This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2019.2909199, IEEE Wireless Communications Letters

Secure Communications for Multi-tag Backscatter Systems

Yu Zhang, *Student Member, IEEE*, Feifei Gao, *Member, IEEE*, Lisheng Fan, *Member, IEEE*, Xianfu Lei, *Member, IEEE*, and George K. Karagiannidis, *Fellow, IEEE*

***Abstract*—In this letter, we investigate a multi-tag backscatter communication system in the presence of an eavesdropper. In order to strengthen transmission security, the optimal tag is chosen among N tags. We consider a practical backscatter communication scenario, where channel correlation between the forward and backscatter links may exist and we study its impact on the system's security. Specifically, we derive an analytical expression for the secrecy outage probability (SOP). Moreover, in order to gain more insights for the system design, we obtain an asymptotic closed-form expression for the SOP over correlated Rayleigh fading channels. Finally, simulations are performed to validate the theoretical analysis.**

***Index Terms*—Backscatter communication, secrecy outage probability, correlated channel, physical layer security.**

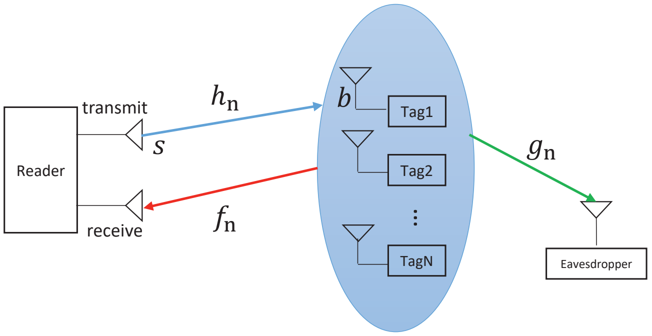

Fig. 1. Backscatter communication systems with a reader, N tags and an eavesdropper.

I. Introduction

Backscatter communications play an important role in Internet of Things (IoT), due to its low cost and energy consumption [1], [2]. Radio frequency identification (RFID) is a typical backscatter communication system, which utilizes the backscatter modulation to realize data transmission [3]. In contrast to traditional communication systems, RFID includes both forward and backscatter links. Specifically, in [4], the authors proposed a *dyadic backscatter channel* model in RFID systems, which includes the forward and backscatter links. In practice, these links can be correlated, since transmit and receive antennas at the reader may be very close or even co-located [5]. Kim *et. al.* investigated the performance of multiple-input multiple-output (MIMO) RFID systems, where the forward and backscatter channel links are modeled as fully correlated or uncorrelated Nakagami-m distributions [6].

Similarly with other wireless systems, privacy and security are also major issues for an RFID system. Due to its broadcast nature, RFID system is vulnerable to potential eavesdropping attack. In the open literature, several works have proposed the lightweight cryptography to deal with the RFID security [7]. Although cryptography can achieve better security performance, it presents high communication overhead and computational complexity.

Due to the limitations of existing RFID systems in cost, size and computational complexity, we consider physical layer security (PLS) as an alternative method to cryptography. The main idea of PLS is to utilize the wireless channel characteristics in order to prevent eavesdroppers getting information from the transmitter. Saad *et. al* in [8] studied the PLS of a single-reader and single-tag model for an RFID system, where the reader not only sends the query signal to power the tag, but also injects artificial noise to interfere with an eavesdropper. Moreover, the authors in [9] investigated the secrecy rate maximization problem in a MIMO RFID system by jointly optimizing the supply energy and precoding matrix of artificial noise at the reader. Considering the reality condition, the authors in [10] proposed a framework for IoT devices secure initialization without increasing any complexity of system. However, the aforementioned works have not derived a useful analytical expression for the system secrecy outage probability (SOP).

In this letter, we propose an optimal multi-tag selection scheme, in the presence of an eavesdropper. In order to evaluate the security performance, an analytical expression for the SOP of the multi-tag selection RFID system has been derived. Furthermore, to gain more insights for the system design, we obtain an asymptotic closed-form expression for the SOP over correlated Rayleigh fading channels. The performance analysis is based on the assumption that the forward and backscatter links subjected to correlated Rayleigh fading.

II. system model

In this letter, we consider a multi-tag backscatter system, which consists of a reader, N distributed tags and an eavesdropper, who can overhear the information from the tag's

Y. Zhang and F. Gao (corresponding author) are with Institute for Artificial Intelligence, Tsinghua University (THUAI), State Key Lab of Intelligent Technologies and Systems, Tsinghua University, Beijing National Research Center for Information Science and Technology (BNRist), Department of Automation, Tsinghua University, Beijing 100084, China (email: zy16@mails.tsinghua.edu.cn, feifeigao@ieee.org).

L. Fan is with the School of Computer Science and Educational Software, Guangzhou University, Guangzhou 510006, China (e-mail: lsfan@gzhu.edu.cn).

X. Lei is with the School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China, and also with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: xflei@home.swjtu.edu.cn).

G. K. Karagiannidis is with the Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, 54 124 Thessaloniki, Greece (e-mail: geokarag@auth.gr).

transmission, as shown in Fig. 1. We denote h_n , f_n and g_n the channel gains from the transmit antenna at the reader to the n-th tag, the n-th tag to the receive antenna at reader and the n-th tag to the eavesdropper, respectively. We assume that all the above channel gains follow Rayleigh distribution [11], i.e., $h_n \sim \mathcal{CN}(0, a)$, $f_n \sim \mathcal{CN}(0, b)$, $g_n \sim \mathcal{CN}(0, c)$. The received signal at the reader from the n-th tag can be expressed as

$$y_{r_n} = h_n f_n sb + n_r, \tag{1}$$

where s is the query signal sent by the reader, b is the information signal from the tag and n_r is the additive white Gaussian noise (AWGN), $n_r \sim \mathcal{CN}(0, \sigma_r^2)$. Due to the architecture of the RFID backscatter system [4], the forward link h_n and the backscatter link f_n can be correlated. In the monostatic RFID system, where the reader uses the same antenna to transmit and receive signals, the forward and backscatter links can be fully correlated. On the other hand, in the bistatic RFID system, where the transmit and receive antennas are placed separately, the forward and backscatter links can be considered as partially correlated channels [6]. In practice, bistatic architecture is more effective than the monostatic one. Next, we consider the bistatic RFID system architecture.

The joint probability density function (PDF) of $|h_n|^2$ and $|f_n|^2$ is [12]

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

where ρ is the channel correlation coefficient, defined as $\rho = \frac{Cov(X_1,X_2)}{\sqrt{Var(X_1)Var(X_2)}}$, with $0 < \rho < 1$ and $I_0(\cdot)$ is the modified Bessel function of the first kind. Note that the infinite series expansion of $I_0(\cdot)$ is [13]

$$I_0(z) = \sum_{k=0}^{\infty} \frac{(\frac{z}{2})^{2k}}{(k!)^2}. \tag{3}$$

On the other hand, at the eavesdropper side, the intercepted signal from the n-th tag can be written as

$$y_{e_n} = h_n g_n sb + n_e, \tag{4}$$

where n_e is the AWGN at eavesdropper, $n_e \sim \mathcal{CN}(0, \sigma_e^2)$, and we assume h_n and g_n are independent with each other, since the eavesdropper is far from reader, compared to the distance with the tag. From (1) and (4), we can derive the received instantaneous signal-to-noise ratios (SNRs) at the reader and eavesdropper as

$$\gamma_{r_n} = \frac{|h_n f_n|^2 P_s}{\sigma_r^2} = |h_n f_n|^2 \bar{\gamma}_r, \tag{5}$$

and

$$\gamma_{e_n} = \frac{|h_n g_n|^2 P_s}{\sigma_e^2} = |h_n g_n|^2 \bar{\gamma}_e, \tag{6}$$

where $P_s = \mathbb{E}\{|s|^2\}$ is the transmit power; $\bar{\gamma}_r$ and $\bar{\gamma}_e$ are the average receive SNR at reader and eavesdropper, respectively. Correspondingly, from (5) and (6), the capacity of the reader and eavesdropper's channels can be written as

$$C_r = \log_2(1 + \gamma_{r_n}) \tag{7}$$

and

$$C_e = \log_2(1 + \gamma_{e_n}), \tag{8}$$

respectively. Using (7) and (8), we can express the instantaneous secrecy capacity of multi-tag RFID backscatter system as [14]

$$C_s = C_r - C_e = \begin{cases} \log_2\left(\frac{1+\gamma_{r_n}}{1+\gamma_{e_n}}\right), & \gamma_{r_n} \geq \gamma_{e_n} \\ 0, & \gamma_{r_n} < \gamma_{e_n}. \end{cases} \tag{9}$$

In the proposed multi-tag backscatter system, we assume the reader has available channel state information (CSI) for h_n, f_n and g_n [1]. Based on the CSI, the reader chooses one tag from the N distributed tags to transmit the information. From (9), it is obvious that the optimal tag selection (TS) scheme is selecting the tag that can maximize the system secrecy capacity, as follows

$$n^* = \arg\max_{1 \leq n \leq N} \frac{1 + |h_n f_n|^2 \bar{\gamma}_r}{1 + |h_n g_n|^2 \bar{\gamma}_e}. \tag{10}$$

III. Secrecy outage probability

In this section, the secrecy outage probability of the proposed scheme is analyzed. The SOP is an important metric to evaluate the secrecy performance, and is defined as the probability that the instantaneous secrecy capacity falls below a certain threshold, R_s. Hence, we derive the SOP of the optimal TS scheme as

$$\begin{aligned} P_{out} &= \Pr\left[\log_2\left(\frac{1 + \gamma_{r_{n^*}}}{1 + \gamma_{e_{n^*}}}\right) < R_s\right] \\ &= \Pr\left[\frac{1 + |h_{n^*} f_{n^*}|^2 \bar{\gamma}_r}{1 + |h_{n^*} g_{n^*}|^2 \bar{\gamma}_e} < \gamma_s\right] \\ &= \Pr\left[\max_{1 \leq n \leq N} \frac{1 + |h_n f_n|^2 \bar{\gamma}_r}{1 + |h_n g_n|^2 \bar{\gamma}_e} < \gamma_s\right], \end{aligned} \tag{11}$$

where $\gamma_s = 2^{R_s}$ is the secrecy SNR threshold. Since all the tags are independent with each other, (11) can be rewritten as

$$\begin{aligned} P_{out} &= \left\{\Pr\left[\frac{1 + |h_1 f_1|^2 \bar{\gamma}_r}{1 + |h_1 g_1|^2 \bar{\gamma}_e} < \gamma_s\right]\right\}^N \\ &= \left\{\Pr\left[|h_1|^2(\bar{\gamma}_r |f_1|^2 - \bar{\gamma}_e \gamma_s |g_1|^2) < \gamma_s - 1\right]\right\}^N. \end{aligned} \tag{12}$$

Denote $w_1 = |h_1|^2$, $w_2 = |f_1|^2$, $w_3 = |g_1|^2$ and

$$u = \bar{\gamma}_r w_2 - \bar{\gamma}_e \gamma_s w_3. \tag{13}$$

From (12), in order to derive the SOP, we need first to obtain the PDF of u. By using basic statistics for the difference of two random variables, we can derive the PDF of u as [17]

$$f(u) = \begin{cases} \frac{1}{\bar{\gamma}_e \gamma_s c + b\bar{\gamma}_r} \exp\left(-\frac{u}{b\bar{\gamma}_r}\right), & u \geq 0 \\ \frac{1}{\bar{\gamma}_e \gamma_s c + b\bar{\gamma}_r} \exp\left(\frac{u}{c\gamma_s \bar{\gamma}_e}\right), & u < 0 \end{cases}. \tag{14}$$

[1] Note that the channel gains h_n and f_n can be estimated by using pilot signals or blind estimation [15], while the eavesdropper channel gain g_n can be obtained through feedback, when the eavesdropper is active. This occurs when the eavesdropper is another active user in the network [16].

$$P_{out} = \left\{ \sum_{k=0}^{\infty} \frac{\rho^k (1-\rho)}{(c\gamma_s \bar{\gamma}_e + b\bar{\gamma}_r)} \left[c\gamma_s \bar{\gamma}_e + b\bar{\gamma}_r - 2\eta_1^{\frac{k+1}{2}} (b\bar{\gamma}_r)^{\frac{1-k}{2}} K_{k+1}\left(2\sqrt{\eta_1 (b\bar{\gamma}_r)^{-1}}\right)/k! \right] \right\}^N . \tag{23}$$

According to the positive and negative value of u, (12) is further written as

$$\begin{aligned} P_{out} &= \{\Pr[w_1 u < \gamma_s - 1]\}^N \\ &= \{\Pr[0 < w_1 < (\gamma_s - 1)/u | u > 0] \Pr[u > 0] \\ &+ \Pr[w_1 > 0 | u < 0] \Pr[u < 0]\}^N \\ &= (I_1 + I_2)^N, \end{aligned} \tag{15}$$

where

$$I_1 = \int_0^{\infty} \int_0^{\infty} \int_0^{\frac{\gamma_s - 1}{u}} f(w_1, w_2) f(u) dw_1 du dw_2, \tag{16}$$

$$I_2 = \int_0^{\infty} \int_{-\infty}^{0} \int_0^{\infty} f(w_1, w_2) f(u) dw_1 du dw_2, \tag{17}$$

and $f(w_1, w_2)$ is the joint PDF of w_1 and w_2, which can be derived by substituting (3) into (2), as

$$f(w_1, w_2) = \sum_{k=0}^{\infty} \lambda_0 w_1^k w_2^k e^{-\lambda_1 w_1} e^{-\lambda_2 w_2}, \tag{18}$$

where

$$\lambda_0 = \frac{\rho^k}{(1-\rho)^{2k+1} (ab)^{k+1} (k!)^2}, \tag{19}$$

$$\lambda_1 = \frac{1}{(1-\rho)a}, \quad \lambda_2 = \frac{1}{(1-\rho)b}. \tag{20}$$

Substituting (14) and (18) into (16) and (17) and by using the integral formula in [13], we obtain

$$\begin{aligned} I_1 = \sum_{k=0}^{\infty} & \left[k! b\bar{\gamma}_r - 2\eta^{\frac{k+1}{2}} (b\bar{\gamma}_r)^{\frac{1-k}{2}} K_{k+1}\left(2\sqrt{\eta (b\bar{\gamma}_r)^{-1}}\right) \right] \\ & \times \frac{\rho^k (1-\rho)}{(c\gamma_s \bar{\gamma}_e + b\bar{\gamma}_r) k!}, \end{aligned} \tag{21}$$

where $\eta = \lambda_1 (\gamma_s - 1)$, and

$$I_2 = \sum_{k=0}^{\infty} \frac{\rho^k (1-\rho) c\gamma_s \bar{\gamma}_e}{(c\gamma_s \bar{\gamma}_e + b\bar{\gamma}_r)}. \tag{22}$$

Substituting (21) and (22) into (15), we finally obtain an analytical expression for the SOP of the proposed scheme as in (23) in the top of the page. It is obvious that (23) is an infinite series and this is too complex to gain insights for the system design. Therefore, we derive the asymptotic SOP, as $\bar{\gamma}_r$ goes to infinity. By substituting the approximation of $K_1(\cdot)$ [18],

$$K_1(z) \sim \frac{1}{z} + \frac{z}{2} \ln\left(\frac{z}{2}\right), \quad z \to 0, \tag{24}$$

into (23), a closed-form expression for the SOP with large γ_e can be obtained as

$$P_{out}^{\infty} = \left[\frac{c\gamma_s \bar{\gamma}_e + \eta \ln(b\bar{\gamma}_r / \eta)}{b\bar{\gamma}_r} \right]^N . \tag{25}$$

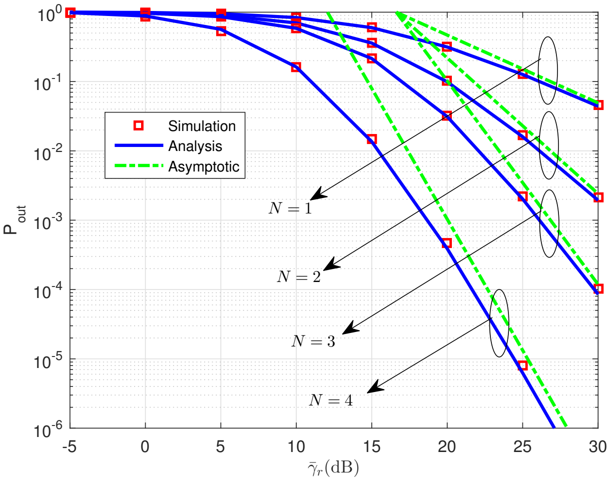

Fig. 2. Secrecy outage probability versus $\bar{\gamma}_r$ over Rayleigh fading with $\bar{\gamma}_e =$ 15 dB, $a = 2, b = 3, c = 1, \rho = 0.5,\ N = 1, 2, 3, 4$.

Moreover, when $\bar{\gamma}_e$ is small, the term $c\gamma_s \bar{\gamma}_e$ in (25) can be ignored. In this case, the asymptotic SOP is given by

$$P_{out}^{\infty} = \left[\frac{\ln(b\bar{\gamma}_r / \eta)}{b\bar{\gamma}_r / \eta} \right]^N , \tag{26}$$

where $b\bar{\gamma}_r / \eta = ab\bar{\gamma}_r (1-\rho)/(\gamma_s - 1)$. From (25) and (26), we can conclude that the asymptotic SOP becomes worse as ρ increases. This happens because the high channel correlation between forward and backscatter links deteriorates the main channel communication performance. Due to the double fading channel characteristics in RFID systems, the channel parameters a and b influence the secrecy performance together. To be more specific, an increase of ab can improve the secrecy performance. Furthermore, we can easily obtain the diversity order as N, when $\bar{\gamma}_r$ goes to infinity.

IV. Numerical Results and Simulations

In this section, we present simulations to validate the derived analytical expressions. The secrecy target rate R_s is set as 1 bps/Hz. The channels h_n, f_n and g_n are assumed to be a combination of path loss and small scale fading, i.e., $h_n = d_{Tx,n}^{-\gamma/2} \tilde{h}_n$, $f_n = d_{Rx,n}^{-\gamma/2} \tilde{f}_n$ and $g_n = d_{E,n}^{-\gamma/2} \tilde{g}_n$, where γ is the path loss exponent, set as $\gamma = 2$, and d is the distance between two nodes. We set $d_{Tx,n} = d_{Rx,n} = d_{E,n} = 2$m [8]. The number of Monte Carlo runs for average is taken as 10^7. The infinity sum is truncated at the first 50 terms.

Fig. 2 demonstrates SOP versus $\bar{\gamma}_r$ for different number of tags. It is clear that the analytical results in (23) match well with the simulations. Several cases of the number of tags are investigated, with $N = 1, 2, 3, 4$. From the curves, we observe that the security performance improves with an increase of $\bar{\gamma}_r$.

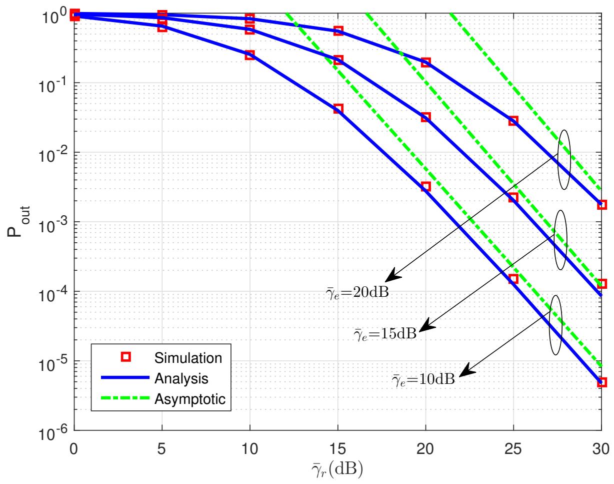

Fig. 3. Secrecy outage probability versus $\bar{\gamma}_r$ over Rayleigh fading with $\bar{\gamma}_e = 10, 15, 20$ dB, $a = 2, b = 3, c = 1, \rho = 0.5, N = 3$.

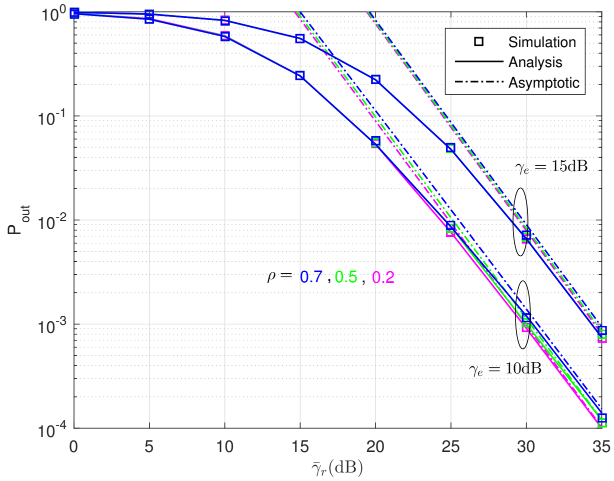

Fig. 4. Secrecy outage probability versus $\bar{\gamma}_r$ over Rayleigh fading with $\bar{\gamma}_e = 15, 10$ dB, $a = 2, b = 3, c = 2, \rho = 0.2, 0.5, 0.7, N = 2$.

Moreover, the asymptotic curves is very close to the exact one at high $\bar{\gamma}_r$, which validates the derived results. The diversity order can be obtained from the slope of the curves at high $\bar{\gamma}_r$, which is approximately equal to N. The secrecy performance and diversity gain can be both improved as increasing N.

Fig. 3 illustrates the effect of $\bar{\gamma}_e$ on the SOP versus $\bar{\gamma}_r$ with $\rho = 0.5$, $N = 3$. It can be observed that the secrecy performance is degraded as $\bar{\gamma}_e$ increases. Moreover, the curves are parallel for different $\bar{\gamma}_e$ at high $\bar{\gamma}_r$, which indicates that the diversity order has nothing to do with the $\bar{\gamma}_e$. Furthermore, it is evident that the analytical results match well with the simulations and the asymptotic curves converge to the exact one at high $\bar{\gamma}_r$.

Fig. 4 depicts the impact of channel correlation on the secrecy performance, where $\bar{\gamma}_e$ is set to 15dB, 10 dB, and $N = 2$. It can be easily observed that the channel correlation between the forward and backscatter links has little influence on the security performance. However, the SOP decreases as ρ decreases, which is in accordance with the analytical results in (26). Finally, the analytical and asymptotic results match well with the simulations for different values of ρ, which verifies the correctness of the derived theoretical results for the optimal tag selection scheme over correlated Rayleigh fading.

V. Conclusion

In this paper, we have proposed an optimal tag selection scheme for RFID backscatter communication systems with an eavesdropper, where the forward and backscatter links are subjected to correlated Rayleigh distribution. We derived an analytical SOP and an asymptotic closed-form expression at high $\bar{\gamma}_e$. We conclude from the past that the channel correlation has a negative influence on the secrecy performance and the diversity order is approximately equal to N.

References

[1] J. Qian, F. Gao, G. Wang, S. Jin, and H. Zhu, "Noncoherent detections for ambient backscatter system," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1412–1422, March. 2017.

[2] C. Zhong, H. A. Suraweera, G. Zheng, I. Krikidis, and Z. Zhang, "Wireless information and power transfer with full duplex relaying," *IEEE Trans. Commun.,* vol. 62, no. 10, pp. 3447–3461, Oct. 2014.

[3] G. Wang, F. Gao, R. Fan, and C. Tellambura, "Ambient backscatter communication systems: Detection and performance analysis," *IEEE Trans. Commun.*, vol. 64, no. 11, pp. 4836-4846, Aug. 2016.

[4] J. D. Griffin and G. D. Durgin, "Gains for RF tags using multiple antennas," *IEEE Trans. Antennas Propag.*, vol. 56, no. 2, pp. 563–570, Oct. 2008.

[5] J. D. Griffin and G. D. Durgin, "Link envelope correlation in the backscatter channel," *IEEE Commun. Lett.*, vol. 11, no. 9, pp. 735–737, Sep. 2007.

[6] D. Y. Kim and D. I. Kim, "Reverse-link interrogation range of a UHF MIMO-RFID system in Nakagami-m fading channels," *IEEE Trans. Industrial Electron.*, vol. 57, no. 4, pp. 1468–1477, Apr. 2010.

[7] E. Vahedi, R. K. Ward, and I. F. Blake, "Security analysis and complexity comparison of some recent lightweight RFID protocols," in *Proc. 4th Int. Conf. Computational Intelligence Security Inf. Syst.,* Spain, Jun. 2011, pp. 92–99.

[8] W. Saad, X. Zhou, Z. Han, and H. V. Poor, "On the physical layer security of backscatter wireless systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2 pp. 3442–3451, Dec. 2014.

[9] Q. Yang, H.-M. Wang, Y. Zhang, and Z. Han, "Physical layer security in MIMO backscatter wireless systems," *IEEE Trans. Wireless Commun.,* vol. 15, no. 11, pp. 7547–7560, Nov. 2016.

[10] T. Pecorella, L. Brilli, and L. Mucchi, "The role of physical layer security in IoT: A novel perspective," *Information,* vol. 7, no. 3, 2016. [Online]. Available: http://www.mdpi.com/2078-2489/7/3/49

[11] C. He and Z. J. Wang, "Closed-form BER analysis of non-coherent FSK in MISO double rayleigh fading/RFID channel," *IEEE Commun. Lett.,* vol. 15, no. 8, pp. 848–850, 2011.

[12] M. K. Simon, *Proability Distributions Involving Gaussian Random Variales: A Handbook for Engineers, Scientists and Mathematicians*, New York: Springer, 2006.

[13] A. Jeffrey and D. Zwillinger, *Table of Integrals, Series, and Products*, Academic Press, 2007.

[14] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory,* vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[15] S. Ma, G. Wang, R. Fan, and C. Tellambura, "Blind channel estimation for ambient backscatter communication systems," *IEEE Commun. Lett.,* vol. 22, no. 6, pp. 1296–1299, Jun. 2018.

[16] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Proc.,* vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[17] M. K. Simon and M.-S. Alouini, *Digital Communications Over Fading Channels.* New York: Wiley, 2000.

[18] Wolfram Research, Inc.: The Wolfram functions site. Available at: http://www.functions.wolfram.com, 2007.