On the Physical Layer Security of Backscatter Wireless Systems

Walid Saad, Xiangyun Zhou, Zhu Han, and H. Vincent Poor

***Abstract*—Backscatter wireless communication lies at the heart of many practical low-cost, low-power, distributed passive sensing systems. The inherent cost restrictions coupled with the modest computational and storage capabilities of passive sensors, such as RFID tags, render the adoption of classical security techniques challenging; which motivates the introduction of physical layer security approaches. Despite their promising potential, little has been done to study the prospective benefits of such physical layer techniques in backscatter systems. In this paper, the physical layer security of wireless backscatter systems is studied and analyzed. First, the secrecy rate of a basic single-reader, single-tag model is studied. Then, the unique features of the backscatter channel are exploited to maximize this secrecy rate. In particular, the proposed approach allows a backscatter system's reader to inject a noise-like signal, added to the conventional continuous wave signal, in order to interfere with an eavesdropper's reception of the tag's information signal. The benefits of this approach are studied for a variety of scenarios while assessing the impact of key factors, such as antenna gains and location of the eavesdropper, on the overall secrecy of the backscatter transmission. Numerical results corroborate our analytical insights and show that, if properly deployed, the injection of artificial noise yields significant performance gains in terms of improving the secrecy of backscatter wireless transmission.**

***Index Terms*—Secrecy rate, backscatter communication, artificial noise, physical layer security.**

I. Introduction

BACKSCATTER systems constitute a class of wireless communication networks in which a transceiver, often known as an interrogator or reader, communicates with and powers up neighboring resource-constrained nodes, known as tags, so as to extract useful data. Each tag is an inexpensive, passive (or semi-passive) sensor-like node that contains information (identification data or sensor measurements) that the reader seeks to acquire. Such passive tags do not have their own transmission circuitry, instead, each tag backscatters its information by appending it to the received reader's signal. Thus, the key characteristics of such a backscatter system include the reliance of the tag on the reader's transmitted signal in order to power up and transmit its data as well as the ability of the reader to act as a transmitter, receiver, and source of power for the tag.

Backscatter systems comprise an emerging wireless technology that has become very popular in many practical systems such as distributed passive sensor networks and radio frequency identification (RFID) systems [1]–[10]. In fact, backscatter communication constitutes the backbone of practical RFID systems that enable the interconnection of physical objects through the use of small, inexpensive chips, i.e., RFID tags, which are remotely powered by a wireless RFID reader [2]. In fact, it is envisioned that, with a proper design of the underlying backscatter communication system, state-of-the-art ultra high frequency (UHF) RFID systems will lie at the heart of future cyberphysical systems such as the Internet of things [2]. In order to reap the benefits of backscatter-based communication systems, a variety of technical challenges must be addressed at different levels ranging from the circuit design of tags to advanced backscatter signal processing [1]–[11]. In [2] and [5], the authors discuss various large-scale applications of RFID systems, particularly in sensor networks, that highlight the need for new techniques to secure and optimize RFID systems. The works in [3], [7], and [10] provide the much needed signal processing basis for studying single and multiple antenna backscatter systems, under various radio conditions. The standardization and practical issues pertaining to RFID security are discussed in [4], from a market perspective. Various issues pertaining to the design of RFID tags and their associated load/throughput are studied in [6], [8], and [9]. Finally, the work in [11] discusses collision avoidance protocols that allow readers to communicate with multiple tags.

Beyond the aforementioned technical challenges, securing backscatter communication systems constitutes a key design issue due to the fact that malicious attacks, such as eavesdropping, can lead not only to data interception but also to serious privacy breaches such as owner tracking or identity modification, among others [12]. These breaches are a direct consequence of the ubiquitous nature of backscatter systems in which the tags can be appended to practically every physical object ranging from retail products to transportation systems, and even body area networks. The challenges of securing backscatter-based systems stem from the practical limitations, in terms of cost, size, and computation, which motivate novel approaches to wireless security [13], [14].

In the existing literature, most security solutions tailored toward backscatter communication are based on concepts from the field of lightweight cryptography – a scaled-down

Manuscript received March 18, 2013; revised August 26, 2013 and January 8, 2014; accepted March 4, 2014. The associate editor coordinating the review of this paper and approving it for publication was J. Wallace.

W Saad is with the Electrical and Computer Engineering Department, University of Miami, Coral Gables, FL, USA (e-mail: walid@miami.edu).

X. Zhou is with the Research School of Engineering, Australian National University, Australia (e-mail: xiangyun.zhou@anu.edu.au).

Z. Han is with the ECE Department, University of Houston, Houston, TX, USA (e-mail: zhan2@uh.edu).

H. V. Poor is with the Electrical Engineering Department, Princeton University, Princeton, NJ, USA (e-mail: poor@princeton.edu).

This research was supported in part by the National Science Foundation under Grants CNS-1265268, CNS-1117560, ECCS-1028782, and CNS-0953377, and in part by the Qatar National Research Foundation. A preliminary version of this work was presented as an invited paper at the Ninth International Symposium on Wireless Communication Systems (ISWCS), Paris, France [43].

Digital Object Identifier 10.1109/TWC.2014.051414.130478

version of standard cryptography, such as in [15]–[19] (and references therein). While these approaches provide a good level of security against a number of attacks, they do exhibit important limitations [14], [20]–[22] such as the reliance on key generation, which requires a reasonable amount of computation and storage on the sensor tags and the need for exchange of cryptographic credentials over the backscatter wireless channel, which increases overhead and can still be received by an eavesdropper, even if encrypted. Beyond lightweight cryptographic approaches, some recent works such as in [22], study the feasibility of implementing basic cryptographic schemes such as the RC5 algorithm on resource-constrained tags. However, the results in [22] show that such an implementation is possible only at very short ranges (e.g., 0.75 meters) and by using prototype tags that possess higher storage and computational power, compared to commercial tags such as those following the electric product code (EPC) global standard [23].

One promising direction to overcome some of the limitations of cryptography in backscatter systems is to develop physical layer (PHY) security mechanisms which exploit wireless channel characteristics such as noise, traditionally seen as impediments, for defending wireless transmission against eavesdropping, without the reliance on secret key exchange or generation [24]. PHY security techniques can be used as either an alternative to cryptography or as a complement that can strengthen existing cryptographic techniques by providing a secure transmission channel for key distribution and exchange. Significant research efforts towards developing PHY security mechanisms for standard wireless networks have been recently conducted [24]–[35]. The pioneering work of Wyner in [24] is among the first to suggest the use of the wireless channel characteristics as a means for securing wireless transmission. In [25]–[29], the authors discuss the key parameters involved in the characterization of the secrecy capacity of a variety of wireless channels and provide the needed theoretical tools to study secrecy in a wireless system. The works in [30]–[32] study the use of relaying as a means to optimize secrecy rates in wireless systems while [33] proposes a practical approach to benefit from physical layer security with little information on the eavesdroppers. Other mobile network applications of physical layer security are studied in [34] and [35]. However, all of these existing works are oriented toward traditional cellular-like systems and thus cannot be directly used in a backscatter communication setting. Remarkably, despite the fact that backscatter systems constitute an ideal setting for deploying PHY security mechanisms, little work has been done to study its feasibility and potential as we propose in this paper.

The main contribution of this paper is to study and analyze the physical layer security of a wireless system that employs backscatter communication. To this end, we study the characteristics and properties of the secrecy rate of a backscatter communication system, given the two key features of the backscatter channel: (i)- the nature of the backscatter channel in which the signal transmitted by the reader is modulated and relayed back by the tag to the reader; and (ii)- the presence of a signal continuously transmitted by the reader for powering the tag during communication. Then, we propose an approach to exploit these two features so as to optimize the overall secrecy. In particular, we develop a scheme in which a reader is able to inject a randomly generated noise signal that is added to the conventional continuous wave signal, in order to interfere with the eavesdropper's reception of the tag's backscatter information signal. While this idea of noise injection has been used in the physical layer security literature that deals with conventional cellular systems such as in [32], [36]–[40], its application to wireless backscatter systems is novel. We show that, in order to benefit from the proposed approach, the reader must optimize the allocation of its limited transmit power between its continuous wave and the noise signal. Within the scope of this paper, we focus our attention on the baseline case of a single reader, single tag model. For this model, we analytically derive various results that provide key insights on how and when perfect secrecy can be achieved using the proposed approach. In particular, we study the impact of key factors, such as antenna gains and location of the eavesdropper, on the overall secrecy of the backscatter transmission. Then, we propose an optimization approach that enables the reader to intelligently determine the amount of power that must be allocated to the artificial noise so as to maximize the overall secrecy of the link. Using various numerical results, we evaluate the performance of the proposed approach and show that the injection of artificial noise yields significant performance gains in terms of improving the secrecy of backscatter transmission.

The rest of this paper is organized as follows: Section II presents the system model for the single reader case. In Section III, we present the proposed approach for improving backscatter secrecy and develop the analysis. In Section IV, we analyze the conditions required for achieving positive secrecy. The proposed approach for optimal power allocation is presented and analyzed in Section V. Finally, conclusions are drawn in Section VI.

II. System Model

Consider a backscatter communication system consisting of a single reader and an associated tag. Hereinafter, we will adopt the terms "tag" and "reader" commonly used in RFID systems. However, the analysis and results in the sequel are not limited to RFID systems, but are also applicable to a broad range of backscatter communication systems (e.g., passive sensor networks). The tag holds information (e.g., identification or sensor data) that needs to be sent to the reader. Here, as is typical in backscatter systems, we consider that the tag is passive (or semi-passive where the battery is used as backup power, but not used for transmission), and hence, cannot initiate transmissions on its own [1]. In order to power up the tag, the reader transmits a standardized continuous wave (CW) carrier signal. This signal induces an RF voltage across the tag antenna which is used to power the tag. Subsequently, the tag transmits back its stored information by controlling the amount of backscatter of the impinging CW carrier signal. In other words, the tag does not generate its own signal, but rather appends its information by modulating the carrier signal sent from the reader which is subsequently echoed back to the reader. This communication model is known as a *backscatter communication* [1]. During this backscatter, the reader continuously transmits the CW carrier signal to power the tag circuit while at the same time receiving the echoed

signal containing the tag's information, i.e., operating in full-duplex mode. In this work, we assume that the reader is able to perfectly separate its received signal from the transmitted signal without any signal leakage[1].

Considering the discrete-time signal model in the baseband, the received signal at the reader is given by [1], [41]:

$$y_R = h_{TR}h_{RT}xs + n_R + h_{TR}n_T, \tag{1}$$

where x is the signal transmitted by the reader, s is the tag's information signal, h_{TR} and h_{RT} are, respectively, the tag-reader and reader-tag channel gains (with the antenna gains taken into account), n_R is additive white Gaussian noise (AWGN) at the reader with power σ_R^2, and n_T is AWGN at the tag which is backscattered to the reader with power σ_T^2. The power of the signal transmitted by the reader is denoted by P_x. The fraction of the received power reflected back in the tag's useful information signal is Γ. Note that $\Gamma < 1$ due to the passive nature of the tag [1].

While many channel models exist for backscatter wireless systems, here, we use the Friis equation to model the power loss of signal propagation, which is commonly adopted for communication over a short distance [1], [7]. In this context, for the reader with a transmit power of P_x, the received power following the backscatter is given by

$$P_R^{\text{rx}} = P_x\Gamma G_{RT}^2 K^2 d_{RT}^{-4}, \tag{2}$$

where G_{RT} represents the combined transmitter-receiver antenna gain of the reader-tag link, d_{RT} is the distance between the reader and the tag, and $K = (\lambda/4\pi)^2$ is a constant dependent on the carrier wavelength λ. Therefore, we can define the signal-to-noise ratio (SNR) at the reader as

$$\gamma_R = \frac{P_x\Gamma G_{RT}^2 K^2 d_{RT}^{-4}}{\sigma_R^2 + \sigma_T^2 G_{RT} K d_{RT}^{-2}}. \tag{3}$$

A. Backscatter Physical Layer Security

One of the most challenging tasks in backscatter systems, such as RFIDs, is the ability to secure the transmission against eavesdropping [1], [12], [13] when confidential information needs to be sent from the tag to the reader. Unlike the traditional cryptographic approach, in this work, we explore the potential of incorporating physical layer security techniques for confidential message transmission from the tag to the reader in the presence of an eavesdropper. Figure 1 shows an illustrative example of such a backscatter communication model.

Similar to the received signal model for the reader, the received signal at the eavesdropper is:

$$y_E = h_{TE}h_{RT}xs + n_E + h_{TE}n_{TE}, \tag{4}$$

where h_{TE} is the tag-eavesdropper channel gain (with the antenna gains taken into account), n_E is AWGN at the eavesdropper with power σ_E^2, and n_{TE} is the AWGN backscattered from the tag to the eavesdropper with power σ_{TE}^2. Note

[1]The assumption of perfect signal separation is commonly used in most existing literature of backscatter communication systems [1], [3], [7], [8]. Note that the difficulty of signal separation at the reader increases as the transmitted signal deviates from a pure CW carrier signal in which case a more advanced transceiver is required to keep the signal leakage at a minimal level as discussed in [41]. In this work, we assume a good transceiver design at the reader and hence the signal leakage is not considered in our analysis.

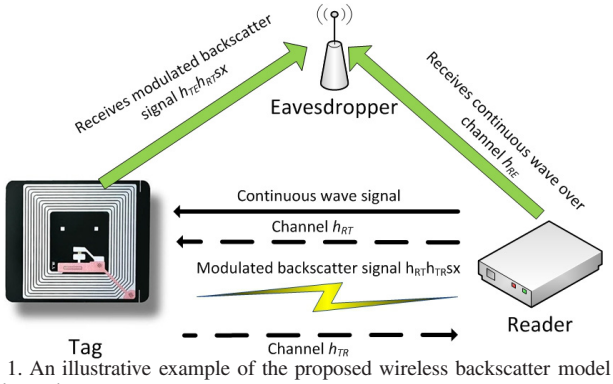


Fig. 1. An illustrative example of the proposed wireless backscatter model in single reader case.

that during the reception of the backscatter signal from the tag, the reader is also transmitting its CW signal which is received by the eavesdropper as well. Thus, the eavesdropper receives the superposition of the CW signal from the reader and the backscattered signal from the tag, because the signals are transmitted continuously. We assume that, in normal backscatter systems, the standardized CW signal is known to the eavesdropper, and hence, can be easily removed from the received signal. This is why this signal term does not appear in (4).

Again using the Friis equation to model the power loss due to signal propagation, the SNR at the eavesdropper is obtained as [1]:

$$\gamma_E = \frac{P_x\Gamma K^2 G_{RT}G_{TE}d_{RT}^{-2}d_{TE}^{-2}}{\sigma_E^2 + \sigma_{TE}^2 G_{TE}K d_{TE}^{-2}}, \tag{5}$$

where G_{TE} represents the combined transmitter-receiver antenna gain of the tag-eavesdropper link, and d_{TE} is the distance between the eavesdropper and the tag.

The performance limits of physical layer security are often characterized by the maximum *secrecy rate* achievable for a given secure transmission scheme. This metric gives the maximum rate at which the transmission of confidential information can be decoded by the legitimate receiver with arbitrarily small error while perfect secrecy against the eavesdropper is maintained. For the backscatter communication considered in this work, the achievable secrecy rate is given by [42]

$$\begin{aligned} C_0^S &= (C_0^R - C_0^E)^+ \\ &= \Big(\log(1+\gamma_R) - \log(1+\gamma_E)\Big)^+ \end{aligned} \tag{6}$$

where $a^+ \triangleq \max(a, 0)$. Here, C_0^R is the capacity of the tag-reader channel and C_0^E is the capacity of the tag-eavesdropper channel. To enable secure communication at the secrecy rate, a properly designed wiretap code is required. From the information-theoretic point of view, different wiretap codes may result in different secrecy levels, e.g., either weak secrecy or strong secrecy [28], although the secrecy rate expression remains the same. In this work, we do not pursue an information-theoretic result on the wiretap coding schemes for achieving a specific type of secrecy. Also, note that the system model can be easily extended to the case in which multiple non-colluding eavesdroppers are present. In such a scenario, C_0^E or equivalently γ_E in (6) would represent the capacity or SNR of the eavesdropper with the strongest signal reception, whereas

the effects of all the other eavesdroppers are irrelevant. Here, we note that, although the case of colluding eavesdroppers is also interesting, in a backscatter system, given the form factor and scale of the system, it is difficult for small, bug-like eavesdroppers to cooperate or perform coordinated attacks, due to cost, size, and computational restrictions. However, the results generated in the subsequent sections can still shed light on this interesting case via some of the parameters pertaining to the eavesdropper's antenna capabilities. For future work, it is indeed of interest to study how collusive eavesdropping can occur in a backscatter system, while taking into account the physical restrictions on the eavesdroppers and while considering the dynamics of such collusive attacks.

From (6), one can see that the condition for having a positive secrecy rate is given by $\gamma_R > \gamma_E$. This condition can be easily violated if the eavesdropper has a very sensitive receiver as compared to the reader, i.e., $\sigma_E^2 \ll \sigma_R^2$ and the tag's backscattered noise power σ_{TE}^2 is small. This is a crucial concern for secrecy, because the receiver noise of the eavesdropper is uncontrollable or even unknown to the reader. In the next section, we propose a low complexity, yet effective noise-injection technique that can significantly improve the physical layer security of backscatter systems and allow secure transmission even when the eavesdropper's receiver noise is arbitrarily small. We then analyze this proposed approach under different scenarios so as to highlight the potential of using PHY security within a backscatter system.

III. The Proposed Noise Injection Scheme

For improving the physical layer security performance, one can explore a key feature of backscatter communication, that is, the CW signal is continuously transmitted by the reader for powering the passive tag during the backscatter communication and, due to the broadcast nature of the wireless channel, this signal is received by the eavesdropper as well. Unfortunately, the conventional CW signal is known to the eavesdropper and hence, does not interfere with the eavesdropper's reception of the tag's backscatter signal. Hence, we propose to superimpose a noise-like random signal generated privately, by the reader on the conventional CW signal. This random signal is statistically identical to AWGN so that the eavesdropper cannot distinguish it from its receiver noise. Hence, instead of transmitting x, the reader transmits $x + z$, where z is the injected noise signal with power P_z. The total transmit power of the reader becomes $P = P_x + P_z$. During the backscatter communication, the received signal at the reader becomes

$$y_R = h_{TR}h_{RT}xs + h_{TR}h_{RT}zs + n_R + h_{TR}n_T, \quad (7)$$

where the first term in the useful signal and the last three terms constitute the combined noise. Note that z in (7) is the noise signal that arrived at the reader after going through the round-trip propagation with unknown delays (due to phase and time shifts) caused by the signal propagation as well as the tag processing. Hence, it is difficult for the reader, which is often a resource-constrained device in RFID systems, to recover the value of z without additional costs, such as channel training and tracking. However, we do note that, if such costs do not constitute a major barrier, then noise cancelation can be done via standard signal processing technique which exploit the fact that the reader itself generated the noise and thus has prior knowledge of the noise signal z. In addition, as the reader is continuously transmitting to the tag, it can infer the tag-reader channel, based on its knowledge of the reader-tag channel, which are often correlated. Nonetheless, in order to account for the possibility that the reader partially cancels this backscattered noise, we will introduce an attenuation factor κ that reflects how successful the reader is in canceling the backscattered noise. However, in practice, as we will see in the subsequent numerical results, the power needed to transmit z for achieving good secrecy performance is usually much smaller than the power of the conventional CW signal x. Hence, the second term in (7) is usually negligible compared to the first term, which implies that, practically, there is little benefit from detecting the backscattered z signal. Moreover, we note that, in contrast to the reader, the eavesdropper may have difficulty in performing a similar noise attenuation due to two main factors: a) the eavesdropper does not have knowledge of the random noise signal that the reader has generated and b) in a backscatter system, an eavesdropper is often a small device with highly limited computational capabilities which prevent it from having an advanced receiver structure.

Given the noise injection described above, the SNR of the backscatter received signal at the reader is given by

$$\gamma_R = \frac{P_x \Gamma G_{RT}^2 K^2 d_{RT}^{-4}}{\kappa P_z \Gamma G_{RT}^2 K^2 d_{RT}^{-4} + \sigma_R^2 + \sigma_T^2 G_{RT} K d_{RT}^{-2}}, \quad (8)$$

where $0 \leq \kappa \leq 1$ is the noise attenuation factor.

The main objective of the proposed noise injection at the reader is to create additional interference at the eavesdropper during the reception of the backscatter signal from the tag. The signal received by the eavesdropper (after removing the conventional CW signal that arrived directly from the reader's transmission) is hence given by

$$y_E = h_{TE}h_{RT}xs + h_{TE}h_{RT}zs + h_{RE}z' + n_E + h_{TE}n_{TE}, \quad (9)$$

where z is the received backscattered noise signal from the tag while z' is the injected noise signal received at the eavesdropper directly from the reader (over the reader-eavesdropper channel), i.e., z and z' represent the transmitted noise signals that are received by the eavesdropper at different time instants (hence slightly different notations are used here). Note that the power of the directly received noise z' is typically much larger than the power of the backscattered noise z. Neither z nor z' is known to the eavesdropper. But, the eavesdropper, if equipped with a directional antenna, can minimize or potentially zero its antenna gain towards the reader, effectively removing the third term in (9) from its received signal. However, in this case, the noise injection would still be beneficial due to the impact of the backscattered noise seen in the second term of (9).

The SNR of the received signal at the eavesdropper is given by (10) where G_{RE} represents the combined transmitter-receiver antenna gain of the reader-eavesdropper link, and d_{RE} is the distance between the reader and the tag. Compared with the eavesdropper SNR without noise injection, given in (5), the benefit of noise injection is clear: the reader can now limit the eavesdropper's SNR by controlling the injected noise power.

$$\gamma_E = \frac{P_x \Gamma G_{RT} G_{TE} K^2 d_{RT}^{-2} d_{TE}^{-2}}{P_z G_{RE} K d_{RE}^{-2} + P_z \Gamma G_{RT} G_{TE} K^2 d_{RT}^{-2} d_{TE}^{-2} + \sigma_E^2 + \sigma_{TE}^2 G_{TE} K d_{TE}^{-2}}, \tag{10}$$

One can also characterize the secrecy performance of the backscatter channel by deriving the achievable secrecy rate of the proposed noise injection scheme. Unfortunately, the exact secrecy rate expression is difficult to obtain due to the non-Gaussian distribution of the combined noise at the eavesdropper. However, we can still use the derived SNR expressions to obtain an approximation of the secrecy rate that can quantify the overall secrecy of the transmission, given as

$$\begin{aligned} C^S &= (C_0^R - C_0^E)^+ \\ &\approx \Big(\log(1+\gamma_R) - \log(1+\gamma_E)\Big)^+, \end{aligned} \tag{11}$$

where γ_R and γ_E are given by (8) and (10), respectively. As discussed previously, the receiver noise at the eavesdropper is uncontrollable and unknown, a robust design approach should aim to provide secrecy in the worst-case scenario by assuming $\sigma_E^2 = \sigma_{TE}^2 = 0$ (with such a worst-case assumption, secrecy is not achievable without noise injection). Therefore, in the subsequent sections of the paper, we provide the performance analysis and design for the worst-case scenario by assuming no noise at the eavesdropper.

IV. Conditions for Positive Secrecy Rate

In this section, we investigate the conditions under which positive secrecy rate can be achieved, i.e., $C^S > 0$. In other words, we seek to better understand the conditions under which the transmission of confidential information is possible with perfect secrecy against the eavesdropper. From (11), the condition for positive secrecy rate reduces to $\gamma_R > \gamma_E$. Using the SNR expressions given in (8) and (10), with the assumption of $\sigma_E^2 = \sigma_{TE}^2 = 0$, this condition is given by

$$\left(\frac{d_{TE}}{d_{RE}}\right)^2 > \frac{G_{TE}}{G_{RE}} \left[\frac{d_{RT}^2 \sigma_R^2 + K G_{RT} \sigma_T^2}{K G_{RT} P_z} - (1-\kappa)\Gamma G_{RT} K d_{RT}^2\right]. \tag{12}$$

From the above condition, we see that noise injection, i.e., $P_z > 0$, is necessary for achieving positive secrecy rate. We can also clearly see that the relative distance of the eavesdropper, i.e., d_{TE}/d_{RE} is an important factor. If the eavesdropper is located close to the tag but far away from the reader, i.e., $d_{TE}/d_{RE} \ll 1$, achieving secrecy becomes a difficult task which requires the reader to inject a strong noise signal. Theoretically, a positive secrecy rate is always achievable with noise injection if the reader does not have a limited power budget for noise injection. This is due to the fact that, by increasing the value of P_z, one can always decrease the right hand side of (12) down to or even below zero. In practice, however, the reader's transmit power is limited (e.g., the maximum transmission power of an RFID reader is typically 30 dBm or 1 Watt [1]). In what follows, we discuss several interesting cases to obtain further insight into when positive secrecy rate can be achieved within various scenarios.

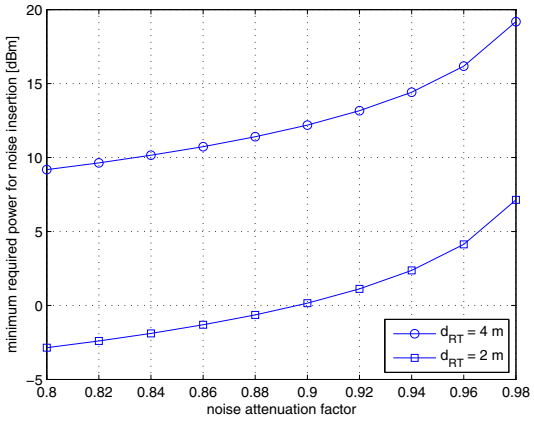


Fig. 2. The minimum required power for noise injection P_z according to (13) for a range of noise attenuation factors κ. The reader-tag distance is set to either 2 m (indicated by square markers) or 4 m (indicated by circular markers). The other system parameters are: the carrier frequency $f_c = 915$ MHz, the tag signal power coefficient $\Gamma = 1/3$, and the receiver noise power $\sigma^2 = -90$ dBm.

A. Case One: Noise Attenuation Enabled at Reader

In this case, we have $\kappa < 1$ and the reader is able to attenuate the noise signal that it injected. With such a noise attenuation, a positive secrecy rate is achievable with a finite noise injection power, regardless of the eavesdropper's location and hardware capability. To see this, we look at the condition for positive secrecy rate given in (12). In order to satisfy this condition regardless of the eavesdropper's parameters, we require the right hand side of (12) to be non-positive. This is satisfied when

$$P_z > \frac{d_{RT}^4 \sigma_R^2 + d_{RT}^2 K G_{RT} \sigma_T^2}{(1-\kappa)\Gamma G_{RT}^2 K^2}, \tag{13}$$

the right hand side of which is finite when $\kappa < 1$. Therefore, as long as the reader is able to adjust the power of the injected noise so as to satisfy (13), secure communication is possible irrespective of the location and antenna gains of the eavesdropper.

Numerical Example: Here we use a numerical example to illustrate the amount of noise power required to guarantee the existence of secure communication. Consider a backscatter communication system with carrier frequency $f_c = 915$ MHz, the tag signal power coefficient $\Gamma = 1/3$, and the AWGN power $\sigma_R^2 = \sigma_T^2 = -90$ dBm. The combined antenna gain of the reader-tag link is assumed to be one, i.e., $G_{RT} = 1$. Typical reader-tag distances of $d_{RT} = 2$ m and $d_{RT} = 4$ m are assumed [1].

Figure 2 shows the minimum required power for noise injection according to (13) for a range of noise attenuation factors. First, this figure clearly shows that as the attenuation capability of the reader gets weaker, i.e., as κ increases, there is a need for a stronger noise signal so as to maintain positive secrecy. Second, Figure 2 conveys a clear message: even with a very insignificant amount of attenuation, e.g., $\kappa = 0.98$,

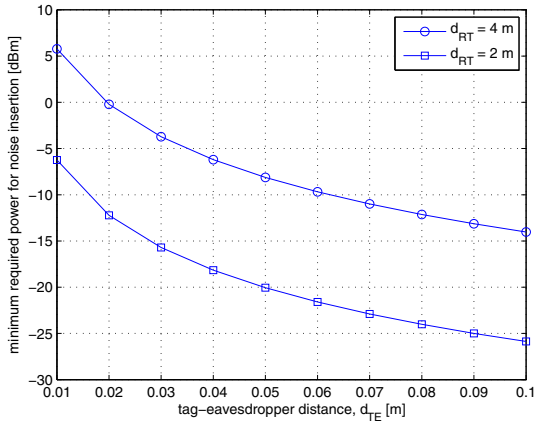


Fig. 3. The minimum required power for noise injection P_z according to (14) for a range of tag-eavesdropper distances d_{TE}. The other system parameters are: the carrier frequency $f_c = 915$ MHz, the tag signal power coefficient $\Gamma = 1/3$, and the receiver noise power $\sigma^2 = -90$ dBm. The reader-tag distance is set to either 2 m (indicated by square markers) or 4 m (indicated by circular markers). The reader, the tag, and the eavesdropper are located on a straight line in this order and they are all equipped with omnidirectional antennas.

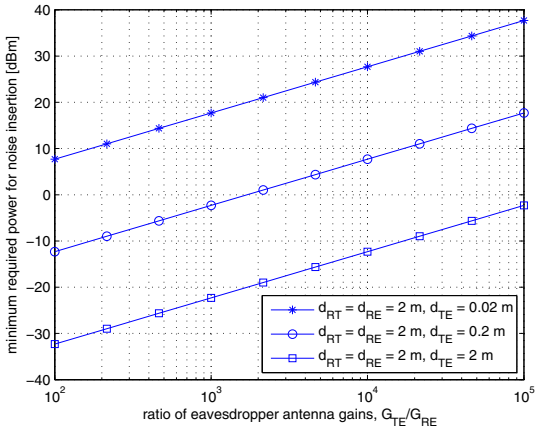


Fig. 4. The minimum required power for noise injection P_z according to (12) versus the eavesdropper's antenna gain ratio G_{TE}/G_{RE}. The reader-tag distance and the reader-eavesdropper distance are set to the same fixed value of $d_{RT} = d_{RE} = 2$ m. The tag-eavesdropper distance is set to three different values: $d_{TE} = 0.02$ m, $d_{TE} = 0.2$ m, and $d_{TE} = 2$ m. The other system parameters are: the carrier frequency $f_c = 915$ MHz, the tag signal power coefficient $\Gamma = 1/3$, and the receiver noise power $\sigma^2 = -90$ dBm. The reader's and tag's antenna gains are set to one.

we are able to achieve secure communication by injecting a relatively small amount of noise, e.g., $P_z = 19.2$ dBm for $d_{RT} = 4$ m or $P_z = 7.2$ dBm for $d_{RT} = 2$ m. These power values are lower than the typical transmit power of an RFID reader, and hence are very practical.

B. Case Two: No Noise Attenuation and Omnidirectional Antennas

Case Two can be considered as a baseline case in which the reader does not pursue additional signal processing for noise attenuation (i.e., $\kappa = 1$) and all communication terminals are equipped with a single omnidirectional antenna. In this case, the condition for positive secrecy rate reduces to

$$\left(\frac{d_{TE}}{d_{RE}}\right)^2 > \frac{d_{RT}^2\sigma_R^2 + KG_{RT}\sigma_T^2}{KP_z}$$
$$\text{or} \qquad P_z > \frac{d_{RE}^2}{d_{TE}^2}\frac{d_{RT}^2\sigma_R^2 + KG_{RT}\sigma_T^2}{K}. \tag{14}$$

For this case, in general, the minimum required noise power depends on the location of the eavesdropper. As the eavesdropper gets closer to the tag, the minimum required noise power increases towards infinity and achieving positive secrecy becomes more challenging. Therefore, it is interesting to study how close the eavesdropper can get to the tag for practical values of the noise power generated by the reader. To this end, we consider the same numerical example as described in Subsection IV-A. For simplicity, we assume that the reader, the tag, and the eavesdropper are located on a straight line in this order, which actually represents a worst-case assumption.

Numerical Example: Figure 3 shows the minimum required power for noise injection according to (14) for a range of tag-eavesdropper distances. In Figure 3, we can see that as the tag-eavesdropper distance becomes smaller, a stronger noise signal would be required to achieve positive secrecy. In particular, Figure 3 conveys a very promising potential for the proposed approach: Even with a very small amount of noise injection, e.g., $P_z = 5.8$ dBm, we allow the eavesdropper to be located as close as 1 cm away from the tag and we can still achieve a positive secrecy rate.

We note that, in this scenario, the worst-case eavesdropper's location in fact depends on the actual application or scenario being considered. For example, if one can physically prevent any person or device from being closer than a certain distance (say 1 meter) away from the tag, the worst-case location can be defined as this distance.

C. Case Three: No Noise Attenuation and Worst-Case Eavesdropper Antenna Gains

In this subsection, we consider the scenario in which the eavesdropper is an advanced device that is equipped with a directional antenna with high directivity. In this case, it is possible for the eavesdropper to place a null towards the reader and/or steer its main antenna beam towards the tag. Theoretically, whenever we have either $G_{RE} = 0$ or $G_{TE} \to \infty$, the condition in (12) is always violated if the reader does not have noise attenuation capabilities. In practice, the values of G_{RE} and G_{TE} are usually finite, but often unknown to the reader. From a secure transmission design point of view, one can assume some worst-case (finite) antenna gains for the eavesdropper and carry out the design accordingly so as to evaluate the potential of noise injection in maintaining positive secrecy. In particular, here, we numerically investigate the minimum required power for noise injection for different values of the eavesdropper's antenna gains. We consider a setup similar to the numerical example described in Subsection IV-A. For ease of illustration, we assume that the reader-tag and reader-eavesdropper distances are the same. On the other hand, we vary the tag-eavesdropper distance to include the effect of eavesdropper location. The antenna gains of the reader and tag are assumed to be one.

Numerical Example: Figure 4 shows the minimum required power for noise injection according to (12), with $\kappa = 0$, for different eavesdropper's antenna gains. In particular, we have considered a wide range of antenna gains with high

directivity. Figure 4 shows that as the eavesdropper's antenna directivity becomes higher, a larger amount of power is needed for the noise signal. Nonetheless, in Figure 4, we can see that, when the eavesdropper is equipped with an expensive directional antenna with $G_{TE}/G_{RE} = 10^5$, the amount of noise power required depends on how close the eavesdropper is to the tag. For a typical tag-eavesdropper distance of $d_{TE} = 2$ m, a very small noise power is usually sufficient to guarantee the existence of secure communication at a positive secrecy rate. As the eavesdroppers becomes closer to the tag, higher (but usually practical) noise powers would be required as shown in Figure 4. Figure 4 provides a network designer with the necessary results to investigate which worst-case antenna gains and eavesdropping location parameters must be considered for dimensioning the RFID system and designing the physical layer security scheme. In particular, the designer can first estimate the capability of an advanced eavesdropping device by specifying its worst-case location and antenna gain. Then, the designer can use the derived analytical results to compute the minimum required artificial noise power to thwart the eavesdropping threat. For example in Figure 4, if the worst-case distance between tag and eavesdropper is about 20 cm and the eavesdropper has a highly directional antenna gain with a ratio of around 10^4, the required artificial noise power is about 8.5 dBm.

In this section, all the numerical results have shown that the tag noise has a negligible effect on the overall secrecy results. This is due to the fact that the backscattered tag noise power received at the reader is much smaller than the reader's own noise power. Therefore, in the remainder of the paper, we ignore the tag noise for simplicity.

V. Optimal Power Allocation for Noise Injection

In the previous section, we have seen that secure communication at a positive secrecy rate can usually be achieved by inserting a small amount of noise at the reader. In practice, the maximum transmit power of the reader is limited, and hence, this power needs to be allocated between the conventional CW signal and the proposed, injected noise signal. Clearly, the performance, in terms of the secrecy rate, depends heavily on this power allocation. In this section, we consider the problem of optimally allocating the total transmission power at the reader between the conventional CW signal and the injected noise in order to maximize the achievable secrecy rate given in (11). To perform this power allocation, the reader must be able to estimate the reader-tag channel. To do so, two approaches can be followed. On the one hand, the reader can use the backscatter signal to estimate the channel. This can be done either jointly with the signal detection or during an initial training phase with the tag. On the other hand, the reader can use MAC-level handshaking protocols (such as those in [1, Chapter 8]) to estimate this channel. Moreover, the reader and tag in a backscatter system are often located at small distances, which makes it easier to estimate the reader-tag channel.

To study the optimal power allocation problem, we define the ratio of power allocated to the conventional CW signal as $\alpha \in (0, 1]$. Hence, we have

$$P_x = \alpha P \qquad \text{and} \qquad P_z = (1-\alpha)P. \tag{15}$$

Hereinafter, we focus on the more interesting case in which a positive secrecy rate can be made possible with the given reader's power budget. From the condition for positive secrecy rate given in (12), we know that the noise power P_z cannot be zero, in other words, α should be strictly less than 1. This implies that there must exist an optimal value of $\alpha \in (0, 1)$.

A. Analytical Solution

The power optimization problem can be written as

$$\arg\max_{\alpha} \frac{1+\gamma_R}{1+\gamma_E} \quad \triangleq \quad \arg\max_{\alpha} f(\alpha), \tag{16}$$

where γ_R and γ_E are given in (8) and (10), respectively, with $\sigma_E^2 = 0$ (recall the worst-case assumption on the eavesdropper's receiver noise).

In general, the objective function $f(\alpha)$ may not be concave. Nevertheless, the optimal α can be easily found since the first derivative of $f(\alpha)$ w.r.t. α gives a quadratic equation in α. In particular, by setting the first derivative of $f(\alpha)$ to 0, we obtain the two local extrema as

$$\alpha_1 = 1 - \frac{\sqrt{a(a+\kappa)[a(b-1)+b-\kappa]} - a(1-\kappa)}{a(b-1)+\kappa(b-\kappa)}, \tag{17}$$

$$\alpha_2 = 1 + \frac{\sqrt{a(a+\kappa)[a(b-1)+b-\kappa]} + a(1-\kappa)}{a(b-1)+\kappa(b-\kappa)}, \tag{18}$$

where

$$a = \frac{\sigma_R^2 d_{RT}^4}{P\Gamma G_{RT}^2 K^2}, \qquad \text{and} \qquad b = 1 + \frac{G_{RE} d_{RT}^2 d_{TE}^2}{\Gamma G_{RT} G_{TE} K d_{RE}^2}.$$

Since $b > 1 \geq \kappa$, it is not difficult to show that $\alpha_2 > 1$ and hence is outside the feasible range. Also, because the optimal α cannot be either 0 or 1, we conclude that α_1 gives the optimal ratio of power allocation.

B. Numerical Results

Although the analytical result on the optimal power allocation was derived in a nice closed form in (17), it cannot be easily used to explore the impacts of various system parameters on the power allocation design. In particular, we are interested in how the optimal power allocation changes as the eavesdropper's location or antenna gain changes. In what follows, we carry out numerical analysis to clearly show the impact of the eavesdropper parameters on the power allocation and on the achievable secrecy rate.

Consider a backscatter communication system with carrier frequency $f_c = 915$ MHz, the tag signal power $\Gamma = 1/3$, and the receiver noise power $\sigma^2 = -90$ dBm. The total transmission power budget of the reader is set to $P = 20$ dBm. The reader is assumed to have no noise attenuation capability. The antenna gains of the reader and tag are assumed to be one.

Impact of the Eavesdropper Location: First, we study the impact of the eavesdropper's location on the power allocation strategy at the reader. Here, for simplicity, we assume that the reader, the tag, and the eavesdropper are located on a straight line in this order and that they are all equipped with omnidirectional antennas.

Figure 5 shows the optimal value of α versus the tag-eavesdropper distance d_{TE} ranging from 0 to 1 m. The reader-tag distance is fixed to either 2 m or 4 m. From Figure 5,

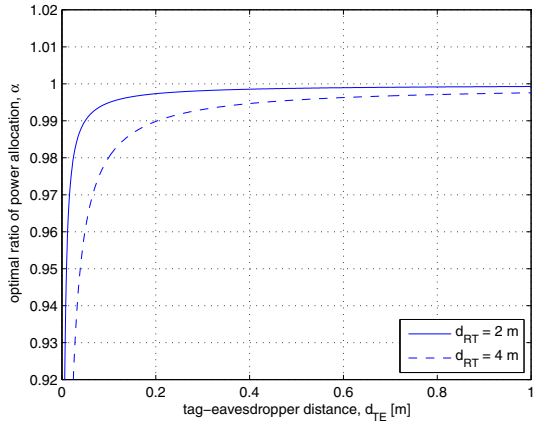


Fig. 5. The optimal value of α versus the tag-eavesdropper distance d_{TE}. The other system parameters are: the carrier frequency $f_c = 915$ MHz, the tag signal power coefficient $\Gamma = 1/3$, and the receiver noise power $\sigma^2 = -90$ dBm. The reader-tag distance is set to either 2 m (indicated by the solid line) or 4 m (indicated by the dashed line). The reader, the tag, and the eavesdropper are located on a straight line in this order and they are all equipped with omnidirectional antennas. The total transmission power budget of the reader $P = 20$ dBm.

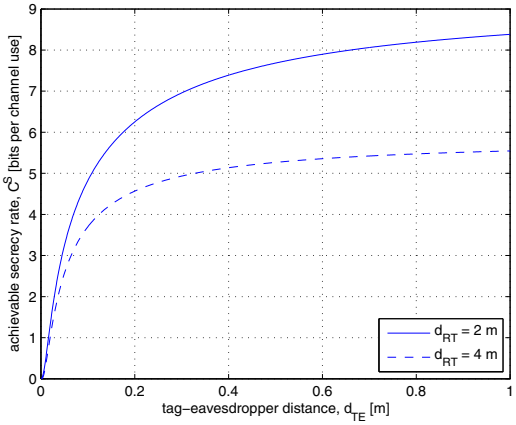


Fig. 6. The achievable secrecy rate C^S with optimal power allocation versus the tag-eavesdropper distance d_{TE}. The other system parameters are: the carrier frequency $f_c = 915$ MHz, the tag signal power coefficient $\Gamma = 1/3$, and the receiver noise power $\sigma^2 = -90$ dBm. The reader-tag distance is set to either 2 m (indicated by the solid line) or 4 m (indicated by the dashed line). The reader, the tag, and the eavesdropper are located on a straight line in this order and they are all equipped with omnidirectional antennas. The total transmission power budget of the reader $P = 20$ dBm.

we can see that the optimal value of α is very close to 1 for nearly all possible values of the tag-eavesdropper distance (including the values of $d_{TE} > 1$ not shown in the figure for ease of presentation), which implies that only a tiny fraction of power is needed for noise injection in order to achieve the optimal physical layer security performance. Only when the tag-eavesdropper distance approaches 0, does the optimal α starts to drop significantly and quickly approaches 0.

Figure 6 shows the secrecy rate C^S achieved by using the optimal value of α. Note that under the worst-case assumption $\sigma_E = 0$, secure communication is not possible without noise injection. In Figure 6, we can first see that the achievable secrecy rate strongly depend on the tag-eavesdropper distance. Indeed, as this distance becomes smaller, the secrecy rate performance becomes smaller. Nonetheless, this figure clearly show the benefit of noise injection. In particular, it shows that the system can enjoy good secrecy rate performance even if the eavesdropper is located very close to the tag, e.g., more than 3 bits per channel use is achievable even when the eavesdropper is only 0.1 meters away from the tag.

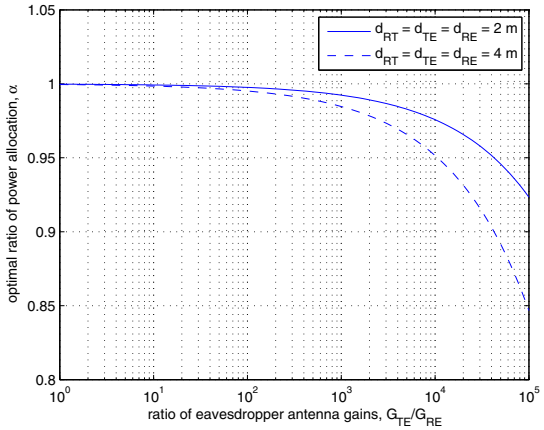


Fig. 7. The optimal value of α versus the eavesdropper's antenna gain ratio G_{TE}/G_{RE}. The reader-tag distance and the reader-eavesdropper distance and the tag-eavesdropper distance are set to the same fixed value of either $d_{RT} = d_{TE} = d_{RE} = 2$ m (indicated by the solid line) or $d_{RT} = d_{TE} = d_{RE} = 4$ m (indicated by the dashed line). The other system parameters are: the carrier frequency $f_c = 915$ MHz, the tag signal power coefficient $\Gamma = 1/3$, and the receiver noise power $\sigma^2 = -90$ dBm. The reader's and tag's antenna gains are set to one. The total transmission power budget of the reader $P = 20$ dBm.

Impact of the Eavesdropper Antenna Gains: Next, we study the impact of the eavesdropper's antenna gains when it is equipped with a directional antenna with potentially high directivity. By either minimizing the antenna gain towards the reader G_{RE} or maximizing the antenna gain towards the tag G_{TE}, the eavesdropper is able to improve its SNR. From the expression for γ_E in (10), we can see that (with the assumption of $\sigma_E = 0$) the ratio of the eavesdropper antenna gain, i.e. G_{TE}/G_{RE}, is an important factor. Therefore, we will consider different values of G_{TE}/G_{RE}. For simplicity, the reader-tag distance and the reader-eavesdropper distance and the tag-eavesdropper distance are set to the same fixed value of either $d_{RT} = d_{TE} = d_{RE} = 2$ m or $d_{RT} = d_{TE} = d_{RE} = 4$ m.

Figure 7 shows the optimal value of α versus the eavesdropper's antenna gain ratio G_{TE}/G_{RE} ranging from 1 to 10^5. Again, we see that the optimal value of α is very close to 1 for a wide range of practical antenna gains. Only when the gain ratio goes beyond 10^3, does the optimal α start to drop, but still remains at a large value even if the gain ratio reaches 10^5. This implies that, for most practical antenna gains, a small portion of the power is needed for noise injection.

Figure 8 shows the secrecy rate C^S achieved by using the optimal value of α. In this figure, we can see that as the ratio of eavesdropper antenna gains increases, the overall secrecy decreases since the eavesdropper is able to cancel out the additional interference over the reader-eavesdropper channel. This decrease has a steeper slope when the eavesdropper is closer to the tag, i.e., for the case in which $d_{RT} = d_{TE} = d_{RE} = 2$ m. Nonetheless, Figure 8 clearly demonstrates that, using the proposed noise injection approach, the system is still able to guarantee a positive secrecy rate even if the gain ratio reaches a value as large as 10^5.

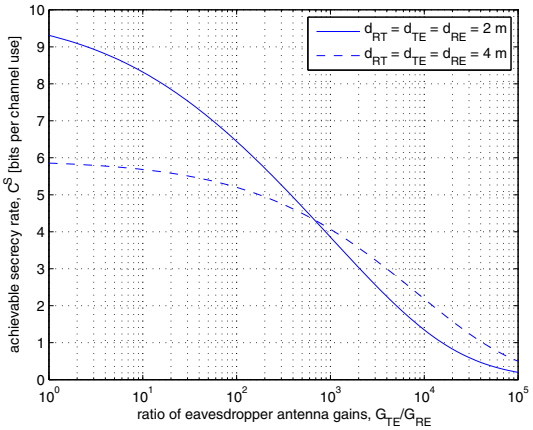


Fig. 8. The achievable secrecy rate C^S with optimal power allocation versus the eavesdropper's antenna gain ratio G_{TE}/G_{RE}. The reader-tag distance and the reader-eavesdropper distance and the tag-eavesdropper distance are set to the same fixed value of either $d_{RT} = d_{TE} = d_{RE} = 2$ m (indicated by the solid line) or $d_{RT} = d_{TE} = d_{RE} = 4$ m (indicated by the dashed line). The other system parameters are: the carrier frequency $f_c = 915$ MHz, the tag signal power coefficient $\Gamma = 1/3$, and the receiver noise power $\sigma^2 = -90$ dBm. The reader's and tag's antenna gains are set to one. The total transmission power budget of the reader $P = 20$ dBm.

VI. Conclusions

In this paper, we have presented an analysis of the physical layer security of wireless systems that employ backscatter communication for transmission. First, we have studied the properties and characteristics of physical layer security in a single reader backscatter system. Then, we have proposed to inject a noise signal at the reader for optimizing the overall secrecy rate while exploiting the unique features of the backscatter channel. We have derived the conditions under which positive secrecy is achievable, under a variety of scenarios that reflect the various capabilities of the legitimate nodes and the eavesdropper. Furthermore, we have shown that the use of such added noise can significantly improve the secrecy of backscatter communication, given proper allocation of power between the continuous wave and the injected noise signals. After deriving a closed-form solution for the optimal power allocation problem, we have numerically studied the achievable performance. Our numerical results have provided important insights into the physical layer security performance of backscatter systems while showing that the proposed noise injection approach can significantly assist in maintaining positive secrecy and a reasonable secrecy rate, under various network scenarios. For future work, one interesting aspect is to investigate how to exploit backscatter channel characteristics, such as propagation delays, to generate secret keys from the physical layer of the backscatter. Here, the reader and tag can exploit the differences in the signal's signature over the tag-reader channel as opposed to the tag-eavesdropper/reader-eavesdropper channel to generate such a secret key. Other extensions can address a variety of issues such as studying the multi-reader/tag case, designing more efficient, backscatter-oriented secrecy achieving codes that are of low complexity, and investigating various elaborate backscatter radio propagation environments.

References

[1] D. M. Dobkin, *The RF in RFID: Passive UHF RFID in Practice*. Newnes, 2007.

[2] S. Roy, V. Jandhyala, J. R. Smith, D. J. Wetherall, B. P. Otis, R. Chakraborty, M. Buettner, D. J. Yeager, Y. C. Ko, and A. P. Sample, "RFID: from supply chains to sensor nets," *Proc. IEEE*, vol. 98, no. 9, pp. 1583–1592, Aug. 2010.

[3] J. D. Griffin, G. D. Durgina, A. Haldi, and B. Kippelen, "RF tag antenna performance on various materials using radio link budgets," *IEEE Antennas Wireless Propag. Lett.*, vol. 5, no. 1, pp. 247–250, Dec. 2006.

[4] T. Philips, T. Karygiannis, and R. Kuhn, "Security standards for the RFID market," *IEEE Security Privacy*, vol. 3, no. 6, pp. 85–89, Nov. 2005.

[5] A. O. Bicen and O. B. Akan, "Energy-efficient RF source power control for opportunistic distributed sensing in wireless passive sensor networks," in *Proc. 2012 IEEE Symp. Comput. Commun.*

[6] A. Blestas, A. G. Dimitriou, and J. N. Sahalos, "Improving backscatter radio tag efficiency," *IEEE Trans. Microwave Theory Techniques*, vol. 58, no. 6, pp. 1502–1509, June 2010.

[7] 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, Feb. 2008.

[8] P. Zhang, J. Gummeson, and D. Ganesan, "BLINK: a high throughput link layer for backscatter communication," in *Proc. 2012 International Conf. Mobile Syst., Applications Services.*

[9] H. Yoshida, S. Sekine, Y. Fujita, T. Suzuki, and S. Otaka, "A 950-MHz rectifier circuit for sensor network tags with 10-m distance," *IEEE J. Solid State Circuits*, vol. 41, no. 1, pp. 35–41, Jan. 2006.

[10] D. Arnitz, U. Muehlmann, and K. Witrisal, "Wideband characterization of backscatter channels: derivations and theoretical background," *IEEE Trans. Antennas Propag.*, vol. 60, no. 1, pp. 257–266, Jan. 2012.

[11] L. Kang, K. Wu, J. Zhang, H. Tan, and L. Ni, "DDC: a novel scheme to directly decode the collisions in UHF RFID systems," *IEEE Trans. Parallel Distributed Comput.*, vol. 23, no. 2, pp. 263–270, Dec. 2011.

[12] A. Juels, "RFID security and privacy: a research survey," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 381–394, Feb. 2006.

[13] ——, "Minimalist cryptography for low-cost RFID tags," in *Proc. 2004 Int. Conf. Security Commun. Netw.*

[14] E. Vahedi, R. K. Ward, and I. Blake, "Security analysis and complexity comparison of some recent lightweight RFID protocols," in *Proc. 2011 Int. Conf. Computational Intelligence Security Inf. Syst.*

[15] S. Piramuthu, "SASI: a new ultralightweight RFID authentication protocol providing strong authentication and strong integrity," *IEEE Trans. Dependable Secure Comput.*, vol. 4, no. 4, pp. 337–340, Dec. 2007.

[16] P. H. Cole and D. C. Ranasinghe, *Networked RFID Systems and Lightweight Cryptography: Raising Barriers to Product Counterfeiting*. Springer, 2007.

[17] B. Calmels, S. Canard, M. Girault, and H. Sibert, "Low-cost cryptography for privacy in RFID systems," in *Proc. 2006 IFIP Int. Conf. Smart Card Research Advanced Applications.*

[18] Y. Cui, K. Kobara, K. Matsuura, and H. Imai, "Lightweight asymmetric privacypreserving authentication protocols secure against active attack," in *Proc. 2007 Int. Workshop Pervasive Comput. Commun. Security.*

[19] P. Peris-Lopez, J. C. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda, "M2AP: a minimalist mutual-authentication protocol for low-cost RFID tags," in *Proc. 2006 Int. Conf. Ubiquitous Intelligence Comput.*

[20] B. Defend, K. Fu, and A. Juels, "Cryptanalysis of two lightweight RFID authentication schemes," in *Proc. 2007 Int. Workshop Pervasive Comput. Commun. Security.*

[21] T. Li and G. Wang, "Security analysis of two ultra-lightweight RFID authentication protocols," in *Proc. 2007 IFIP SEC.*

[22] H.-J. Chae, D. J. Yeager, J. R. Smith, and K. Fu, "Maximalist cryptography and computation on the WISP UHF RFID tag," in *Proc. 2007 RFID Security.*

[23] EPCGlobal, "EPC radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications," Tech. Rep. Available: http://www.epcglobalinc.org

[24] A. D. Wyner, "The wire-tap channel," *Bell System Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[25] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wire-tap channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, Article ID 142374, 12 pages, 2009.

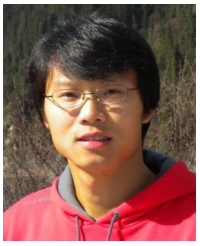
[26] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Sept. 2008.

[27] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 2007 Conf. Inf. Sciences Syst.*

[28] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.
[29] Y. Liang, L. Lai, S. Shamai, and H. V. Poor, "A broadcast approach for fading wiretap channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 842–858, Feb. 2014.
[30] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
[31] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: interaction between source, eavesdropper and friendly jammer," *EURASIP J. Wireless Commun. Netw., Special Issue on Wireless Physical Layer Security*, vol. 2009, June 2009.
[32] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two way relay communications with untrusted relay and friendly jammers," *IEEE Trans. Veh. Technol.*, to appear, 2012.
[33] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *Proc. 2011 IEEE INFOCOM*.
[34] Y. Liang, H. V. Poor, and L. Ying, "Secrecy throughput of MANETs with active and passive attacks," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6692–6702, Oct. 2011.
[35] S. Vasudevan, D. Goeckel, and D. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *Proc. 2010 ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, pp. 21–30.
[36] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.
[37] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71–74, Feb. 2012.
[38] S. Gerbracht, C. Scheunert, and E. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 704–716, Apr. 2012.
[39] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.
[40] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.
[41] C. M. Angerer, R. Langwieser, and M. Rupp, "RFID reader receivers for physical layer collision recovery," *IEEE Trans. Commun.*, vol. 58, no. 12, pp. 3526–3537, Dec. 2010.
[42] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.
[43] W. Saad, Z. Han, and H. V. Poor, "On the physical layer security of backscatter RFID systems," in *Proc. 2012 Int. Symp. Wireless Commun. Syst.*

Walid Saad (S'08–M'10) received his B.E. degree in computer and communications engineering from Lebanese University in 2004, his M.E. in Computer and Communications Engineering from the American University of Beirut (AUB), Lebanon, in 2007, and his Ph.D. degree from the University of Oslo, Norway, in 2010. Currently, he is an Assistant Professor at the Electrical and Computer Engineering Department at the University of Miami, Coral Gables, FL. Prior to joining UM, he has held several research positions at institutions such as Princeton University and the University of Illinois at Urbana-Champaign. His research interests include wireless and small cell networks, game theory, network science, cognitive radio, wireless security, smart grids, and self-organizing networks. He has co-authored one book and over 85 international conference and journal publications in these areas.

In 2013, Dr. Saad received the NSF CAREER award for his research on self-organizing wireless systems. He is an Associate Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS and the IEEE COMMUNICATION SURVEYS & TUTORIALS. He was the author/co-author of the papers that received the Best Paper Award at the 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), in June 2009, at the 5th International Conference on InternetMonitoring and Protection (ICIMP) in May 2010, and at IEEE WCNC in 2012. Dr. Saad is a recipient of several awards from the University of Miami that include the Provost Research Award (2011 and 2013) and the Eliahu I. Jury Award for early career researcher in 2013.



Xiagyun Zhou (S-08–M'11) is a Lecturer at the Australian National University (ANU), Australia. He received the B.E. (hons.) degree in electronics and telecommunications engineering and the Ph.D. degree in telecommunications engineering from the ANU in 2007 and 2010, respectively. From June 2010 to June 2011, he worked as a postdoctoral fellow at UNIK - University Graduate Center, University of Oslo, Norway. His research interests are in the fields of communication theory and wireless networks.

Dr. Zhou serves on the editorial board of the following journals: IEEE COMMUNICATIONS LETTERS, *Security and Communication Networks (Wiley)*, and *Ad Hoc & Sensor Wireless Networks*. He has also served as a TPC member of major IEEE conferences. Currently, he is the Chair of the ACT Chapter of the IEEE Communications Society and Signal Processing Society. He is a recipient of the Best Paper Award at the 2011 IEEE International Conference on Communications.

Zhu Han (S'01–M'04–SM'09–F'14) received the B.S. degree in electronic engineering from Tsinghua University, in 1997, and the M.S. and Ph.D. degrees in electrical engineering from the University of Maryland, College Park, in 1999 and 2003, respectively. From 2000 to 2002, he was an R&D Engineer of JDSU, Germantown, Maryland. From 2003 to 2006, he was a Research Associate at the University of Maryland. From 2006 to 2008, he was an assistant professor in Boise State University, Idaho. Currently, he is an Associate Professor in Electrical and Computer Engineering Department at the University of Houston, Texas. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, wireless multimedia, security, and smart grid communication. Dr. Han is an Associate Editor of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS since 2010. Dr. Han is the winner of IEEE Fred W. Ellersick Prize 2011. Dr. Han is an NSF CAREER award recipient 2010.

H. Vincent Poor Poor (S'72–M'77–SM'82–F'87) received the Ph.D. degree in EECS from Princeton University in 1977. From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990 he has been on the faculty at Princeton, where he is the Michael Henry Strater University Professor of Electrical Engineering and Dean of the School of Engineering and Applied Science. Dr. Poor's research interests are in the areas of information theory, statistical signal processing and stochastic analysis, and their applications in wireless networks and related fields including social networks and smart grid. Among his publications in these areas are the recent books *Principles of Cognitive Radio* (Cambridge University Press, 2013) and *Mechanisms and Games for Dynamic Spectrum Allocation* (Cambridge University Press, 2014).

Dr. Poor is a member of the National Academy of Engineering, the National Academy of Sciences, and Academia Europaea, and is a fellow of the American Academy of Arts and Sciences, the Royal Academy of Engineering (U.K.), and the Royal Society of Edinburgh. He received the Marconi and Armstrong Awards of the IEEE Communications Society in 2007 and 2009, respectively. Recent recognition of his work includes the 2010 IET Ambrose Fleming Medal for Achievement in Communications, the 2011 IEEE Eric E. Sumner Award, and honorary doctorates from Aalborg University, the Hong Kong University of Science and Technology, and the University of Edinburgh.