Zero Reconciliation Secret Key Extraction in MIMO Backscatter Wireless Systems

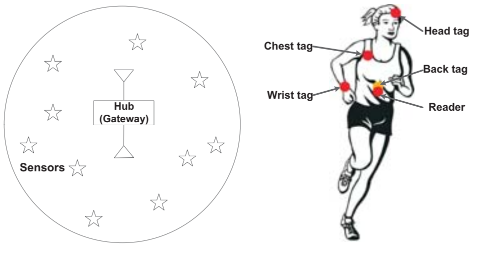
Shichao Lv*† Xiang Lu* Zhuo Lu‡ Xiaoshan Wang*† Ning Wang§ Limin Sun*
*Beijing Key Laboratory of IOT Information Security Technology, IIE CAS, Beijing 100093, China.
†University of Chinese Academy of Sciences, Beijing 100049, China.
‡Department of Computer Science, University of Memphis, TN 38152, USA.
§Beijing University of Posts and Telecommunications, Beijing 100876, China.
Emails: {lvshichao,luxiang,wangxiaoshan,sunlimin}@iie.ac.cn, wangning8566@bupt.edu.cn, zlu1@memphis.edu

***Abstract*—In this paper, we propose a new security design, called as Zero Reconciliation Secret Key Extraction, for backscatter wireless systems, in which a reader needs to establish secret keys for multiple tags. Our design is able to eliminate the reconciliation process in conventional physical layer based key establishment, therefore improving the efficiency while still maintaining security in such a process. The essence in our design is to use a channel state information (CSI) characteristic, named *CSI Ratio*, at the reader to differentiate multiple tags, then employ multiple-input multiple-output (MIMO) precoding for legitimate tags to effectively and securely establish secret keys, at the same time leveraging artificial jamming to forestall eavesdropping attacks in the network. We evaluate our design with real-world experimental data and show that the proposed approach can achieve relatively high secret key extraction rates and maintain low bit error rates.**

I. Introduction

Backscatter wireless communication is an emerging technology envisioned to power up, as well as connect, small computing devices through continuously ambient signals. With those ambient signals, the small devices are able to not only harvest energy for their own operations, but also transmit data by modulating reflections of ambient signals. Thus, the small devices become "fully-passive" sensors [1] breaking free from resource limits, and accommodate to be ubiquitously deployed for uninterrupted data sensing towards the vision of Internet of Things (IoT) [2]. In virtue of salient features such as energy harvesting, backscatter wireless systems are currently attracting more and more attentions in the research community [2–5], and also being adopted in a range of compelling applications, such as backscatter sensor networks [3] and radio frequency identification (RFID) systems [4], as illustrated in Fig. 1.

Within applications of backscatter wireless systems, RFID is the most prominent commercial one and widely used in article tracking, position location and other passive data sensing scenarios [6]. Generally, an RFID system is composed of a reader/interrogator and a small, simple and low-cost tag. The reader firstly transmits an incident signal to remotely power up the tag, while the tag reflects a portion of the incident signal with encoded digital symbols by varying the input impedance of its antenna. Finally, the reader recovers the original data by demodulating the backscattered signals. Despite outstanding performance on data sensing, RFID, like other backscatter wireless communication technologies, is also facing new challenges in terms of longer communication range and higher throughput, especially for the limited uplink from the RFID tag to the reader [7, 8]. To provide better uplink efficiency, researchers have proposed to add multiple antennas at both sides [6, 9], thereby forming a multiple-input multiple-output (MIMO) scenarios between a reader and multiple tags.



(a) Sensor application [3] (b) RFID application [4]

Fig. 1. Backscatter wireless communication applications.

However, the MIMO backscatter architecture brings not only a significant performance boost, but also more vulnerabilities that can be potentially used to compromise data communication. For example, in multi-antenna wireless energy harvesting [9], faked channel state information (CSI) [10] can easily fail the energy harvesting process thus "dumbing" tags. Moreover, the reader needs to combat powerful eavesdroppers that are equipped with multiple antennas and thus can break self-interference based security design for RFID [11]. In this regard, device authenticity and message confidentiality are paramount issues in MIMO backscatter wireless systems, which are, however, not well explored in the literature.

To address these problems, secret key establishment plays a critical role in initializing secure communications. Conventional cryptography-based key establishment methods and existing wireless channel randomness based key generation schemes [12] cannot be easily adopted in the context of MIMO backscatter communications because of two major issues. Firstly, the cost, size and computational resource-

*Shichao Lv, Xiang Lu, Xiaoshan Wang and Limin Sun were supported in part by the Strategic Priority Research Program of the Chinese Academy of Sciences (Grant No. XDA06040104). *(Corresponding author: Xiang Lu)*

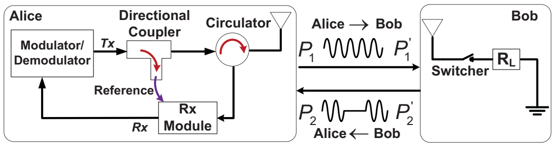


Fig. 2. Backscatter signaling at the physical layer.

constrained tags are not able to perform intensive computations that commonly exist in cryptography-based key establishment schemes, such as Diffie-Hellman. Secondly, channel randomness based key generation schemes require two communication parties measure the channel in rounds of probing and response. However, because of lack of transmission circuits, tags cannot initiate the probing process in such designs. As a result, in this paper, we offer a feasible, efficient, and secure solution, called Zero Reconciliation Secret Key Extraction, to achieve secure key establishment between MIMO backscatter communicators. Our contributions are three-fold.

- Using a CSI characteristic named *CSI Ratio* between different antennas at the reader to differentiate and authenticate multiple tags.
- Precoding for legitimate tags such that every tag can view his/her key in an orthogonal way and cannot see other's key due to inter-user signal cancelation. The precoding design can completely eliminate the reconciliation process in traditional physical layer based security design.
- Artificial jamming at the reader against eavesdropping attacks to securely provide secret key extraction from being overheard.

In addition, we evaluate our design with real-world experimental data to demonstrate the feasibility and effectiveness of our security design.

The remainder of this paper is organized as follows. Section II presents preliminaries and states the problem. Section III details our proposed schemes. In Section IV, we present experimental results. We discuss related work in Section V and conclude in Section VI.

II. Preliminaries and Problem Statement

In this section, we first introduce the basic backscatter communication scenario, then present the security threats faced by the MIMO backscatter wireless system, and lastly state the research problem and design goal.

A. Backscatter Communication Scenario

In a backscatter communication system as shown in Fig. 2, the reader (Alice) transmits a high power continuous waveform, whereas the tag (Bob) acts as a backscatter node to transmit signals by reflecting back the reader's continuous waveform, which drives a load resistor R_L to be the on/off state at the antenna, thereby encoding its messages. For example, Bob transmits a "1" bit when R_L is on, which results in the impedance increase and the power increase, including Bob's reflecting signal $P_2^{'}$ and Alice's received signal P_2. Conversely, when a "0" bit is transmitted, R_L is off, which leads to the decrease of the impedance, as well as $P_2^{'}$ and P_2. In this way, Bob is able to modulate Alice's signals to encode its own messages.

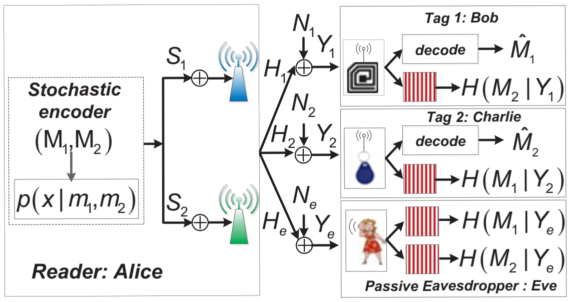


Fig. 3. The system and attack model in a MIMO backscatter system.

MIMO backscatter wireless systems feature multiple antennas on the reader side. Fig. 3 illustrates an example of secure backscatter communication scenarios. As shown in Fig. 3, there are four parties, one reader (Alice) and three tags (Bob, Charlie and Eve). Among these tags, Bob and Charlie are legitimate nodes, and Eve plays an eavesdropper role. Alice, as the reader, is equipped with two antennas, whereas each tag has only one antenna. For the sake of simplicity, we here only draw the downlink in Fig. 3.

In the MIMO backscatter communication process, Alice sends independent messages M_1 and M_2 to Bob and Charlie, separately, which are encoded as S_1 and S_2. Correspondingly, Bob, Charlie and Eve's channels are $H_1 = (h_{11}, h_{12})$, $H_2 = (h_{21}, h_{22})$ and $H_e = (h_{e1}, h_{e2})$. Thus, in the downlink, the received signals can be represented as follows.

$$\begin{pmatrix} Y_1 \\ Y_2 \\ Y_e \end{pmatrix} = \begin{pmatrix} H_1 \\ H_2 \\ H_e \end{pmatrix} \begin{pmatrix} S_1 \\ S_2 \end{pmatrix} + \begin{pmatrix} N_1 \\ N_2 \\ N_e \end{pmatrix}, \tag{1}$$

where N_1, N_2 and N_e are three independent additional white Gaussian noises (AWGNs), with zero-mean and variances as σ_1^2, σ_2^2 and σ_e^2, respectively. Alice's max power is P.

B. Security Threats in MIMO Backscatter Systems

Backscatter communication generally faces two kinds of threats. First, legitimate nodes may deliberately intercept other's messages. For example, Bob may attempt to decode Charlie's message M_2 in Fig. 3. We call such an attack, *inside attack*, because it is launched by legitimate nodes. Second, the eavesdropper Eve does not belong to the system, but may try to listen to communications between the reader and legitimate nodes. Such an attack is named as *outside attack*. It is worth mentioning that, in this paper, we focus on protecting authenticity and confidentiality, thus do not consider attacks targeting availability (e.g., jamming attacks) that may attempt to disrupt normal communication, which can be complementary to our work.

C. Problem Statement and Design Goal

Different from the conventional physical layer based key extraction methods, the design goal of our scheme is to ensure

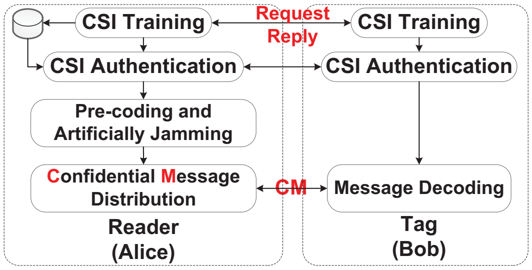


Fig. 4. A diagram of the secret key extraction scheme.

the reader sends only one signal, which can make all tags extract their own secrete keys from it. At the same time, neither the inside nor outside attackers can decode a key that does not belong to them. The design goal is formulated as follows.

$$\begin{pmatrix} Y_1 \\ Y_2 \\ Y_e \end{pmatrix} = \begin{pmatrix} H_1 \\ H_2 \\ H_e \end{pmatrix} S + \begin{pmatrix} N_1 \\ N_2 \\ N_e \end{pmatrix} \xrightarrow{Decoding} \begin{pmatrix} M_1 \\ M_2 \\ N_e^{'} \end{pmatrix}. \qquad (2)$$

where $N_e^{'}$ can be considered as an AWGN with variance $\sigma_{e^{'}}^2$. In the following, we present our design to achieve this goal.

III. Zero Reconciliation Secret Key Extraction

In this section, we present the details of Zero Reconciliation Secret Key Extraction for MIMO backscatter systems. We first give the design overview then describe the key components.

A. Scheme Overview

As shown in Fig. 4, our mechanism includes three major components: CSI training and authentication, precoding and artificial jamming, and confidential message distribution.

1) CSI training and authentication. This is necessary to authenticate a tag at the reader. We introduce a new tag authentication process for efficient CSI authentication. In the training phase, the reader profiles the CSI data of the tags via a request/reply process, then stores it in a database for the CSI authentication phase. Because of CSI changes (e.g., due to a tag's movement), the database needs to be updated in a timely manner. Once a tag backscatters a message to the reader, the tag's signal must go through the CSI authentication phase, during which the reader authenticates the signal by verifying its CSI in the database.
2) Precoding and artificial jamming. After collecting all the tags' CSI, the reader computes the precoding matrix for addressing the multi-user interference and confidential message leakage issue (therefore preventing inside attacks) and also designs artificial jamming based on CSI (therefore preventing outside attacks).
3) Confidential message distribution. After designing the precoding matrix and artificial jamming, the reader will broadcast all keys as confidential messages in a wireless signal transmitted to all tags that will securely receive their respective keys in the presence of both inside and outside attacks.

One advantage in our method is to leverage precoding and artificial jamming to securely deliver a group of keys from the reader to tags in the presence of both inside and outside attacks. Thus, compared with conventional physical layer based key generation, it not only avoids multiple one-to-one key deliveries, but also eliminates the reconciliation process that is used to solve the disagreement secret bits between two communicators during one delivery [12]. This substantially improves the efficiency during group secret key negotiation. In the following, we describe our technical details.

B. CSI Training and Authentication

Without loss of generality, we describe our system using the one-reader-and-three-tags scenario in Fig. 3. The design can be easily extended to scenarios with more users and more antennas.

The first step for secure key delivery is that the reader (Alice) must know some signals are indeed from her tags (Bob and Charlie) under potential mimicry or camouflage CSI attacks [13, 14]. To this end, we present a novel CSI training and authentication method, which uses a CSI property called *CSI Ratio*, to defend against CSI-based attacks and therefore identify a legitimate tag's time-varying CSI characteristics. We define the CSI ratio as follows.

Definition 1. *In the frequency domain, the CSI Ratio of a tag is defined as the ratio of CSI amplitude-frequency response of the tag's signal between antennas 1 and 2 at the reader. The CSI Ratio is written as* $CSIRatio = |H_1(f)|/|H_2(f)|$, *where* $H_1(f)$ *and* $H_2(f)$ *are CSI amplitude-frequency responses at frequency* f *at antennas 1 and 2, respectively.*

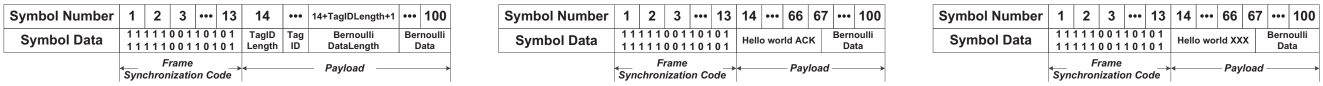
The CSI Ratio is not only time-varying, but also dependent on the tag's location and environment as well as the relative position between the tag and the reader.

In the backscatter communication scenario, the reader that works in a full duplex mode continuously transmits her continuous wave (e.g., a carrier wave) to power up the circuit of a tag, while receiving the reflected signal containing the tag's information. Using the discrete-time baseband signal model, the received signal y_R at the reader is given by [5],

$$y_R = h_{RT} * h_{TR} * sx + h_{RT} * n_T + n_R, \qquad (3)$$

where s is the signal transmitted by the reader, x is the tag's information signal, h_{TR} and h_{RT} are the reader-tag and tag-reader channel, respectively. n_T is AWGN at the tag which is backscattered to the reader with power σ_T^2, n_R is AWGN at the reader with power σ_R^2. For simplicity, we assume that $h_{RT} * n_T + n_R$ is a mixed signal equivalent to AWGN with variance σ_{TR}^2. The operator "$*$" means convolution in the time domain.

Given the basic signal reception model in (3), consider our scenario in Fig. 3: the uplink time-domain CSI from Bob (tag) to Alice (reader) are $h_{a_1,b}$, $h_{a_2,b}$, and the downlink one from Alice to Bob are h_{b,a_1}, h_{b,a_2}. During the CSI training phase, the following operations will be executed between Alice and Bob in every round.



(a) CSI training initialization packet

(b) CSI training ACK packet

(c) CSI training and authentication phase packet

Fig. 5. CSI training and authentication packet formats

1) Alice → Bob. In the first timeslot, Alice broadcasts a CSI training initialization packet whose content is illustrated in Fig. 5(a).
2) Alice ← Bob. During receiving the training initialization packet, Bob backscatters an ACK packet (whose content is depicted in Fig. 5(b)) to Alice.
3) Alice → Bob. Next, using only the first antenna, Alice transmits the packet s, which is the CSI training and authentication packet used in our protocol, including ten frames as specified in Fig. 5(c). Bob's receive signal can be written as $y_{b,a_1} = h_{b,a_1} * s$ without considering noise.
4) Alice ← Bob. During receiving the training y_{b,a_1}, Bob backscatters his data x by reflecting y_{b,a_1} to Alice who still uses her first antenna to receive. Because Alice's first antenna is transmitting s at the same time, this generates the self interference $i_{a_1} = h_{a_1,a_1} * s$. Thus, the received signal at Alice's antenna 1 becomes:

$$\begin{aligned} y_{a_1} &= i_{a_1} + h_{a_1,b} * (y_{b,a_1} x) + n_{a_1} \\ &= i_{a_1} + h_{a_1,b} * h_{b,a_1} * sx + n_{a_1}, \end{aligned} \tag{4}$$

where n_{a_1} is AWGN with power $\sigma_{a_1}^2$. After removing i_{a_1} using standard self-interference cancelation procedures in backscatter communications, Alice's received signal at antenna 1 in the frequency domain can be written as (without considering noise)

$$Y_{a_1}(f) = H_{a_1,b}(f) \cdot H_{b,a_1}(f) \cdot SX(f). \tag{5}$$

5) Alice → Bob. Using only antenna 2, Alice transmits the same packet s to Bob. Now Bob gets $y_{b,a_2} = h_{b,a_2} * s$.
6) Alice ← Bob. Similarly, Bob backscatters his data x by reflecting y_{b,a_2} to Alice. The received signal at Alice's antenna 2 in the frequency domain is (without considering noise)

$$Y_{a_2}(f) = H_{a_2,b}(f) \cdot H_{b,a_2}(f) \cdot SX(f). \tag{6}$$

7) Alice then computes Bob's *CSI Ratio* between antennas 1 and 2,

$$CSIRatio = \frac{|Y_{a_1}(f)|}{|Y_{a_2}(f)|} = \frac{|H_{a_1,b}(f) \cdot H_{b,a_1}(f)|}{|H_{a_2,b}(f) \cdot H_{b,a_2}(f)|}, \tag{7}$$

which can be used as a *wireless link signature*, which is unknown to others, to authenticate Bob.
8) Alice and Bob repeat the above operations several times until the fluctuation of measured *CSI Ratio* becomes stabilized (e.g., as long as the variance of measured results less than or equal to our experimental lower threshold $CSIRatio_{var}$, we can end the circulation). In addition, Alice calculates the mean value $CSIRatio_{avg}$ of all the received *CSI Ratios* for the later use in the CSI authentication phase.

Remark 1. *In order to avoid the interference between Bob and Charlie, Bob and Charlie's CSI training operations should comply with a Time Division Multiple Access (TDMA) scheme. For the sake of simple implementation, we assume that Bob and Charlie's training order is simply controlled by the "*Tag ID*" field in Alice's initialization packet as specified in Fig. 5(a).*

The CSI authentication phase is similar to the training one. The only difference is the last step, in which Alice calculates the Euclidean distance between $CSIRatio_{auth}$ with $CSIRatio_{avg}$ and compares it with a threshold $CSIRatio_{\eta}$ to verify Bob's $CSIRatio_{auth}$.

$$\|CSIRatio_{auth} - CSIRatio_{avg}\|^2 \overset{H_1}{\underset{H_0}{\gtrless}} CSIRatio_{\eta}. \tag{8}$$

Remark 2. *It is widely known that CSI (therefore CSI Ratio) fluctuates due to movement or environmental change. Therefore, the CSI authentication phase should shortly follow the training phase. In addition, upon receiving the new $CSIRatio_{auth}$, as long as it passes the authentication in* (8)*, Alice should update/refresh her database (e.g., using a first-in first-out (FIFO) queue storage structure).*

C. Precoding and Artificial Jamming

After all CSI data is authenticated, Alice should transmit k_1 and k_2 to Bob and Charlie, respectively. To ensure security, (i) Bob and Charlie should be able to only obtain their own keys, not the other's (i.e., no inside attacks); (ii) Eve cannot obtain any key from her received signals (i.e., no outside attacks). To this end, we need to precode the transmitted signal instead of directly sending k_1 and k_2. Denote by $W = (W_1 \ W_2)$ the precoding matrix, the receive signal vector in (2) can be re-written as

$$\begin{pmatrix} Y_1 \\ Y_2 \\ Y_e \end{pmatrix} = \begin{pmatrix} H_1 \\ H_2 \\ H_e \end{pmatrix} (W_1 \ W_2) \begin{pmatrix} k_1 \\ k_2 \end{pmatrix} + \begin{pmatrix} N_1 \\ N_2 \\ N_e \end{pmatrix}. \tag{9}$$

It is easy to verify in (9) that if the conditions $H_1 W_2 = H_2 W_1 = 0, H_1 W_1 \neq 0, H_2 W_2 \neq 0$ hold at the same time, we can meet the design goal to prevent both inside and outside attacks. The essential idea here is to create orthogonal signals arriving at Bob and Charlie, while the precoded signal arriving at Eve becomes artificial jamming. We adopt the block diagonalization (BD) algorithm [15] to precode the signal in an efficient way. Besides, although Alice does not known Eve's CSI, she has obtained both Bob and Charlie's CSI. Based on the above BD algorithm, Alice is able to generate some artificial AWGN noises and project noises into the orthogonal space of H_1 and H_2 along with the precoding. As a consequence, Eve's channel will be rapidly deteriorated, whereas Bob and Charlie's channels are not affected at all.

D. Confidential Message Distribution and Message Decoding

After Alice precodes the broadcast signal. Bob or Charlie can use the maximum likelihood (ML) algorithm to decode their keys k_1 and k_2. Specifically,

$$\hat{k}_j = \operatorname{argmin} \|Y_j - H_j W_j k_j\|^2 \quad \text{for } j = 1 \text{ or } 2. \qquad (10)$$

However, because of artificial jamming, Eve cannot decode anything using the ML algorithm.

IV. Evaluation with Realistic Experimental Data

In order to validate the feasibility of our proposed approach, we set up our evaluation scenario as that shown in Fig. 3, in which Alice wants to send keys to Bob and Charlie in the presence of an outside attacker, Eve. We use USRP2 devices to measure the realistic CSI data among them, working at 910MHz with 200KHz bandwidth.

In the CSI training phase, we average 10 CSI Ratios from Bob and Charlie, which are shown in Table I. The empirical $CSIRatio_{var}$ threshold is set to be 0.5. We consider the CSI results are stabilized as long as the variance of test values is less than the threshold 0.5. Using the CSI Ratios for Bob and Charlie, we validate their effectiveness against any mimicry or camouflage attacks. Fig. 6(a) depicts the relationship between Cumulative Distribution Function (CDF) of the CSI authentication success rate versus $CSIRatio_{\eta}$.

Then, we validate the feasibility and security of the proposed secret key extraction method. Fig. 6(b) illustrates the bit error rate (BER) for Bob, Charlie and Eve as a function of signal noise ratio (SNR). The BER for Bob to decode k_1 or Charlie to decode k_2 always gracefully decreases with SNR increasing. However, Eve's BER is always around 0.5 for decoding k_1 or k_2, which indicates her uncertainty about the messages is equivalent to make a wild guess thanks to precoding based artificial jamming.

We next measure the secret key rate in different modulation methods in Fig. 6(c). For BPSK and QPSK, the sum of Bob's and Charlie's secret key rates increases until it reaches twice of the modulation order. We can see that precoding the key via authenticated CSI is very efficient as it completely eliminates a reconciliation process in the existing physical-layer based key establishment. We can also see that in 16QAM and 64QAM, more decoding errors occur, leading to an unsatisfactory secret key rate. This indicates that higher-order modulation may not be good for efficient key generations because it is more susceptible to noise and interference. Overall, we conclude that our new method can achieve relatively fast secret key generation rates.

V. Related Work

1) Secret Key Extraction Exploiting MIMO Reciprocal CSI: In MIMO communication scenarios, [16] investigated the information theoretic limits and proposed three practical schemes for secret key generation. Exploiting the channel diversity also help improve key generation rates. [17] demonstrated that their CSI based secret key extraction scheme is much faster than received signal strength (RSS) based design via 802.11n measurements. However, most existing key generation designs requires a reconciliation process.

2) Authentication Based on Multiple Antennas Reciprocal CSI: Recently, a new virtual multi-path attack [13] has been proposed to inject fake aggregated signal to the realistic wireless channel for hiding impersonate movements or location changes. A defense strategy was also proposed to exploit an auxiliary receiver or antenna named helper to detect such an attack. The work in [18] proposed a novel signal processing technique, which extensively leverages the angle-of-arrival (AOA) information of multiple antennas at access point (AP), to obtain a signature for uniquely identifying the clients in a 802.11 network. Their experimental results showed that the AOA based signature is much more secure than those based on channel impulse response or RSS, relying on extra hardware.

3) Jamming Passive Attacker Using Artificial Noise: To defend against a passive attacker in MIMO multi-user communication scenarios, the sender can precode confidential messages into the null space of channels between the sender and eavesdropper (.e.g, [19]) if the sender knows the eavesdropper's CSI. However, in many communication scenarios, it is not practical to assume that the eavesdropper's CSI is known. Thus, it is very difficult to conceal the confidential messages without the eavesdropper's CSI. Although it is hard to directly block information leakage from the eavesdropper with its CSI, we do know the CSI information of legitimate receivers. If that is the case, we can degrade the eavesdropper's channel by sending carefully-designed artificial interference without affecting legitimate nodes too much (i.e., sender projects these artificial noise into the null space of the channel matrix between the sender and the desired receivers) [20].

VI. Conclusion

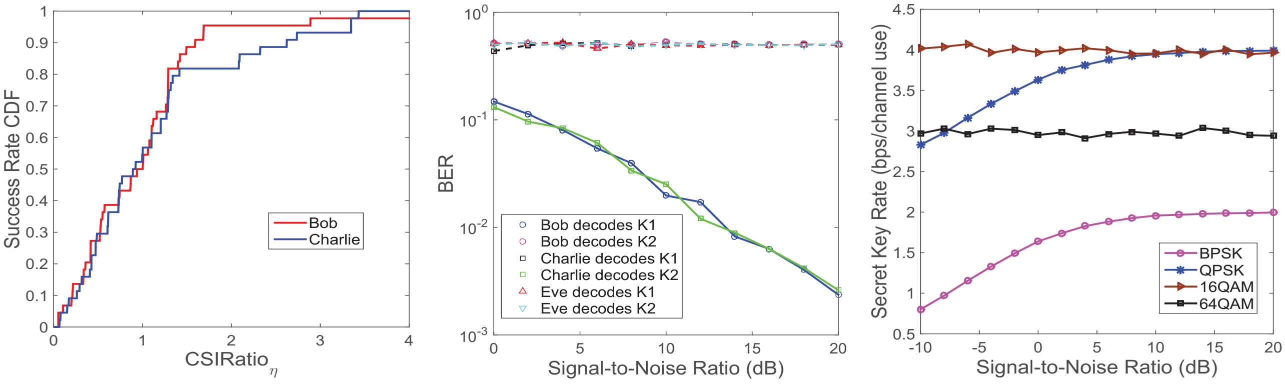
In this paper, we proposed a novel zero reconciliation secret key extraction scheme for backscatter wireless systems. The scheme uses a new CSI Ratio-based authentication method, precoding and artificial jamming to defense key generation and distribution against inside and outside threats. We demonstrated the efficiency and security of the proposed scheme via extensive analysis and real-world data evaluation.

References

[1] H. Schwerdt, S. S. W. Xu, A. Abbaspour-Tamijani, B. Towe, F. Miranda, and J. Chae, "A fully-passive wireless microsystem for recording of neuropotentials using rf backscattering methods," *Journal of Microelectromech System*, vol. 20, no. 5, pp. 1119–1130, 2011.

TABLE I
CSI RATIO TEST RESULTS.

TagID	Test 1	Test 2	Test 3	Test 4	Test 5	Test 6	Test 7	Test 8	Test 9	Test 10	Test 11	Average	Variance
Bob	2.5286	2.6266	2.6848	3.1888	2.4407	2.7638	3.7433	4.7876	2.9424	2.7644	3.6542	3.1022	0.4531
Charlie	2.9519	2.464	2.587	2.4766	0.9245	2.1465	1.1804	3.4527	1.9128	2.1457	2.0362	2.2071	0.4737



(a) CSI authentication success rate.

(b) Bit error rate.

(c) Secret key rate.

Fig. 6. Evaluation results.

[2] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetheral, and J. R. Smith, “Ambient backscatter: Wireless communication out of thin air,” in *ACM SIGCOMM’13*, 2013.

[3] G. Vannucci, A. Bletsas, and D. Leigh, “A software-defined radio system for backscatter sensor networks,” *IEEE Trans. Wireless Comm*, vol. 7, no. 6, pp. 2170–2179, 2008.

[4] J. Grosinger, “Feasibility of backscatter rfid systems on the human body,” *EURASIP Journal. Embedded Systems*, vol. 2013, no. 1, pp. 1–10, 2013.

[5] W. Saad, X. Zhou, Z. Han, and H. V. Poor, “On the physical layer security of backscatter wireless systems,” *IEEE Trans. Wireless Comm*, vol. 13, no. 6, pp. 3442–3451, 2014.

[6] J. D. Griffin, “High-frequency modulated-backscatter communication using multiple antennas,” Ph.D. dissertation, Geogia Institute of Technology, 2009.

[7] C. Boyer and S. Roy, “Backscatter communication and rfid: Coding, energy, and mimo analysis,” *IEEE Trans. on Communications*, vol. 62, no. 3, pp. 770–785, 2014.

[8] A. Parks, A. Liu, S. Gollakota, and J. R. Smith, “Turbocharging ambient backscatter communication,” in *ACM SIGCOMM’14*, 2014.

[9] G. Yang, C. H, and Y. Guan, “Multi-antenna wireless energy transfer for backscatter communication systems,” *arXiv:1503.04604*, 2015.

[10] Y. Tung, S. Han, D. Chen, and K. G. Shin, “Vulnerability and protection of channel state information in multiuser mimo networks,” in *ACM CCS’14*, 2014.

[11] H. Hassanieh, J. Wang, D. Katabi, and T. Kohno, “Securing rfids by randomizing the modulation and channel,” in *USENIX NSDI’15*, 2015.

[12] T. Wang, Y. Liu, and A. V. Vasilakos, “Survey on channel reciprocity based key establishment techniques for wireless systems,” *Wireless Networks*, vol. 21, no. 6, pp. 1835–1846, 2015.

[13] S. Fang, Y. Liu, W. Shen, and H. Zhu, “Where are you from?: confusing location distinction using virtual multipath camouflage,” in *ACM MobiCom’14*, 2014.

[14] Y.-C. Tung, S. Han, D. Chen, and K. G. Shin, “Vulnerability and protection of channel state information in multiuser mimo networks,” in *ACM CCS’14*, 2014.

[15] Q. H. Spencer, A. L. Swindlehurst, and M. Haardt, “Zero-forcing methods for downlink spatial multiplexing in multiuser mimo channels,” *IEEE Trans. Signal Processing*, vol. 52, no. 2, pp. 461–471, 2004.

[16] J. Wallace, “Secure physical layer key generation schemes: performance and information theoretic limits,” in *IEEE ICC’09*, 2009.

[17] H. Liu, Y. Wang, J. Yang, and Y. Chen, “Fast and practical secret key extraction by exploiting channel response,” in *IEEE INFOCOM13*, 2013.

[18] J. Xiong and K. Jamieson, “Securearray: Improving WiFi security with fine-grained physical-layer information,” in *ACM MobiCom’13*, 2013.

[19] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas I: The misome wiretap channel,” *IEEE Trans. Information Theory*, vol. 56, no. 7, pp. 3088–3104, 2010.

[20] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Trans. Wireless Comm*, vol. 7, no. 6, pp. 2180–2189, 2008.