Bulletin of Electrical Engineering and Informatics
Vol. 11, No. 6, December 2022, pp. 3353~3360
ISSN: 2302-9285, DOI: 10.11591/eei.v11i6.3981

Secrecy capacity analysis of bi-static backscatter communication systems

Phung Ton That[1], Duy-Hung Ha[2], Hong-Nhu Nguyen[3]
[1]Faculty of Electronics Technology, Industrial University of Ho Chi Minh City (IUH), Ho Chi Minh City, Vietnam
[2]Wireless Communications Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University (TDTU), Ho Chi Minh City, Vietnam
[3]Faculty of Electronics and Telecommunications, Saigon University (SGU), Ho Chi Minh City, Vietnam

Article Info

Article history:

Received Apr 19, 2022
Revised Aug 5, 2022
Accepted Aug 30, 2022

Keywords:

Backscatter communication
Bi-static architecture
Ergodic secrecy capacity
Strictly positive secrecy capacity

ABSTRACT

The rapid adoption of battery-free internet-of-things (IoT) sensors in multiple environments ranging from agriculture to wildlife surveillance, has seen increased research interest in backscatter communication (BSC) technology. BSC is viewed as a potential technology to enable the further spread of sustainable battery-free IoT applications in environments and scenarios where bulkier-sized battery-powered IoT devices would be unsuitable. In this study, we investigate the secrecy capacity of a bi-static BSC network in the presence of a malicious eavesdropper. The proposed BSC system consists of a reader, multiple backscatter devices, and an eavesdropper. We derive closed-form strictly positive secrecy capacity (SPSC) expressions and ergodic secrecy capacity (ESC) expressions for the BSC reader. Monte Carlo simulations verify the exact capacity expressions.

Corresponding Author:

Duy-Hung Ha
Wireless Communications Research Group, Faculty of Electrical and Electronics Engineering
Ton Duc Thang University
Ho Chi Minh City, Vietnam
Email: haduyhung@tdtu.edu.vn

1. INTRODUCTION

The rapid adoption and proliferation of internet-of-things (IoT) in scenarios and environments ranging from infrastructure monitoring (such as bridges, roads, and pipelines) to implanted health-care monitoring, has driven backscatter communication (BSC) research [1]. BSC devices enable the design and deployment of sustainable ultra-low-power IoT solutions into scenarios unsuitable for bulkier battery-powered IoT devices such as inside the human body for healthcare monitoring [2]. Research by Jang *et al*. [3] define a backscatter tag as a device that reflects nearby transmitter excitation signals and then selectively amplifies, or modifies the phase, and/or frequency of the signal for modulation. A nearby receiver captures the backscattered signal and extracts the information injected by the tag. There are three types of BSC architectures, which are [2]-[4]: i) monostatic: the reader utilizes the same antenna as an emitter and receiver, to receive signals from the backscatter sensors; ii) Bi-static: here, the transmitter and receiver are not located on the same device. But are separated apart geographically. This architecture is suitable for long-range transmissions; iii) ambient: the transmitter scatters radio frequency (RF) signals over a short-range and the reader receives and decodes the backscattered signals from the tags [5]-[8].

The monostatic model is the cheapest of the three to design since they require fewer antenna elements, however, in this paper, we prefer the bi-static model to explain in the consistently following section. Various recent works have focused on secure communications for BSC. In [9]-[12] proposed a physical layer security (PLS) solution over an alternative to application layer security by cryptography. As cryptography is computationally complex for existing radio frequency identification (RFID) systems. Which are also another example of BSC systems. The authors obtained asymptotic closed-form secrecy outage probability (SOP) expressions for their proposed system operating in correlated Rayleigh fading conditions. Song *et al*. [13], studied PLS with artificial noise (AN) utilized to decrease the signal-to-noise interference noise (SINR) of the eavesdropper. PLS was investigated for ambient BSC systems with multiple tags, the authors derived exact detection rates for the eavesdropper and the reader [14], [15]. Motivated by these recent ideas in securing BSC systems, we add the following contributions to the growing field of BSC security: we derive exact strictly positive secrecy capacity (SPSC) expressions as well as ergodic secrecy capacity expressions (ESC) for the backscatter communication reader with channel gain following Rayleigh distribution and we also present performance curves demonstrating the improvement of secrecy capacity at the reader. All closed-form expressions are verified by Monte Carlo simulations.

The remainder of this paper is as follows. In section 2, we describe the bi-static backscatter communication system located in the vicinity of an eavesdropper. Then, section 3 describes our closed-form equations SPSC expressions. In section 4, we derive the ESC expressions, followed by a discussion of our findings in section 5 and a summary in section 6.

2. BI-STATIC BACKSCATTER COMMUNICATION SYSTEM MODEL

In this study, we evaluate the secrecy capacity performance of a multiple backscatter devices (BDs) system, which consists of a reader, K BDs, and a nearby located eavesdropper, as illustrative in Figure 1. We define p_k, q_k and g_k as the channel gains from the transmitter antenna at the reader to the *k-th* BD, the *k-th* BD to the receive antenna at the reader, and the *k-th* BD to the eavesdropper, respectively. We assume that all the channel gains over Rayleigh fading distribution [11], i.e., $p_k \sim CN(0, \lambda_p)$, $q_k \sim CN(0, \lambda_q)$, and $g_k \sim CN(0, \lambda_g)$.

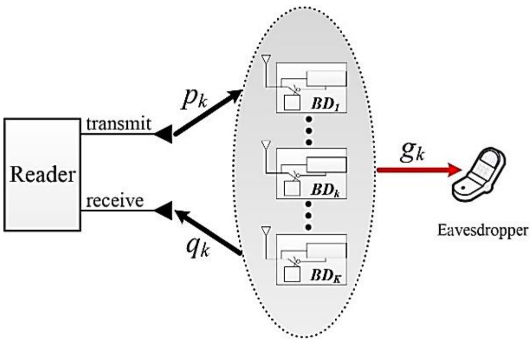

Figure 1. Insecure bi-static backscatter communication

As multiple BDs form a group, the best BD is selected before transmitting. The BD selection strategy is expressed as [3]:

$$k^* = arg \max_{0 \le k \le K} |\bar{Z}_k|^2, \bar{Z} \in \{p, q, g\}. \quad (1)$$

The received signal at the reader from the *k-th* BD is written as [12]:

$$\bar{y}_{R_k} = \sqrt{P_S} p_k q_k s x + \bar{\omega}_k, \quad (2)$$

where P_S is the reader transmitter power, s is the reader query signal, x is the BD information signal, and $\bar{\omega}_k$ is the additive white Gaussian noise (AWGN) in which $\bar{\omega}_k \sim CN(0, N_0)$. Due to the architecture of the backscatter system [16], p_k and q_k are correlated. On the other hand, in the bi-static system, p_k, and q_k channels are considered partially interested [17]. In reality, bi-static architecture is preferred to the monostatic system. Therefore, in this paper, we assume the proposed system is bi-static. In another case, at the eavesdropper, we calculate the intercepted signal from the *k-th* BD can be written as:

$$\bar{y}_{E_k} = \sqrt{P_E} p_k g_k s x + \bar{\omega}_{E_k}, \quad (3)$$

where P_E is the transmit power of the eavesdropper, g_k denotes the channels gain from the BD to the eavesdropper, $\bar{\omega}_{E_k}$ and is the AWGN at eavesdropper with $\bar{\omega}_{E_k} \sim CN(0, N_0)$. From (1)-(3), we calculate the received instantaneous signal-to-noise-ratios (SNRs) at the reader and the eavesdropper as:

$$\bar{\gamma}_{R_{k^*}} \triangleq \frac{P_S |p_{k^*}|^2 |q_{k^*}|^2}{N_0} = \rho_S |p_{k^*}|^2 |q_{k^*}|^2, \quad (4)$$

$$\bar{\gamma}_{E_{k^*}} \triangleq \frac{P_E |p_{k^*}|^2 |g_{k^*}|^2}{N_0} = \rho_E |p_{k^*}|^2 |g_{k^*}|^2, \quad (5)$$

where $\rho_S = \frac{P_S}{N_0}$ and $\rho_E = \frac{P_E}{N_0}$ are the transmit SNR. We can see, from (4) and (5), the channel capacity of the reader and capacity of the eavesdropper's channels can be present as:

$$C_{R_{k^*}} = log_2\left(1 + \bar{\gamma}_{R_{k^*}}\right), \quad (6)$$

and

$$C_{E_{k^*}} = log_2\left(1 + \bar{\gamma}_{E_{k^*}}\right) \quad (7)$$

Using (6) and (7), we can express the immediate secrecy capacity of the reader system as [18]:

$$\overline{C}_S = \left[C_{R_{k^*}} - C_{E_{k^*}}\right]^+ = \begin{cases} \left[\log_2\left(\frac{1+\bar{\gamma}_{R_{k^*}}}{1+\bar{\gamma}_{E_{k^*}}}\right)\right]^+, & if \quad \bar{\gamma}_{R_{k^*}} \geq \bar{\gamma}_{E_{k^*}} \\ 0, & otherwise \end{cases}, \quad (8)$$

where $[x]^+ = max(x, 0)$.

3. STRICTLY POSITIVE SECRECY CAPACITY ANALYSIS

3.1. The channel models

Let us start with the Rayleigh fading channel, the probability-density-functions (PDF) and cumulative-distribution-functions (CDF) of p, q, and g are given by [19].

$$f_{|p|^2}(x) = \frac{1}{\lambda_p} e^{-\frac{x}{\lambda_p}}, \quad (9)$$

$$f_{|q|^2}(y) = \frac{1}{\lambda_q} e^{-\frac{y}{\lambda_q}}, \quad (10)$$

$$f_{|g|^2}(z) = \frac{1}{\lambda_g} e^{-\frac{z}{\lambda_g}}, \quad (11)$$

and

$$F_{|p|^2}(x) = 1 - e^{-\frac{x}{\lambda_p}}, \quad (12)$$

$$F_{|q|^2}(y) = 1 - e^{-\frac{y}{\lambda_q}}, \quad (13)$$

$$F_{|g|^2}(z) = 1 - e^{-\frac{z}{\lambda_g}}, \quad (14)$$

further, we have random variables (RVs) $f_{|\bar{Z}_{k^*}|^2}(x)$ as exponential distributions which $\bar{Z} \in \{p, q, g\}$, are then $f_{|\bar{Z}_{k^*}|^2}(x)$ to presented following [20]:

$$f_{|Z_{k^*}|^2} = \sum_{k=1}^{K} \frac{k\Upsilon(K,k)}{\lambda_Z} e^{-\frac{k}{\lambda_Z}x}, \quad (15)$$

where $\Upsilon(K,k) = \frac{(-1)^{k-1}K!}{k!(K-k)!}$.

3.2. SPSC of reader

From (6)-(8), the SPSC for decode and forward (DF) case can be expressed as [21]:

$$\begin{aligned} S &= \Pr\left(\overline{C}_S > 0\right) = \Pr\left(\log_2\left(\frac{1+\overline{\gamma}_{R_{k^*}}}{1+\overline{\gamma}_{E_{k^*}}}\right) > 0\right) = \Pr\left(\overline{\gamma}_{R_{k^*}} > \overline{\gamma}_{E_{k^*}}\right) \\ &= \Pr\left(\left|p_{k^*}\right|^2\left|q_{k^*}\right|^2 > \frac{\rho_E}{\rho_S}\left|p_{k^*}\right|^2\left|g_{k^*}\right|^2\right) = \Pr\left(\left|q_{k^*}\right|^2 > \frac{\rho_E}{\rho_S}\left|g_{k^*}\right|^2\right) = \int_0^{+\infty} f_{\left|g_{k^*}\right|^2}(x)\int_{\frac{\rho_E}{\rho_S}x}^{+\infty} f_{\left|q_{k^*}\right|^2}(y)\,dxdy. \end{aligned} \tag{16}$$

Proposition 1: the closed-form expression of SPSC to the reader is written as:

$$S = \sum_{k_2=1}^{K}\sum_{k_3=1}^{K}\frac{k_2\rho_S\lambda_q\Upsilon(K,k_2)\Upsilon(K,k_3)}{(k_2\rho_S\lambda_q+k_3\rho_E\lambda_g)}. \tag{17}$$

Proof 1: from (16) we use PDF of (15), S is expanded as (18):

$$\begin{aligned} S &= \int_0^{+\infty} f_{|g_{k^*}|^2}(x)\int_{\frac{\rho_E}{\rho_S}x}^{+\infty} f_{|q_{k^*}|^2}(y)dxdy = \sum_{k_2=1}^{K}\sum_{k_3=1}^{K}\frac{k_2k_3\Upsilon(K,k_2)\Upsilon(K,k_3)}{\lambda_g\lambda_q}\int_0^{+\infty} e^{-\frac{k_2}{\lambda_g}x}\int_{\frac{\rho_E}{\rho_S}x}^{+\infty} e^{-\frac{k_3}{\lambda_q}y}\,dxdy \\ &= \sum_{k_2=1}^{K}\sum_{k_3=1}^{K}\frac{k_2\Upsilon(K,k_2)\Upsilon(K,k_3)}{\lambda_g}\int_0^{+\infty} e^{-x\left(\frac{k_2}{\lambda_g}+\frac{\rho_E k_3}{\rho_S\lambda_q}\right)}dx. \end{aligned} \tag{18}$$

finally, we have SPSC of the system as shown in:

$$S = \sum_{k_2=1}^{K}\sum_{k_3=1}^{K}\frac{k_2\rho_S\lambda_q\Upsilon(K,k_2)\Upsilon(K,k_3)}{(k_2\rho_S\lambda_q+k_3\rho_E\lambda_g)}. \tag{19}$$

based on the aforementioned results, *Proof 1* is complete.

4. ERGODIC SECRECY CAPACITY ANALYSIS

The exact closed-form expressions for ESC are derived by [22], (4).

$$\bar{C}_S = \left[\underbrace{\left\{C_{R_{k^*}}\right\}}_{A_1} - \underbrace{\left\{C_{E_{k^*}}\right\}}_{A_2}\right]^+, \tag{20}$$

where {•} denotes expectation operation.

Proposition 2: the closed-form expression of ESC to the reader is written by:

$$\overline{C}_S = \left[\sum_{k_1=1}^{K}\sum_{k_2=1}^{K}\frac{\Upsilon(K,k_1)\Upsilon(K,k_2)}{ln\,2}G_{1,3}^{3,1}\left(\frac{k_2k_1}{\rho_S\lambda_p\lambda_o}\middle|\begin{matrix}0\\0,1,0\end{matrix}\right) - \sum_{k_3=1}^{K}\sum_{k_4=1}^{K}\frac{\Upsilon(K,k_3)\Upsilon(K,k_4)}{ln\,2}n \times G_{1,3}^{3,1}\left(\frac{k_3k_4}{\rho_E\lambda_p\lambda_g}\middle|\begin{matrix}0\\0,1,0\end{matrix}\right)\right]^+ \tag{21}$$

Proof 2: first, we can calculate A_1 as follows:

$$A_1 = \left\{C_{R_{k^*}}\right\} = \left\{\log_2\left(1+\overline{\gamma}_{R_{k^*}}\right)\right\} = \left\{\log_2\left(1+\rho_S\left|p_{k^*}\right|^2\left|q_{k^*}\right|^2\right)\right\} = \frac{1}{\ln 2}\int_0^{+\infty}\frac{1}{1+x}\left[1-F_{\left|p_{k^*}\right|^2\left|q_{k^*}\right|^2}\left(\frac{x}{\rho_S}\right)\right]dx. \tag{22}$$

we have $F_{|p_{k^*}|^2|q_{k^*}|^2}(x)$ is calculated as:

$$F_{|p_{k^*}|^2|q_{k^*}|^2}\left(\frac{x}{\rho_S}\right) = Pr\left(|p_{k^*}|^2 < \frac{x}{|q_{k^*}|^2\rho_S}\right) = \int_0^{+\infty} f_{|q_{k^*}|^2}(y)\int_0^{\frac{x}{\rho_S y}} f_{|p_{k^*}|^2}(z)dydz$$

$$= \sum_{k_1=1}^{K}\sum_{k_2=1}^{K} \Upsilon(K,k_1)\,\Upsilon(K,k_2)\frac{k_1k_2}{\lambda_q\lambda_p}\int_0^{+\infty} e^{-\frac{k_1}{\lambda_q}y}\int^{\frac{x}{\rho_S y}} e^{-\frac{k_2}{\lambda_p}z}\,dyd$$

$$= \sum_{k_1=1}^{K}\sum_{k_2=1}^{K} \Upsilon(K,k_1)\,\Upsilon(K,k_2)\frac{k_1}{\lambda_q}\int_0^{+\infty} e^{-\frac{k_1}{\lambda_q}y}\left(1-e^{-\frac{k_2x}{\rho_S\lambda_p y}}\right)dy \tag{23}$$

$$= \sum_{k_1=1}^{K}\sum_{k_2=1}^{K} \Upsilon(K,k_1)\,\Upsilon(K,k_2)\left(\frac{k_1}{\lambda_q}\int_0^{+\infty} e^{-\frac{k_1}{\lambda_q}y} - \frac{k_1}{\lambda_q}\int_0^{+\infty} e^{-\frac{k_1 y}{\lambda_q}} e^{-\frac{k_2x}{\rho_S\lambda_p y}}\right)dy$$

$$= \sum_{k_1=1}^{K}\sum_{k_2=1}^{K} \Upsilon(K,k_1)\,\Upsilon(K,k_2)\left(1-\frac{k_1}{\lambda_q}\int_0^{+\infty} e^{-\frac{k_1y}{\lambda_q}-\frac{k_2x}{\rho_S\lambda_p y}}\right)dy$$

using [23], (3.324.1), $F_{|p_{k^*}|^2|q_{k^*}|^2}(x)$ as shown in:

$$F_{|p_{k^*}|^2|q_{k^*}|^2}(x) = \left[1-\sum_{k_1=1}^{K}\sum_{k_2=1}^{K}\Upsilon(K,k_1)\,\Upsilon(K,k_2)\times 2\sqrt{\frac{k_2k_1x}{\rho_S\lambda_p\lambda_q}}K_1\left(2\sqrt{\frac{k_2k_1x}{\rho_S\lambda_p\lambda_q}}\right)\right] \tag{24}$$

Putting (19) into (17) A_1 as shown in:

$$A_1 = \sum_{k_1=1}^{K}\sum_{k_2=1}^{K}\frac{\Upsilon(K,k_1)\Upsilon(K,k_2)}{\ln 2}\int_0^{+\infty}\frac{1}{1+x}2\sqrt{\frac{k_2k_1x}{\rho_S\lambda_p\lambda_q}}K_1\left(2\sqrt{\frac{k_2k_1x}{\rho_S\lambda_p\lambda_q}}\right)dx \tag{25}$$

in doing so, we make use of the equalities [23], [24], (9.34.3) as:

$$\frac{1}{1+x} = G_{1,1}^{1,1}\left(x\middle|{}_0^0\right), \tag{26}$$

and

$$2\sqrt{\frac{k_2k_1x}{\rho_S\lambda_p\lambda_q}}K_1\left(2\sqrt{\frac{k_2k_1x}{\rho_S\lambda_p\lambda_q}}\right) = G_{0,2}^{2,0}\left(\frac{k_2k_1x}{\rho_S\lambda_p\lambda_q}\middle|\,\overset{-}{1,0}\right) \tag{27}$$

Submitting (27) and (26) into (25), A_1 as shown in:

$$A_1 = \sum_{k_1=1}^{K}\sum_{k_2=1}^{K}\frac{\Upsilon(K,k_1)\Upsilon(K,k_2)}{\ln 2}\int_0^{+\infty}G_{1,1}^{1,1}\left(x\middle|{}_0^0\right)G_{0,2}^{2,0}\left(\frac{k_2k_1x}{\rho_S\lambda_p\lambda_q}\middle|\,\overset{-}{1,0}\right)dx \tag{28}$$

with the help of the [23], (7.811.1), A_1 is calculated as:

$$A_1 = \sum_{k_1=1}^{K}\sum_{k_2=1}^{K}\frac{\Upsilon(K,k_1)\Upsilon(K,k_2)}{\ln 2}G_{1,3}^{3,1}\left(\frac{k_2k_1}{\rho_S\lambda_p\lambda_q}\middle|\begin{matrix}0\\0,\quad 1,\quad 0\end{matrix}\right) \tag{29}$$

similarly, by solving A_1, A_2 can be obtained as:

$$\begin{aligned} A_2 &= E\left\{C_{E_{k^*}}\right\} = E\left\{\log_2\left(1+\bar{\gamma}_{E_{k^*}}\right)\right\} = E\left\{\log_2\left(1+\rho_E\left|p_{k^*}\right|^2\left|g_{k^*}\right|^2\right)\right\} \\ &= \frac{1}{\ln 2}\int_0^{+\infty}\frac{1}{1+x}\left[1-F_{|p_{k^*}|^2|g_{k^*}|^2}\left(\frac{x}{\rho_E}\right)\right]dx = \sum_{k_3=1}^{K}\sum_{k_4=1}^{K}\frac{\Upsilon(K,k_3)\Upsilon(K,k_4)}{\ln 2}G_{1,3}^{3,1}\left(\frac{k_2k_1}{\rho_E\lambda_p\lambda_g}\middle|\begin{matrix}0\\0,\quad 1,\quad 0\end{matrix}\right). \end{aligned} \tag{30}$$

finally, by substituting (30) and (29) into (20) we can obtain (21).
Proof 2 is completed.

5. NUMERICAL RESULTS

In this section, we set the channel gains $\lambda_p = d_p^{-\frac{\beta}{2}}$, $\lambda_q = d_q^{-\frac{\beta}{2}}$, and $\lambda_g = d_g^{-\frac{\beta}{2}}$ which β is the path loss exponent. Monte-Carlo results average over 10^7 independent sample space trials. Especially, the main parameters can be seen in Table 1. Figure 2 plots the curves between SPSC and transmit SNR, with different values of K. In (17) is used to plot the analytical lines. From Figure 2, we notice that the reader experiences different secrecy capacity performances. In the case of varying the number of distributed backscatter devices, the performance of the k=6 line has better compared to the others in the lower SNR region. In the case of varying the number of distributed backscatter devices, the $K = 6$ line has the best performance compared to the others in the lower SNR region. Both lines approach the ceiling $\rho_S = 20\ dB$, meaning that no performance improvements can be achieved with a greater number of K devices. We can see the analytical curves match well with Monte-Carlo simulations. In Figure 3, we observe the curves between SPSC and transmit SNR, with different values ρ_E. From Figure 3, we notice that the reader experiences different secrecy capacity performances with different values of eavesdropper SNR. Both lines approach the ceiling $\rho_S = 20\ dB$.

From Figure 4, consider the curves between ESC and transmit SNR, with different values K. In (21) is used to plot the analytical lines. Here, we observe that the reader experiences different ergodic secrecy capacity performances with different values of K distributed backscatter devices. The best performance is achieved when there are many backscatter devices. In Figure 5, corresponding observes between ESC and transmit SNR, with different values ρ_E. Here, we see that the reader experiences different ergodic secrecy capacity performance with different numbers of K distributed backscatter devices. The best performance is achieved when the eavesdropper SNR ρ_E has the lowest value. Finally, in Figure 6, we can see the relationship between ESC and K, different values ρ_E. Here, we see that the reader experiences significant performance gaps with different values of eavesdropper SNR ρ_E. The best performance is achieved when the eavesdropper SNR $\rho_E = 0dB$.

Table 1. Simulation parameters [25]

Parameters	Values	Parameters	Values
K	2	ρ_E	15 dB
β	2	d_p	2 m
d_q	2 m	d_g	2 m

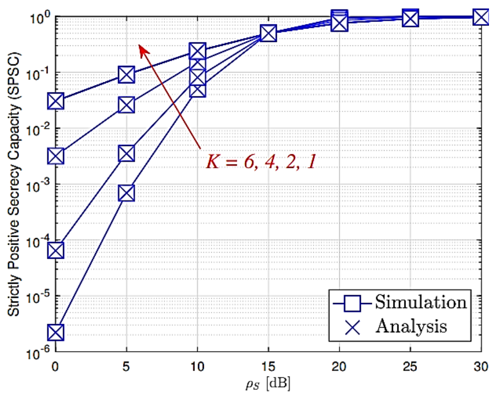

Figure 2. Strictly positive secrecy capacity versus ρ_S in dB varying K

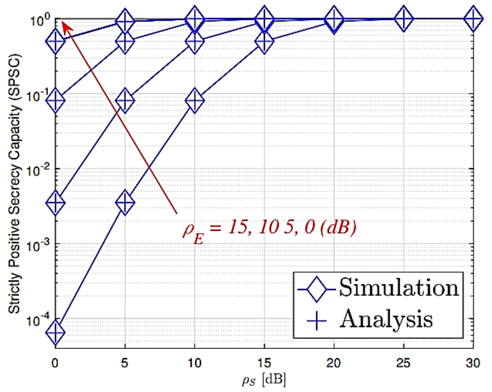

Figure 3. Strictly positive secrecy capacity versus ρ_S in dB varying ρ_E

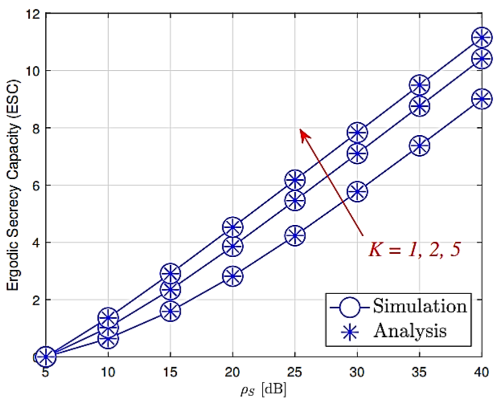

Figure 4. Ergodic secrecy capacity versus ρ_S in dB varying K

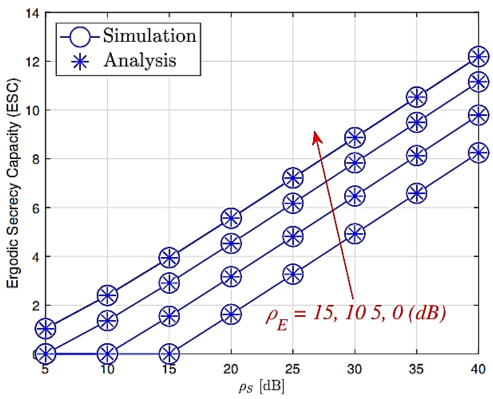

Figure 5. Ergodic secrecy capacity versus ρ_S in dB varying ρ_E

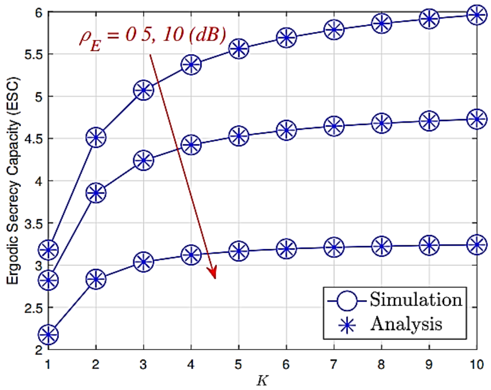

Figure 6. Ergodic secrecy capacity versus K varying ρ_E

6. CONCLUSION

In this study, we provided the secrecy capacity analysis of a bi-static backscatter communication system located in the vicinity of an eavesdropper. We derived exact expressions of the strictly positive and ergodic secrecy capacity of the backscatter reader device. The number of distributed backscatter devices contributes significantly to the ESC of the reader but has no significant impact on the strictly positive secrecy capacity performance. In future work, we will consider the impact of non-orthogonal multiple access (NOMA) on the secrecy capacity of the system.

REFERENCES

[1] C. Xu, L. Yang, and P. Zhang, "Practical backscatter communication systems for battery-free internet of things: a tutorial and survey of recent research," in *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 16-27, Sep. 2018, doi: 10.1109/MSP.2018.2848361.

[2] D. Mishra and E. G. Larsson, "Sum throughput maximization in multi-tag backscattering to multi-antenna reader," in *IEEE Transactions on Communications*, vol. 67, no. 8, pp. 5689-5705, Aug. 2019, doi: 10.1109/TCOMM.2019.2912381.

[3] K. H. Jang, S. M. Kim, and J. Kim, "Performance analysis of multi-tag multi-reader ambient backscatter communication systems," *2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN)*, 2019, pp. 422-425, doi: 10.1109/ICUFN.2019.8806036.

[4] F. Jameel, S. Zeb, W. U. Khan, S. A. Hassan, Z. Chang, and J. Liu, "NOMA-enabled backscatter communications: toward battery-free IoT networks," in *IEEE Internet of Things Magazine*, vol. 3, no. 4, pp. 95-101, Dec. 2020, doi: 10.1109/IOTM.0001.2000055.

[5] X. Lu, D. Niyato, H. Jiang, D. I. Kim, Y. Xiao, and Z. Han, "Ambient backscatter assisted wireless powered communications," in *IEEE Wireless Communications*, vol. 25, no. 2, pp. 170-177, Apr. 2018, doi: 10.1109/MWC.2017.1600398.

[6] A. Guerra, F. Guidi, D. Dardari, A. Clemente, and R. D'Errico, "A millimeter-wave indoor backscattering channel model for environment mapping," in *IEEE Transactions on Antennas and Propagation*, vol. 65, no. 9, pp. 4935-4940, Sep. 2017, doi: 10.1109/TAP.2017.2728088.

[7] F. Jameel, T. Ristaniemi, I. Khan, and B. M. Lee, "Simultaneous harvest-and-transmit ambient backscatter communications under rayleigh fading," in *EURASIP Journal on Wireless Communications and Networking*, no. 1, pp. 1-9, 2019, doi: 10.1186/s13638-019-1480-7.

[8] J. Guo, X. Zhou, S. Durrani, and H. Yanikomeroglu, "Design of non-orthogonal multiple access enhanced backscatter communication," in *IEEE Transactions on Wireless Communications*, vol. 17, no. 10, pp. 6837-6852, Oct. 2018, doi: 10.1109/TWC.2018.2864741.

[9] Y. Li, M. Jiang, Q. Zhang, and J. Qin, "Secure beamforming in MISO NOMA backscatter device aided symbiotic radio networks," in *arXiv preprint arXiv:1906.03410*, Jun 2019, doi: 10.48550/arXiv.1906.03410.

[10] B. Lyu, Z. Yang, G. Gui, and H. Sari, "Optimal time allocation in backscatter assisted wireless powered communication networks," in *Sensors*, vol. 17, no. 6, p. 1258, 2017, doi: 10.3390/s17061258.

[11] C. He and Z. J. Wang, "Closed-form BER analysis of non-coherent FSK in MISO double Rayleigh fading/RFID channel," in *IEEE Communications Letters*, vol. 15, no. 8, pp. 848-850, Aug. 2011, doi: 10.1109/LCOMM.2011.061011.110276.

[12] Y. Zhang, F. Gao, L. Fan, X. Lei, and G. K. Karagiannidis, "Secure communications for multi-tag backscatter systems," *in IEEE Wireless Communications Letters*, vol. 8, no. 4, pp. 1146-1149, Aug. 2019, doi: 10.1109/LWC.2019.2909199.

[13] H. Song, Y. Gao, N. Sha, Q. Zhou, and F. Yao, "A distinctive method to improve the security capacity of backscatter wireless system," *2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, 2017, pp. 272-276, doi: 10.1109/IAEAC.2017.8054020.

[14] J. You, G. Wang, and Z. Zhong, "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), 2015, pp. 43-47, doi: 10.1049/cp.2015.0911.

[15] T. S. Muratkar, A. Bhurane, P. K. Sharma and A. Kothari, "Physical layer security analysis in ambient backscatter communication with node mobility and imperfect channel estimation," in *IEEE Communications Letters*, vol. 26, no. 1, pp. 27-30, Jan. 2022, doi: 10.1109/LCOMM.2021.3123893.

[16] J. D. Griffin and G. D. Durgin, "Gains for RF tags using multiple antennas," in *IEEE Transactions on Antennas and Propagation*, vol. 56, no. 2, pp. 563-570, Feb. 2008, doi: 10.1109/TAP.2007.915423.

[17] D. Kim, H. Jo, H. Yoon, C. Mun, B. Jang, and J. Yook, "Reverse-link interrogation range of a UHF MIMO-RFID system in nakagami- m fading channels," in *IEEE Transactions on Industrial Electronics*, vol. 57, no. 4, pp. 1468-1477, Apr. 2010, doi: 10.1109/TIE.2009.2030134.
[18] D.-T. Do and M.-S. Van Nguyen, “Impact of untrusted relay on physical layer security in non-orthogonal multiple access networks,” in *Wireless Personal Communications*, vol. 106, no. 3, pp. 1353-1372, Jun. 2019, doi: 10.1007/s11277-019-06219-y.
[19] D. -T. Do, C. -B. Le, and F. Afghah, "Enabling full-duplex and energy harvesting in uplink and downlink of small-cell network relying on power domain based multiple access," in *IEEE Access*, vol. 8, pp. 142772-142784, 2020, doi: 10.1109/ACCESS.2020.3013912.
[20] C.-B. Le and D.-T. Do, “Outage performance of backscatter NOMA relaying systems equipping with multiple antennas,” in *Electronics Letters*, vol. 55, no. 19, pp. 1066-1067, Sep. 2019, doi: 10.1049/el.2019.1390.
[21] J. Chen, L. Yang, and M. -S. Alouini, "Physical layer security for cooperative NOMA systems," in *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4645-4649, May 2018, doi: 10.1109/TVT.2017.2789223.
[22] W. Liu, Z. Ding, T. Ratnarajah, and J. Xue, "On ergodic secrecy capacity of random wireless networks with protected zones," in *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6146-6158, Aug. 2016, doi: 10.1109/TVT.2015.2477315.
[23] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 6th ed. New York, NY, USA: Academic Press, 2000.
[24] T.-L. Nguyen, C.-B. Le, and D.-T. Do, “Performance analysis of multi-user NOMA over α-κ-μ shadowed fading,” in *Electronics Letters*, vol. 56, no. 15, pp. 771-773, Jul. 2020, doi: 10.1049/el.2019.4265.
[25] W. Saad, X. Zhou, Z. Han, and H. V. Poor, "On the physical layer security of backscatter wireless systems," in *IEEE Transactions on Wireless Communications*, vol. 13, no. 6, pp. 3442-3451, June 2014, doi: 10.1109/TWC.2014.051414.130478.

BIOGRAPHIES OF AUTHORS

Phung Ton That was born in Thua Thien-Hue, Viet Nam. He received the B.S. degree in electronics and telecommunications engineering (2007) and the M.S. degree in electronics engineering (2010) from the University of Technology, Vietnam. He is currently a lecturer at the Faculty of Electronics Technology (FET), Industrial University of Ho Chi Minh City. His research interest are optical materials, wireless communication in 5G, energy harvesting, performance of cognitive radio, physical layer security, and NOMA. He can be contacted at email: tonthatphung@iuh.edu.vn.

Duy-Hung Ha received B.S. and M.S. degrees in Electronics and Telecommunications Engineering from Institute of Post and Telecommunication, Vietnam; University of transport and communications, Ha Noi, Vietnam in 2007 and 2014. In 2017, he joined Faculty of Electrical and Electronics Engineering of Ton Duc Thang University, Vietnam as a lecturer. In 2021, he is degrees Ph.D in communication technology at VSB Technical University of Ostrava, Czech Republic. His major interests are cooperative communications and physical-layer security. He can be contacted at email: haduyhung@tdtu.edu.vn.

Hong-Nhu Nguyen received a B.Sc. in Electronics Engineering from Ho Chi Minh city University of Technology in 1998, M. Eng in Electronics Engineering from the University of Transport and Communications (Vietnam) in 2012 and his Ph.D. degree in telecommunications from Technical University of Ostrava, Czech Republic in 2021. He is currently working as lecturer at Saigon University. His research interests include applied electronics, wireless communications, cognitive radio, NOMA, and energy harvesting. He can be contacted at email: nhu.nh@sgu.edu.vn.