Preventing Identity Attacks in RFID Backscatter Communication Systems: A Physical-layer Approach

Ahsan Mahmood*, Waqas Aman*†, M. Mahboob Ur Rahman*, M. A. Imran† and Qammer H. Abbasi†
*Electrical engineering department, Information Technology University, Lahore 54000, Pakistan
†Department of Electronics and Nano Engineering, University of Glasgow, Glasgow, G12 8QQ, UK
*{ahsan.mahmood,waqas.aman,mahboob.rahman}@itu.edu.pk,
†{muhammad.imran,qammer.abbasi}@glasgow.ac.uk

***Abstract*—This work considers identity attack on a radio-frequency identification (RFID)-based backscatter communication system. Specifically, we consider a single-reader, single-tag RFID system whereby the reader and the tag undergo two-way signaling which enables the reader to extract the tag ID in order to authenticate the legitimate tag (L-tag). We then consider a scenario whereby a malicious tag (M-tag)—having the same ID as the L-tag programmed in its memory by a wizard—attempts to deceive the reader by pretending to be the L-tag. To this end, we counter the identity attack by exploiting the non-reciprocity of the end-to-end channel (i.e., the residual channel) between the reader and the tag as the fingerprint of the tag. The passive nature of the tag(s) (and thus, lack of any computational platform at the tag) implies that the proposed light-weight physical-layer authentication method is implemented at the reader. To be concrete, in our proposed scheme, the reader acquires the raw data via two-way (challenge-response) message exchange mechanism, does least-squares estimation to extract the fingerprint, and does binary hypothesis testing to do authentication. We also provide closed-form expressions for the two error probabilities of interest (i.e., false alarm and missed detection). Simulation results attest to the efficacy of the proposed method.**

***Index Terms*—backscatter communication, authentication, identity attacks, hardware reciprocity, transmitter identification, intrusion detection**

I. Introduction

In Backscatter communication systems, the reader/interrogator sends out a continuous-wave signal, while the tag utilizes passive reflection and load modulation of incident radio frequency wave to respond back to the reader. This two-way (challenge-response) message exchange helps the reader extract useful information from the intended tag [1]. Backscatter communication systems are widely utilized in a number of application scenarios, e.g., transport and medical industries, access control, smart parking and smart grids, to name a few [2]. The increasing demand of high data rates in backscatter systems has prompted the researchers to build full-duplex backscatter communication systems. In a typical single-reader, single-tag, full-duplex backscatter system, the reader transmits and receives the radio signal simultaneously whereas the tag load modulates and backscatters the radio signal transmitted by the reader.

The broadcast nature of back-scatter communication makes it vulnerable to many attacks by adversaries. To counter such attacks in many wireless communication systems, crytpo based measures have been widely used. But, there are limitations of crypto based measures. One main draw back is the dependency on the share secret or secret key among legal nodes. Recently, authors in [3] reported that in today's word crpto based measures are at high risk to change of integrity due to advances in quantum computers, and thus, crpto based measures are quantum insecure. In this regards, physical layer security (PLS) which exploits the unique characteristics of the propagation medium [4], [5] is a promising approach to complement the crypto-based schemes at the higher layers of the protocol stack.

One essential ingredient of the PLS is Physical layer authentication (PLA)—basically a tool which a receiver could utilize to verify the identities of the transmit nodes. PLA has received considerable attention of the researchers due to its light-weight implementation and robust nature. PLA exploits the random features of the propagation medium which are nearly impossible to clone unless and until the malicious node is co-located with the legitimate node whose probability is almost

zero in practice. To date, there are various features reported for physical layer authentication, e.g., received signal strength [6], channel impulse response [7], [8] channel frequency response [9], carrier frequency offset [10], pathloss [11] and I/Q imbalance [12] etc. More recently, distance, angle and position of the transmit node were reported in [10] to thwart the impersonation attack in an underwater acoustic sensor network.

Though there are many works reported on the physical layer security in backscatter communication systems, most of them counter the eavesdropping attacks through resource allocation and artificial noise generation. Thus, there are only a handful of works which study physical layer authentication in half-duplex backscatter communication. Specifically, [13] exploited the propagation signatures of the tag, while [14] used analogue fingerprints of the tag. Finally, [15] reported difference of the radio signal as a fingerprint to authenticate the tag. *In contrast to previous works, this work thwarts identity attacks on RFID-based backscatter systems by exploiting residual channel as tag fingerprint in order to carry out physical layer authentication at the reader.*

Organization: The rest of the paper is organized as follows, Section II describes the system model of an RFID-based backscatter communication system that is under attack by a malicious tag. Section III presents the proposed physical layer authentication method. Section IV discusses simulation results. Finally, Section V concludes the work.

Notations: Unless otherwise specified, we use $(.)^H$ for hermitian, $(.)^T$ for transpose, $(.)^{-1}$ for inverse, uppercase bold face letters for matrix and lowercase bold face letters for vectors (e.g. $\mathbf{X}$ is for matrix $\mathbf{x}$ for vector). Finally, $\mathcal{CN}$ means complex normal.

II. System Model

We consider an RFID-based backscatter communication system that comprises a single reader and a single tag. We then consider the situation whereby a malicious tag (M-tag) launches identity attack on the reader by pretending to be the legitimate tag (L-tag), (see Fig. 1). We also learn from Fig. 1 that the traditional authentication mechanism at the reader fails as soon as the M-tag has the same tag ID as that of the L-tag. Therefore, this work proposes to carry out physical layer authentication at the reader whereby the reader measures the fingerprint (residual channel) and compares it against the pre-stored ground truth[1]

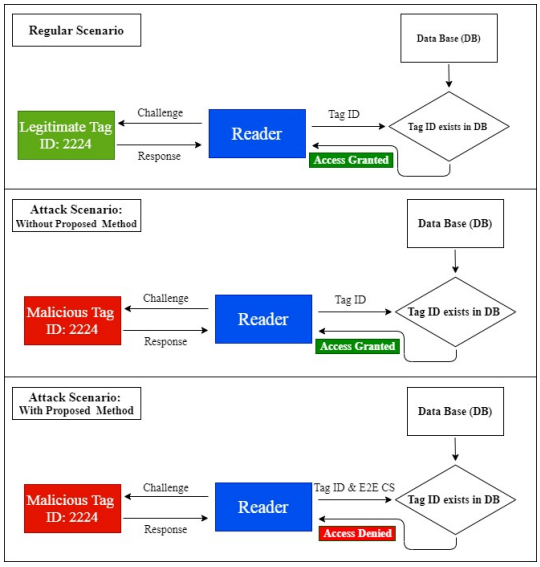

Fig. 1. The System Model: consider an RFID-based access control system which fails (i.e., it grants access to the M-tag) when the tag ID of the M-tag is the same as the tag ID of the L-tag. The proposed method counters such identity attacks by doing physical layer authentication at the reader.

III. Proposed Physical-Layer Authentication

The proposed physical layer authentication method consists of two steps: (i) feature/fingerprint acquisition using two-way message exchange followed by least-squares estimation of the fingerprint, (ii) binary hypothesis testing for tag identification.

A. Fingerprint Acquisition

1) Two-Way Challenge-Response Signaling: We consider "reader-talk-first" communication protocol [16]. For the the two-way (challenge-response) message exchange, tag follows amplify and forward (AF) relaying mechanism. The reader transmits the challenge message x_R with power P_R, and a while later, receives the backscattered response signal (see Fig. 2). The challenge message received at the tag at time n is:

$$y_T[n] = \sqrt{P_R}.x_R[n].h_{TR} + \sqrt{P_{SI,T}}z_T[n] \qquad (1)$$

where h_{TR} is the end-to-end directional channel from the reader to the tag; $z_T[n]$ is the self-interference signal seen by the tag, and $\sqrt{P_{SI,T}}$ is the power of self-interference signal at the tag. Inline with previous

[1]Note that the reader acquires the ground truth/fingerprint of the L-tag on a secure channel offline, and later, estimates the residual channel on the insecure/open channel online.

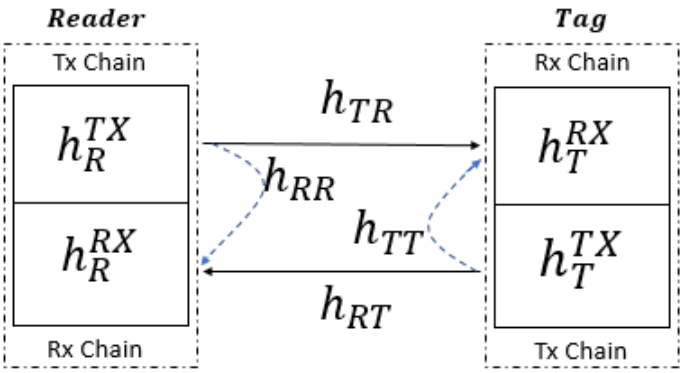

Fig. 2. Two-Way challenge-response signaling

literature [17], [18], we do not consider noise in Eq. (1). The response message received at the reader is:

$$y_R[n] = \eta h_{RT} y_T[n] + \sqrt{P_{SI,R}} z_R[n] \tag{2}$$

where h_{RT} is the end-to-end directional channel from the tag to the reader. Equivalently:

$$y_R[n] = \sqrt{P_R}\eta h_{RT} h_{TR} x[n] + \sqrt{P_{SI,T}}\eta h_{RT} z_T[n] + \sqrt{P_{SI,R}} z_R[n] + n_R \tag{3}$$

Where η, $z_R[n]$ and $\sqrt{P_{SI,R}}$ represent amplification factor, self-interference signal and power of interference signal at the reader, respectively. Inline with the previous literature [19], We assume that the self-interference signals $z_R[n] \sim \mathcal{CN}(0,1)$ and $z_T[n] \sim \mathcal{CN}(0,1)$.

Let $n_{RT} = \sqrt{P_{SI,T}}\eta h_{RT} z_T[n] + \sqrt{P_{SI,R}} z_R[n] + n_R$. Then, Eq. (3) can be written as:

$$y_R[n] = \sqrt{P_R}\eta \hat{h}_{RT} x[n] + n_{RT} \tag{4}$$

where $n_{RT} \sim \mathcal{CN}(0, \sigma_R^2 + P_{SI,R} + P_{SI,T}|\eta h_{RT}|^2)$, while $\hat{h}_{RT} = h_{TR} h_{RT}$ is the end-to-end residual channel between the reader and the tag.

2) Least-squares estimation of residual channel: To estimate the fingerprint $\hat{h}_{RT}$ of the tag, the reader sends N training symbols $\mathbf{x}_R = [x[1]\ x[2]\ ...\ x[N]]^T$ during the challenge phase. The tag acts as AF relay and backscatters the amplified signal. Thus, the reader receives $\mathbf{y}_R = [y[1]\ y[2]\ ...\ y[N]\ ]^T$ during response phase:

$$\mathbf{y}_R = \hat{\mathbf{x}}_R\ \hat{h}_{RT} + \mathbf{n}_{RT} \tag{5}$$

where $\hat{\mathbf{x}}_R = \eta\sqrt{P_R}.\mathbf{x}_R$, $\sigma_{RT}^2 = \sigma_R^2 + P_{SI,R} + P_{SI,T}|\eta h_{RT}|^2$. Then, the least-squares estimate is given as:

$$\hat{h} = (\hat{\mathbf{x}}_R^H.\hat{\mathbf{x}}_R)^{-1}.\hat{\mathbf{x}}_R^H.\mathbf{y}_R \tag{6}$$

which implies that $\hat{h} \sim \mathcal{CN}(\hat{h}_{RT}, \sigma_{\hat{h}}^2)$. Here, $\sigma_{\hat{h}}^2 = \frac{\sigma_{RT}^2}{\eta^2 P_R ||\mathbf{x}_R||^2}$, while $||\mathbf{x}||$ is l_2 norm of vector $\mathbf{x}_R$.

B. Binary Hypothesis Testing

With the estimate of the tag's fingerprint and perfect ground truth in hand, the reader performs binary hypothesis testing for tag identification. The binary hypothesis test is defined as:

$$\begin{cases} H_0(\text{L-tag is present}): & \upsilon = \hat{h}_{RT} + \epsilon \\ H_1(\text{M-tag is present}): & \upsilon = \hat{h}_{RE} + \epsilon \end{cases} \tag{7}$$

Here $\epsilon \sim \mathcal{CN}(0, \sigma_{\hat{h}}^2)$ is the estimation error. Then, $\upsilon|H0 \sim \mathcal{CN}(\hat{h}_{RT}^{(L)}, \sigma_{\hat{h}}^2)$ and $\upsilon|H1 \sim \mathcal{CN}(\hat{h}_{RT}^{(M)}, \sigma_{\hat{h}}^2)$. The test statistic T is given as:

$$T = |\upsilon - \hat{h}_{RT}| \underset{H_0}{\overset{H_1}{\gtrless}} \delta \tag{8}$$

where δ is a threshold, a design parameter. Let $t = \upsilon - \hat{h}_{RT}$, then $t|H_0 \sim \mathcal{CN}(0, \sigma_{\hat{h}}^2)$ and $t|H_1 \sim \mathcal{CN}(\hat{h}_M - \hat{h}_{RT}^{(L)}, \sigma_{\hat{h}}^2)$. Further, $T|H_0 \sim Rayleigh(\sqrt{(\sigma_{\hat{h}}^2/2)})$. Now, the probability of false alarm is:

$$P_{fa} = Pr(T > \delta|H_0) = exp(\frac{-\delta^2}{\sigma_{\hat{h}}^2}) \tag{9}$$

By setting P_{fa} to desired tolerance, δ is computed as:

$$\delta = \sqrt{-ln(P_{fa})\sigma_{\hat{h}}^2} \tag{10}$$

The performance of proposed method can be completely characterized by probability of false alarm and probability of missed detection. Since we are following Neyman-Pearson criterion, the performance of proposed method is solely dependent on success probability of M-tag or probability of missed detection. Then, $T|H_1 \sim Rice(\hat{h}_M - \hat{h}_{RT}^{(L)}, \sqrt{\sigma_{\hat{h}}^2/2})$. The success probability of M-tag can be expressed as:

$$P_{md} = Pr(T < \delta|H_1) \tag{11}$$

Let $\mu = \hat{h}_M - \hat{h}_{RT}^{(L)}$ and $\hat{\sigma} = \sigma_{\hat{h}}^2/2$. Then,

$$P_{md} = 1 - \mathcal{Q}_1(\frac{\mu}{\hat{\sigma}}, \frac{\delta}{\hat{\sigma}}) \tag{12}$$

where $Q_1(.,.)$ is the Marcum Q-function of order 1.

IV. Simulation Results

We define signal-to-interference-plus-noise ratio (SINR) at the reader as: $SINR = \frac{\eta^2 P_R}{\sigma^2_{RT}}$. We set $f = 20$ MHz, $\sigma^2 = \sigma^2_R = \sigma^2_T = 1$.

Fig. 3 shows the receiver operating characteristic (ROC) for various different values of SINR. Note that $P_d = 1 - P_{md}$ is the probability of detection. To obtain this plot, We sweep the P_{fa} from zero to one and then the threshold is calculated accordingly, then, for the given threshold we compute P_d. We observe that P_d increases with increase in the P_{fa} as well as with increase in SINR. Note also that we cannot simultaneously minimize both errors (i.e P_{md} and P_{fa}).

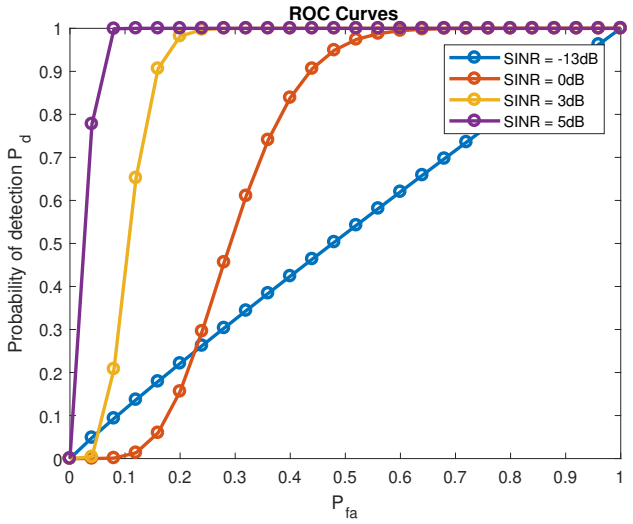

Fig. 3. ROC curves: for any pre-specified P_{fa}, probability of detection increases with increase in SINR

Fig. 4 shows the ROC curves for different values of Eve's fingerprint. We observe that for any pre-specified P_{fa}, probability of detection increases as the fingerprint of the M-tag becomes more dissimilar to the fingerprint of the L-tag. We fixed SNR to 5 dB to obtain this result.

V. Conclusion

This work studied identity attack on an RFID-based backscatter communication system and proposed to utilize the so-called residual channel as the fingerprint of the tag(s) in order to verify the identity of the tag(s) at the reader. In our proposed scheme, the reader acquired the raw data via two-way (challenge-response) message exchange mechanism, did least-squares estimation to extract the fingerprint, and did binary hypothesis testing to do the authentication. We also provided closed-form expressions for the two error probabilities of interest

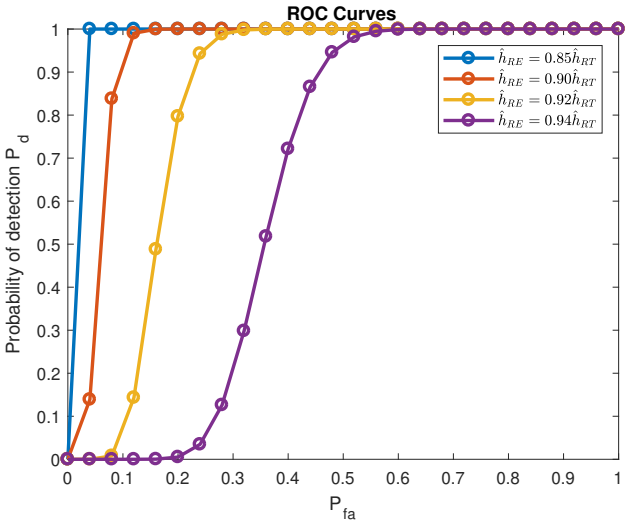

Fig. 4. ROC curves: for any pre-specified P_{fa}, probability of detection increases as the fingerprint of the M-tag becomes more dissimilar to the fingerprint of the L-tag

(i.e., false alarm and missed detection). Finally, simulation results attested to the efficacy of the proposed method.

Future work will look into other relevant features/fingerprints (e.g., tag antenna impedance, tag antenna gain etc.) which could further improve the accuracy of the proposed physical layer authentication scheme.

References

[1] J. Niu and G. Y. Li, "An overview on backscatter communications," *Journal of Communications and Information Networks*, vol. 4, no. 2, pp. 1–14, 2019.

[2] N. Van Huynh, D. T. Hoang, X. Lu, D. Niyato, P. Wang, and D. I. Kim, "Ambient backscatter communications: A contemporary survey," *IEEE Communications Surveys Tutorials*, vol. 20, no. 4, pp. 2889–2922, 2018.

[3] C. Gidney and M. EkerÃ¥, "How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits," 2019.

[4] W. Aman, G. A. S. Sidhu, T. Jabeen, F. Gao, and S. Jin, "Enhancing physical layer security in dual-hop multiuser transmission," in *2016 IEEE Wireless Communications and Networking Conference*, 2016, pp. 1–6.

[5] W. Aman, G. A. S. Sidhu, H. M. Furqan, and Z. Ali, "Enhancing physical layer security in af relayâassisted multicarrier wireless transmission," *Transactions on Emerging Telecommunications Technologies*, vol. 29, no. 6, p. e3289, 2018, e3289 ett.3289. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3289

[6] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 44–58, 2013.

[7] A. Mahmood, W. Aman, M. O. Iqbal, M. M. U. Rahman, and Q. H. Abbasi, "Channel impulse response-based distributed

physical layer authentication," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, 2017, pp. 1–5.

[8] S. Zafar, W. Aman, M. M. U. Rahman, A. Alomainy, and Q. H. Abbasi, "Channel impulse response-based physical layer authentication in a diffusion-based molecular communication system," in *2019 UK/ China Emerging Technologies (UCET)*, 2019, pp. 1–2.

[9] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2571–2579, 2008.

[10] W. Aman, M. M. U. Rahman, J. Qadir, H. Pervaiz, and Q. Ni, "Impersonation detection in line-of-sight underwater acoustic sensor networks," *IEEE Access*, vol. 6, pp. 44 459–44 472, 2018.

[11] M. M. U. Rahman, Q. H. Abbasi, N. Chopra, K. Qaraqe, and A. Alomainy, "Physical layer authentication in nano networks at terahertz frequencies for biomedical applications," *IEEE Access*, vol. 5, pp. 7808–7815, 2017.

[12] P. Hao, X. Wang, and A. Behnad, "Performance enhancement of i/q imbalance based wireless device authentication through collaboration of multiple receivers," in *2014 IEEE International Conference on Communications (ICC)*, 2014, pp. 939–944.

[13] Z. Luo, W. Wang, J. Xiao, Q. Huang, T. Jiang, and Q. Zhang, "Authenticating on-body backscatter by exploiting propagation signatures," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, 09 2018.

[14] G. S. Smith and M. Coetzee, "Afa-rfid: Physical layer authentication for passive rfid tags," in *2015 Information Security for South Africa (ISSA)*, 2015, pp. 1–8.

[15] J. Han, C. Qian, Y. Yang, G. Wang, H. Ding, X. Li, and K. Ren, "Butterfly: Environment-independent physical-layer authentication for passive rfid," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, pp. 1–21, 12 2018.

[16] F. Pebay-Peyroula and J. Reverdy, "A true full-duplex communication between hf contactless reader and card," in *2011 IEEE International Conference on RFID-Technologies and Applications*, 2011, pp. 473–478.

[17] S. Gong, X. Huang, J. Xu, W. Liu, P. Wang, and D. Niyato, "Backscatter relay communications powered by wireless energy beamforming," *IEEE Transactions on Communications*, vol. 66, no. 7, pp. 3187–3200, 2018.

[18] X. Jia and X. Zhou, "Performance characterization of relaying using backscatter devices," 2019.

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