the CDF of Y, which can be derived as follows

$$\begin{aligned} F_Y(y) &= Pr\,(Y_1 - Y_2 < y) = Pr\,(Y_1 < Y_2 + y) \\ &= \int_{y_2=0}^\infty \int_{y_1=0}^{y_2+y_1} f_{Y_1}(y_1)\,f_{Y_2}(y_2)\,dy_1\,dy_2 \\ &= 1 - \frac{\Omega_{hn}\,e^{\frac{-y}{\Omega_{hn}}}}{\Omega_{hn} + \pi_n\Omega_{gn}}, \end{aligned} \tag{7}$$

where Y_1 and Y_2 are exponentially distributed random variables with parameters Ω_{hn} and $\pi_n\,\Omega_{gn}$, respectively. By substituting (7) into (6), the SOP can be formulated as follows

$$\begin{aligned} P_s^n &= 1 - \frac{\Omega_{hn}}{\Omega_{fn}(\Omega_{hn} + \pi_n\Omega_{gn})}\int_0^\infty exp\left(-\frac{\mu_o}{x} - \frac{x}{\Omega_{fn}}\right)dx \\ &\overset{(a)}{=} 1 - \frac{(\frac{\Omega_{hn}}{\Omega_{fn}})\sqrt{4\mu_o\Omega_{fn}}}{\Omega_{hn} + \pi_n\Omega_{gn}} K_1\left(\sqrt{\frac{4\mu_o}{\Omega_{fn}}}\right), \end{aligned} \tag{8}$$

where $\mu_o = \frac{\pi_n - 1}{\rho\,\beta\,\Omega_{hn}}$, K_1 is the Bessel function, and (a) follows from [14, Eq. (3.324.1)].

4 Ergodic Secrecy Rate (ESR)

For the sake of analyzing the time-varying security features of the wireless channels, we need to evaluate the average secrecy transmission rate which can be found be averaging over wireless fading channels. Consequently, the ergodic secrecy rate can be mathematically formulated as the expectation of the non-negative secrecy capacity follows

$$\begin{aligned} ESR &= E\left\{\left[C_n^s\right]^+\right\} = E\left\{[C_n - C_{en}]^+\right\} \\ &\geqslant [E\{C_n\} - E\{C_{en}\}]^+ \end{aligned} \tag{9}$$

where the lower bound can be expressed as $ESR_{LB} = E\{C_n\} - E\{C_{en}\}$. In the following we derive the expectation of both C_n and C_{ne} over Rayleigh fading channels as follows

$$E\{C_n\} = \frac{T_n}{\ln(2)} E\{\ln(1+\gamma_{nR})\} = \frac{T_n}{\ln(2)} \int_0^\infty \frac{1-F_{\gamma_{nR}}(x)}{1+x} dx \tag{10}$$

where $F_{\gamma_{nR}}(x)$ is the CDF of γ_{nR}, which can be derived as follows

$$\begin{aligned} F_{\gamma_{nR}}(x) &= Pr\left(|h_n|^2\,|f_n|^2 < \frac{x}{\rho\beta}\right) \\ &= \int_{w_1=0}^{\infty} \int_{w_2=0}^{\frac{x}{\rho\beta w_1}} f_{|h_n|^2}(w_2)\, f_{|f_n|^2}(w_1)\, dw_1\, dw_2 \\ &\overset{(b)}{=} 1 - \sqrt{\frac{4x}{\rho\,\beta\,\Omega_{hn}\,\Omega_{fn}}}\, K_1\left(\sqrt{\frac{4x}{\rho\,\beta\,\Omega_{hn}\,\Omega_{fn}}}\right) \end{aligned} \tag{11}$$

where $\mu_1 = \frac{4}{\rho\,\beta\,\Omega_{hn}\,\Omega_{fn}}$, $f_{|h_n|^2}(.)$ and $f_{|f_n|^2}(.)$ are the PDFs of the exponentially distributed random variables $|h_n|^2$ and $|f_n|^2$, respectively, and (b) follows from [14, Eqs. (3.324.1)]. By substituting (11) into (10), $E\{C_n\}$ can be reformulated as follows

$$\begin{aligned} E\{C_n\} &= \frac{T_n}{\ln(2)} \int_0^\infty \frac{\sqrt{\mu_1 x}\; K_1\left(\sqrt{\mu_1 x}\right)}{1+x}\, dx \\ &= \frac{T_n\sqrt{\mu_1}}{\ln(2)} \int_0^\infty x^{\frac{1}{2}} (1+x)^{-1}\, K_1\left(\sqrt{\mu_1 x}\right) dx \end{aligned} \tag{12}$$

Notice that the integration in (12) has no closed-form expression in terms of elementary functions. However, the integrands of (12) can be expressed in terms of Meijer's G-functions relying on [1, Eqs. (10,14)] as follows

$$E\{C_n\} = \frac{T_n\sqrt{\mu_1}}{2\;\ln(2)} \int_0^\infty x^{\frac{1}{2}}\, G_{1,\,1}^{1,\,1}\left({0 \atop 0}\middle| x\right)\, G_{0,\,2}^{2,\,0}\left({- \atop \frac{1}{2},-\frac{1}{2}}\middle|\frac{\mu_1 x}{4}\right) dx \tag{13}$$

where the integration in (13) can be solved using [1, Eq. (21)] as follows

$$E\{C_n\} = \frac{T_n}{\ln(2)}\, G_{1,\,3}^{3,\,1}\left({0 \atop 0,0,1}\middle|\frac{\mu_1}{4}\right) \tag{14}$$

By using similar approach, we could derive the CDF $F_{\gamma_{nE}}(x) = 1 - \sqrt{\mu_2 x} K_1(\sqrt{\mu_2 x})$, then the C_{ne} can be expressed as follows

$$E\{C_{ne}\} = \frac{T_n}{\ln(2)}\, G_{1,\,3}^{3,\,1}\left({0 \atop 0,0,1}\middle|\frac{\mu_2}{4}\right) \tag{15}$$

where $\mu_2 = \frac{4}{\rho\ \beta\ \Omega_{gn}\ \Omega_{fn}}$. By substituting (14) and (15), the lower bound of the ESR can be expressed as follows

$$ESR_{LB} = \frac{T_n}{\ln(2)} \left(G^{\,3,\,1}_{\,1,\,3}\left({}^{\;\;0}_{0,0,1} \middle| \frac{\mu_1}{4} \right) - G^{\,3,\,1}_{\,1,\,3}\left({}^{\;\;0}_{0,0,1} \middle| \frac{\mu_2}{4} \right) \right) \tag{16}$$

5 Asymptotic Performance Analysis

Since the expressions of the SOP and the ESR are given in terms of the Bessel and Meijer's G-functions, for the sake of providing more insights on the effect of different parameters, the asymptotic SOP and ESR are developed in this section using the residue theorem and [3]. The asymptotic values of the Meijer's G-functions at high SNR ($\rho \to \infty$) can be found by evaluating the residue of the integrands at the closest poles to the contour of Mellin-Barness integral [13].

5.1 Asymptotic SOP

By transforming the Bessel function into an equivalent meijer G-function using [1, Eq. (14)], we can express the SOP as follows

$$P_s^n = 1 - \Psi_n \rho^{-\frac{1}{2}}\, G^{\,2,\,0}_{\,0,\,2}\left({}^{\quad -}_{\frac{1}{2},-\frac{1}{2}} \middle| \frac{\mu_o}{\Omega_{fn}} \right) \tag{17}$$

where

$$\Psi_n = \frac{2}{(\Omega_{hn} + \pi_n \Omega_{gn})} \sqrt{\frac{(\pi_n - 1)\Omega_{hn}}{\beta\ \Omega_{fn}}} \tag{18}$$

By applying the residue theorem on (17), where asymptotic value of the meijer G-function equals to the negative of the residue at the smallest pole on the right of the contour of Mellin-Barness integral since $\frac{\mu_o}{\Omega_{fn}} \to 0$ as $\rho \to \infty$. Since the closest pole to the contour in this case is a first order pole at $S = 0.5$, the asymptotic value of the G-function in (17) can be expressed as follows

$$\begin{aligned} G_o^{\infty} &= -Res\left[\Gamma(0.5 - s)\ \Gamma(-0.5 - s)\ \left(\frac{\mu_o}{\Omega_{fn}} \right)^s, 0.5 \right] \\ &= \left(\frac{\pi_n - 1}{\beta\ \Omega_{fn}^2\ \rho} \right)^{-\frac{1}{2}} \end{aligned} \tag{19}$$

where $\Gamma(.)$ is the Gamma function [14, Eqs. (3.310.1)] and $Res[f, S_o]$ is the residue of a function (f) at the pole S_o. By substituting (19) into (17), the asymptotic expression of the SOP can be expressed as follows

$$P_s^{n,\infty} = 1 - \frac{\Omega_{hn}}{\Omega_{hn} + \pi_n\ \Omega_{gn}} \tag{20}$$

and consequently the diversity order can be derived as follows

$$d_n = -\lim_{\rho\to\infty} \frac{\log(P_s^{n,\infty})}{\log \rho} = 0 \tag{21}$$

5.2 *Asymptotic ESR*

By applying the residue theorem to (16), we can find the negative of residue at the smallest pole on the right, which is a second order pole $S = 0$. Knowing that the residue of f_i at a K-order pole S_o is given as $\frac{1}{(K-1)!}\lim_{S\to S_o}\frac{d^{K-1}}{d_S^{K-1}}\left((S-S_o)^K\ f_i\right)$, the asymptotic values of the two G-functions in (16) are given as $G_i^{\infty} = 2\gamma + \ln(Z_i)$, where $i \in \{1, 2\}$, $Z_i = \frac{\mu_i}{4}$, $f = \Gamma^2(-s)\ \Gamma(1-s)\ \Gamma(1+s)\ Z_i^s$, and γ is the Euler-Macheroni constant [14, Eqs. (8.367.1)]. By substituting G_1^{∞} and G_2^{∞} into (16), the asymptotic ESR can be expressed as follows

$$\begin{aligned} ESR_{LB}^{\infty} &\approx \frac{T_n}{\ln(2)} ln\left(\frac{\mu_2}{\mu_1}\right) \\ &\approx \frac{T_n}{ln(2)} \ln\left(\frac{\Omega_{hn}}{\Omega_{gn}}\right) \end{aligned} \tag{22}$$

6 Results and Discussions

In this section, representative numerical results are presented to illustrate the derived performance metrics, based on which some insights are highlighted. Monte Carlo simulations are generated to corroborate the proposed analysis. Unless mentioned otherwise, the simulation parameters used for generating the plots are as follows: the channels mean powers are $\Omega_{fn} = 2,\ \Omega_{hn} = 5,\ \Omega_{gn} = [0.1,\ 1],\ \Omega_{fo} = 1,\ \Omega_{fe} = 1$, a normalized system bandwidth of 1 Hz, the secrecy rate threshold $R_s = 0.01$ bits per channel use, and the tag reflection Coefficient $B = [0.5,\ 0.7]$.

Figure 2 plots the secrecy outage probability of the nth tag as a function of ρ for two different reflection coefficient (B) and two different mean powers for the tag-to-eavesdropper channel (Ω_{gn}) given a fixed mean power for the tag-to-reader channel mean power (Ω_{hn}). The simulation results show the improvement of the SOP with

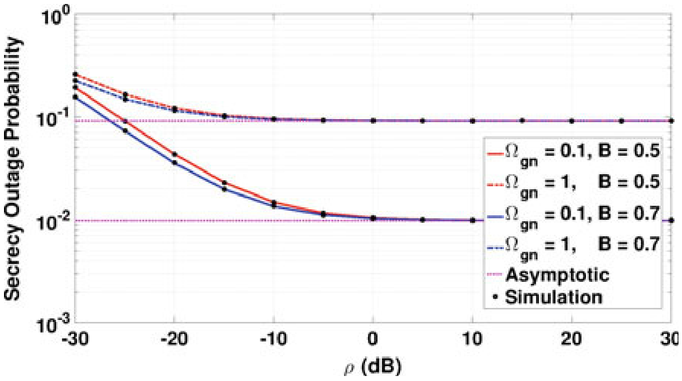

Fig. 2 The SOP as a function of the transmit SNR (ρ) for $\Omega_{fn} = 2,\ \Omega_{hn} = 5,\ \Omega_{fo} = 1$, and $\Omega_{fe} = 1$

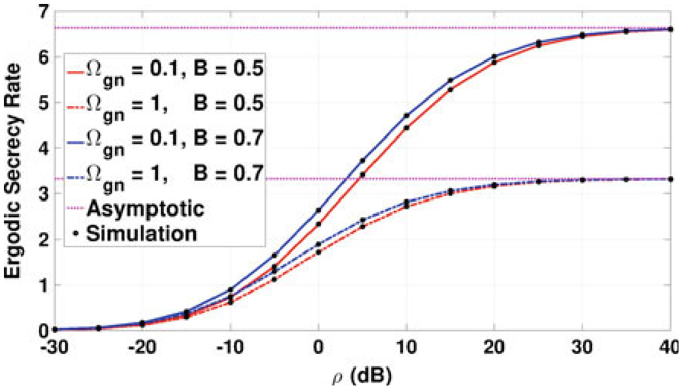

Fig. 3 The ESR as a function of the transmit SNR (ρ) for $\Omega_{fn} = 2,\ \Omega_{hn} = 5,\ \Omega_{fo} = 1$, and $\Omega_{fe} = 1$

the increase of ρ. However, we can see that for all cases, there is a floor for the SOP that depends on the value of Ω_{gn} (since we assume a fixed value of Ω_{hn}). Notice also the effect of the reflection coefficient (B) on the SOP, where the increase in B improves the SOP.

Figure 3 plots ergodic secrecy rate as a function of ρ for the same parameter settings as Fig. 2. The results show an improvement in the achievable ESR with the increase of the reflection coefficient due to the improvement of the SNR. However, we can acquire a higher improvement in the ESR when the eavesdropper channel (i.e., when $\Omega_{gn} = 0.1$) is much weaker than the reader channel similar to the improvement in SOP in Fig. 2. Notice also that the ESR is much higher when the eavesdropper channel is weak. The asymptotic behavior of the ESR show a ceiling at high SNR (i.e., $\rho \to \infty$), where the ESR saturates at the value derived in (22).

In addition, the analytical results closely follow the simulation results, which corroborates the analysis and the derivation of both SOP and ESR. Notice that the asymptotic ESR and SOP perfectly match the analytical results starting from 0 dB up to high SNR and saturates at different values for all cases. The saturation level of the ESR is inversely proportional to the logarithm of Ω_{gn}, which confirms the asymptotic analytical results in (22). On the other hand, we can see that the saturation level of the SOP is directly proportional with Ω_{gn}, which means that having a lower Ω_{gn} leads to a better SOP, which also coincides with the asymptotic results in (20).

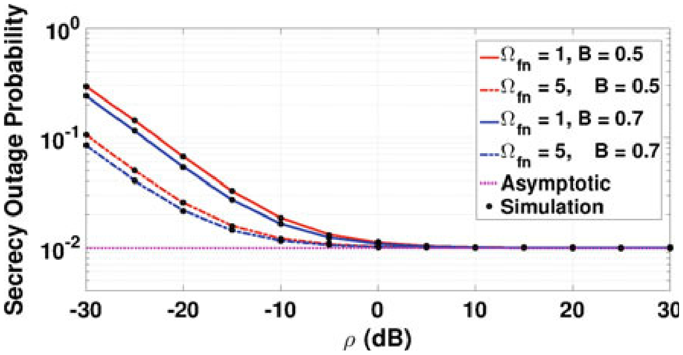

Fig. 4 The SOP as a function of the transmit SNR (ρ) for $\Omega_{gn} = 0.1$, $\Omega_{hn} = 5,\ \Omega_{fo} = 1$, and $\Omega_{fe} = 1$

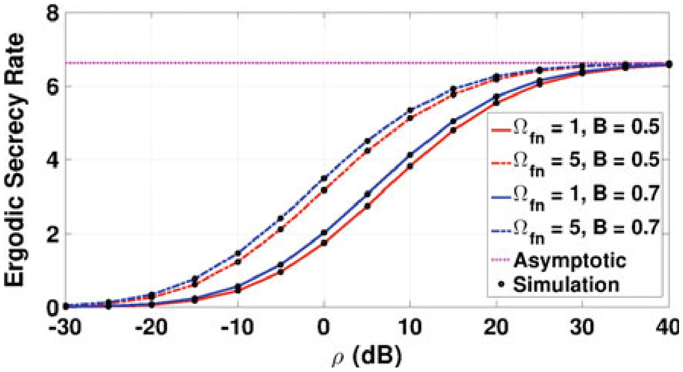

Fig. 5 The ESR as a function of the transmit SNR (ρ) for $\Omega_{gn} = 0.1$, $\Omega_{hn} = 5,\ \Omega_{fo} = 1$, and $\Omega_{fe} = 1$

Figures 4 and 5 plot the SOP and ESR versus ρ similar to Fig. 2 and Fig. 3, respectively, however, we fix both $\Omega_{gn} = 0.1$ and $\Omega_{hn} = 5$, while we change the values of B and the mean power of the source-to-tag channel, i.e., $\Omega_{fn} = [1,\ 5]$. The results show that increasing the channel mean power improves both SOP and ESR since this means that the tag is closer to the RF power source. Notice that the saturation levels (i.e., the ceiling of the ESR and the floor of the SOP) are constant for all scenarios since the asymptotic expressions of both SOP and ESR do not depend on Ω_{fn} or B as shown in (20) and (22).

7 Conclusion

Being motivated by investigating the interplay between physical-layer security and ambient backscattering systems, we studied the physical layer security of an ambient backscattering IoT system where battery-less IoT tags are communicating with a reader in the presence of a passive eavesdropper. Closed-form expression of the secrecy outage probability and ergodic secrecy rate are derived to investigate the performance of different parameters. The results shows that both SOP and ESR improves when the eavesdropper channel is weaker than the reader channel. Extensive simulations were conducted to verify the correctness of the analytical derivations. As a future extension, we intend to derive the system SOP and ESR taking into consideration the worst-case IoT tag.

Acknowledgments This research was supported in part by the China NSFC Grant (61872248, U1736207), Guangdong NSF 2017A030312008, Fok Ying-Tong Education Foundation for Young Teachers in the Higher Education Institutions of China (Grant No.161064), GDUPS (2015), and Shenzhen Science and Technology Foundation (No. ZDSYS20190902092853047). The research is partially supported by Benha University, Egypt research fund (Project 2/1/14).

References

1. Adamchik, V.S., Marichev, O.I.: The algorithm for calculating integrals of hypergeometric type functions and its realization in reduce system. In: Proceedings of the International Symposium on Symbolic and Algebraic Computation, ISSAC '90, pp. 212–224. ACM, New York, NY, USA (1990)
2. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of Things: a survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutor. **17**(4), 2347–2376 (2015)
3. Chergui, H., Benjillali, M., Saoudi, S.: Performance analysis of project-and-forward relaying in mixed MIMO-pinhole and Rayleigh dual-hop channel. IEEE Commun. Lett. **20**(3), 610–613 (2016)
4. ElHalawany, B.M., El-Banna, A.A., Wu, K.: Physical-layer security and privacy for vehicle-to-everything. IEEE Commun. Mag. (2019) (Forthcoming)
5. ElHalawany, B.M., Ruby, R., Riihonen, T., Wu, K.: Performance of cooperative NOMA systems under passive eavesdropping. In: 2018 IEEE Global Communications Conference (GLOBECOM), pp. 1–6 (2018)
6. ElHalawany, B.M., Wu, K.: Physical-layer security of NOMA systems under untrusted users. In: 2018 IEEE Global Communications Conference (GLOBECOM), pp. 1–6 (2018)
7. Hong, T., Liu, C., Kadoch, M.: Machine learning based antenna design for physical layer security in ambient backscatter communications. Wirel. Commun. Mob. Comput. **2019**(14870656), 10 (2019)
8. Jameel, F., Ristaniemi, T., Khan, I., Lee, B.M.: Simultaneous harvest-and-transmit ambient backscatter communications under rayleigh fading. EURASIP J. Wirel. Commun. Netw. **2019**(1), 166 (2019)
9. Kang, X., Liang, Y., Yang, J.: Riding on the primary: a new spectrum sharing paradigm for wireless-powered IoT devices. In: 2017 IEEE International Conference on Communications (ICC), pp. 1–6 (2017)
10. Lu, X., Niyato, D., Jiang, H., Kim, D.I., Xiao, Y., Han, Z.: Ambient backscatter assisted wireless powered communications. IEEE Wirel. Commun. **25**(2), 170–177 (2018)
11. Lyu, B., You, C., Yang, Z., Gui, G.: The optimal control policy for RF-powered backscatter communication networks. IEEE Trans. Veh. Technol. **67**(3), 2804–2808 (2018)
12. Nguyen, T.L.N., Shin, Y., Kim, J., Kim, D.: Signal detection for ambient backscatter communication with OFDM carriers. Sensors **19**(3), 517 (2019)
13. Capelas de Oliveira, E.: Special Functions, pp. 17–67. Springer International Publishing, Cham (2019)
14. Ryzhik, I., Gradshteyn, I.: Table of Integrals, Series, and Products, 7th edn. Academic Press (2007)
15. Song, H., Gao, Y., Sha, N., Zhou, Q., Yao, F.: A distinctive method to improve the security capacity of backscatter wireless system. In: 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), pp. 272–276 (2017)
16. Van Huynh, N., Hoang, D.T., Lu, X., Niyato, D., Wang, P., Kim, D.I.: Ambient backscatter communications: a contemporary survey. IEEE Commun. Surv. Tutor. **20**(4), 2889–2922 (2018)
17. Wang, N., Wang, P., Alipour-Fanid, A., Jiao, L., Zeng, K.: Physical layer security of 5G wireless networks for IoT: challenges and opportunities. IEEE Internet of Things J. 1 (2019)

18. Wyner, A.D.: The wire-tap channel. Bell Syst. Tech. J. **45**(8), 1355–1387 (1975)
19. Xu, C., Yang, L., Zhang, P.: Practical backscatter communication systems for battery-free Internet of Things: a tutorial and survey of recent research. IEEE Signal Proces. Mag. **35**(5), 16–27 (2018)
20. Yang, Q., Wang, H., Zhang, Y., Han, Z.: Physical layer security in MIMO backscatter wireless systems. IEEE Trans. Wirel. Commun. **15**(11), 7547–7560 (2016)
21. You, J., Wang, G., Zhong, Z.: Physical layer security-enhancing transmission protocol against eavesdropping for ambient backscatter communication system. In: 6th International Conference on Wireless, Mobile and Multi-media (ICWMMN 2015), pp. 43–47 (2015)