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.

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
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., \( h_n \sim CN(0, \sigma^2), f_n \sim CN(0, b), g_n \sim CN(0, c). \) The received signal at the reader from the \( n \)-th tag can be written as

\[
y_{r_n} = h_n f_n s b + n_r,
\]

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), \( n_r \sim CN(0, \sigma^2_r) \). 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]

\[
f_{|h_n|^2, |f_n|^2}(x_1, x_2) = \exp \left( -\frac{(x_1-1-r\rho) - (x_2-1-(1-r)\rho)h}{ab(1-\rho)} \right)
\times I_0 \left( \frac{2\sqrt{abx_1x_2}}{ab(1-\rho)} \right),
\]

where \( \rho \) is the channel correlation coefficient, defined as \( \rho = \frac{\text{Cov}(X_1, X_2)}{\sqrt{\text{Var}(X_1)\text{Var}(X_2)}} \), with \( 0 \leq \rho < 1 \) 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]

\[
I_0(z) = \sum_{k=0}^{\infty} \frac{\left( \frac{z}{2} \right)^{2k}}{(k!)^2}.
\]

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

\[
y_{e_n} = h_n g_n s b + n_e,
\]

where \( n_e \) is the AWGN at eavesdropper, \( n_e \sim CN(0, \sigma^2_e) \), 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

\[
\gamma_r = \frac{|h_n f_n|^2 P_s}{\sigma^2_r} = |h_n f_n|^2 \bar{\gamma}_r, \quad (5)
\]

and

\[
\gamma_e = \frac{|h_n g_n|^2 P_s}{\sigma^2_e} = |h_n g_n|^2 \bar{\gamma}_e, \quad (6)
\]

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

\[
C_r = \log_2(1 + \gamma_r) \quad (7)
\]

and

\[
C_e = \log_2(1 + \gamma_e), \quad (8)
\]

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

\[
C_s = C_r - C_e = \begin{cases} 
\log_2 \left( \frac{1 + \gamma_r}{1 + \gamma_e} \right), & \gamma_r \geq \gamma_e, \\
0, & \gamma_r < \gamma_e. 
\end{cases} \quad (9)
\]

In the proposed multi-tag backscatter system, we assume the reader has available channel state information (CSI) for \( h_n, f_n \) and \( g_n \). 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

\[
n^* = \max_{1 \leq n \leq N} \left[ 1 + h_n f_n^2 |\bar{\gamma}_r| \right] 
\]

\[
\max_{1 \leq n \leq N} \frac{1 + h_n f_n^2 |\bar{\gamma}_r|}{1 + h_n g_n^2 |\bar{\gamma}_e|} < \gamma_s, \quad (10)
\]

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

\[
P_{out} = \Pr \left[ \log_2 \left( \frac{1 + \gamma_r}{1 + \gamma_e} \right) < R_s \right] 
= \Pr \left[ \frac{1 + h_n f_n^2 |\bar{\gamma}_r|}{1 + h_n g_n^2 |\bar{\gamma}_e|} < \gamma_s \right] 
= \Pr \left[ \max_{1 \leq n \leq N} \frac{1 + h_n f_n^2 |\bar{\gamma}_r|}{1 + h_n g_n^2 |\bar{\gamma}_e|} < \gamma_s \right], \quad (11)
\]

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

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

Denote \( w_1 = |h_1|^2, w_2 = |f_1|^2, w_3 = |g_1|^2 \) and

\[
u = \gamma_r w_2 - \gamma_e \gamma_s w_3. \quad (13)
\]

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]

\[
f(u) = \begin{cases} 
\frac{1}{\gamma_r \gamma_e + bw_r} \exp \left( -\frac{u}{bw_r} \right), & u \geq 0, \\
\frac{1}{\gamma_r \gamma_e + bw_e} \exp \left( -\frac{u}{bw_e} \right), & u < 0. \quad (14)
\end{cases}
\]

\(^1\text{Note that the channel gains } h_n \text{ and } f_n \text{ can be estimated by using pilot signals or blind estimation [15], while the eavesdropper channel gain } g_n \text{ can be obtained through feedback, when the eavesdropper is active. This occurs when the eavesdropper is another active user in the network [16].}
According to the positive and negative value of \( u \), (12) is further written as

\[
P_{\text{out}} = \left\{ \Pr[w_1u < \gamma_s - 1]\right\}^N
\]

where \( \Pr[0 < w_1 < \gamma_s - 1/u | u > 0] \Pr[u > 0] + \Pr[w_1 > 0 | u < 0] \Pr[u < 0]\right\}^N = (I_1 + I_2)^N, \tag{15}\]

where

\[
I_1 = \int_0^\infty \int_0^\infty \int_0^\infty f(w_1, w_2) f(u) dw_1 dw_2, \tag{16}
\]

\[
I_2 = \int_0^\infty \int_0^\infty \int_0^\infty f(w_1, w_2) f(u) dw_1 dw_2, \tag{17}
\]

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

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

where

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

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

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

\[
I_1 = \sum_{k=0}^\infty \left[ k! b_{\tilde{\gamma}_r} - 2 \eta \frac{1}{2^{k+1} (b_{\tilde{\gamma}_r})^{k+1}} K_{k+1} \left( 2 \sqrt{\eta (b_{\tilde{\gamma}_r})^{-1}} \right) \right] \frac{\rho^k (1 - \rho)}{(c_{\gamma_s \gamma} + b_{\tilde{\gamma}_r} k!)}, \tag{21}\]

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

\[
I_2 = \sum_{k=0}^\infty \frac{\rho^k (1 - \rho) c_{\gamma_s \gamma} e_{\gamma_s \gamma}}{(c_{\gamma_s \gamma} + b_{\tilde{\gamma}_r} k!)}. \tag{22}\]

Substituting (21) and (22) into (15), we finally obtain an analytical expression for the SOP of the proposed scheme 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 \( \tilde{\gamma}_r \) goes to infinity. By substituting the approximation of \( K_1(\cdot) \) [18],

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

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

\[
P_{\text{out}}^\infty = \left[ c_{\gamma_s \gamma} e_{\gamma_s \gamma} + \eta \ln \left( \frac{b_{\tilde{\gamma}_r}/\eta}{b_{\tilde{\gamma}_r}} \right) \right]^N. \tag{25}\]

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

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

where \( b_{\tilde{\gamma}_r}/\eta = ab_{\tilde{\gamma}_r} (1 - \rho)/(\gamma_s - 1) \). From (25) and (26), we can conclude that the asymptotic SOP becomes worse as \( \rho \) 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 \( \tilde{\gamma}_r \) 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 \( h_{n,s} \) and \( f_n \) and \( g_n \) are assumed to be a combination of path loss and small scale fading, i.e., \( h_n = \gamma^{-\gamma/2} h_n \), \( f_n = f_0^{-\gamma/2} f_n \) and \( g_n = d_0^{-\gamma/2} g_n \), where \( \gamma \) is the path loss exponent, set as \( \gamma = 2 \), and \( d \) is the distance between two nodes. We set \( d_{T_x,n} = d_{R_x,n} = d_{E,n} = 2m \) [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 \( \gamma_s \) 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 \( \tilde{\gamma}_r \).
out
P
out
10
-6
10
-5
10
-4
10
-3
10
-2
10
-1
10
0
P out
Simulation
Analysis
Asymptotic
¯γe= 20dB
¯γe=15dB
¯γe= 10dB
Fig. 3. Secrecy outage probability versus \(\bar{\gamma}_r\) over Rayleigh fading with \(\gamma_e = 10, 15, 20\) dB, \(a = 2, b = 3, c = 1, \rho = 0.5, N = 3\).

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 \(\gamma_e\) on the SOP versus \(\bar{\gamma}_r\) with \(\rho = 0.5, N = 3\). It can be observed that the secrecy performance is degraded as \(\gamma_e\) increases. Moreover, the curves are parallel for different \(\gamma_e\) at high \(\bar{\gamma}_r\), which indicates that the diversity order has nothing to do with the \(\gamma_e\). 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 \(\gamma_e\) 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 \(\rho\) 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 \(\rho\), 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 \(\bar{\gamma}_r\). 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


