BatAu: A Batch Authentication Scheme for Backscatter Devices in a Smart Home Network

1st Yishan Yang
School of Cyber Engineering
Xidian University
Xi'an, China
ysyangxd@stu.xidian.edu.cn

2nd Masoud Kaveh
School of Electrical Engineering
Aalto University
Espoo, Finland
masoud.kaveh@aalto.fi

3rd Jiajun Li
School of Cyber Engineering
Xidian Unversity
Xi'an, China
jiajunli1204@stu.xidian.edu.cn

4th Yifan Zhang
School of Electrical Engineering
Aalto University
Espoo, Finland
yifan.1.zhang@aalto.fi

5th Zheng Yan
School of Cyber Engineering
Xidian University
Xi'an, China
zyan@xidian.edu.cn

6th Kai Zeng
College of Engineering and Computing
George Mason University
Fairfax, VA, USA
kzeng2@gmu.edu

***Abstract*—With the maturity of the Internet of Things (IoT), many IoT applications have been popularized and promoted. As one of the IoT technology, backscatter communication (BC) has aroused research interest due to its low-cost and ultra-low power consumption characteristics. Due to their simple design and battery-less functionalities, backscatter devices (BDs) have been introduced as the main candidates for deploying in smart home networks (SHN). Although batch authentication in BC systems is crucial and efficient for SHN security, existing schemes have only focused on radio frequency identification (RFID) devices and no literature has given a general solution for BD batch authentication. In this paper, we propose a scheme named BatAu for authenticating batch BDs applied in SHN by extracting physical layer features in multiplexing signals. We conduct numerical simulations with various settings to show its desirable performance.**

***Index Terms*—backscatter communication, physical layer authentication, batch authentication**

I. Introduction

With the development of the Internet of Things (IoT) technology, IoT applications have increased with exponential growth in both size and number of devices. More energy is needed to be consumed to drive IoT devices for ensuring the normal operation of an entire network. However, battery-powered wireless devices need regular maintenance and replacement. This kind of expensive and inflexible power supplication has become the bottleneck of IoT applications. Backscatter communication (BC), a kind of low-cost and ultra-low power consumption technology, has received widespread attention due to its potential to alleviate the above challenges. By reflecting incident signals, backscatter devices (BD) can communicate with others without generating signals by themselves. This kind of simple and inexpensive device is very suitable to be deployed in IoT applications such as smart homes, smart cities, and the Internet of Vehicles.

A smart home network (SHN) can provide a comfortable residence environment by controlling in-house equipment such as lighting and air conditioning systems. As environmental-friendly and energy-saving devices, BDs can be deployed as an important part of SHN. Such an SHN system consists of two main types of devices: BDs and an access point (AP). BDs can be placed at different locations and have a wide range of functionalities, such as gas leak detection. AP is a controller which can communicate with multiple BDs to obtain the current state of the SHN and control a corresponding system to act. However, the open nature of wireless communication leads to security threats in SHN like impersonation, replay, and relay attacks. For example, once attackers get illegal access to the AP, sensitive information of the system could be stolen. To ensure information credibility from multiple BDs, it is crucial for AP to authenticate all involved BDs efficiently. Authenticating multiple BDs in a batch can effectively provide fundamental security for SHN with high efficiency to defend against such attacks.

As a supplement for upper layer protocol, physical layer authentication (PLA) establishes a secure channel for wireless communication systems [1]. PLA exploits inherent physical layer attributes, like channel statement information (CSI), received signal strength (RSS), and time of arrival/flight (ToA/ToF), as fingerprints for identifying or locating a device. For hard cloning and forging of fingerprints and not requiring additional computation, PLA is regarded as a promising security solution. However, the existing literature in PLA lacks a solution for batch authentication of BDs. Most of the existing physical layer authentication schemes are focused on how to identify a single BD in various applications, such as wearable BD [2], RFID [3], [4], robotic network [5] and general BC system [6]. A few works [7], [8] can authenticate two BDs simultaneously. But they cannot authenticate more than two tags in a batch.

A solution for multiple BDs authentication by utilizing physical layer fingerprints is still an opening question. Difficulties lie in the following two aspects when solving batch authentication by PLA. Firstly, signal collision happens when multiple BDs send signals together. Secondly, feature selection is not a trivial problem when deploying multiple BDs in a system.

In this paper, we explore the possibility of batch authentication by proposing an authentication scheme named BatAu to authenticate a group of BDs simultaneously and enhance the security of SHN with high efficiency. Power-domain non-orthogonal multiple access (PD-NOMA) has been shown as an attractive technology to allow multiple devices to be served by the same source [9], [10]. Mixed incident signals in an SHN enabled by BDs can be treated as a PD-NOMA-aided BC system. CSI describes the propagation process of the wireless signal between the transmitter and the receiver, which includes the effects of distance, scattering, and fading on the signals. By utilizing the mixed features CSI of group NOMA signals, a group of BDs can be authenticated by AP in a batch.

The main contributions of this paper are as follows:

1) We propose BatAu to support batch BDs authentication in SHN. With the aid of PD-NOMA, AP can authenticate multiple BDs in a batch without the problem of signal collision. The scheme has the ability to resist identity impersonation, replay, and relay attacks.
2) By extracting physical layer characteristics, BatAu imposes low computation and power consumption overheads to BDs applied in SHN. To the best of our knowledge, BatAu is the first batch authentication scheme by utilizing inherent physical layer attributes.
3) We show the usability of BatAu through numerical simulations. We adopt different parameters in extensive numerical simulations to evaluate the performance of BatAu regarding accuracy, latency, and availability.

The rest of the paper is organized as follows. We review a number of existing schemes related to batch authentication and PLA in Section II. Then, we elaborate the system/security model of BatAu, its design and its security against different attacks in Section III. In section IV, we present our evaluation results by conducting numerical simulations. Finally, we draw a conclusion in the last section.

II. Related Work

This section reviews existing batch authentication and PLA schemes.

A. Batch Authentication Schemes

Existing batch authentication schemes applied in BC systems have mainly focused on distinguishing RFID tags. Weis et al. [11] proposed a hash function-based scheme named HashLock, which can support multiple RFID tags authenticated in a batch. In HashLock, the reader sent a random number r as an authentication request. After receiving the request, the tag calculates a hash value by inputting its secret key and r as a response. The authentication server then searches for whether there exists a key to satisfy the hash value to make an authentication decision. The complexity of the key search is linear to the number of tags in the system, which leads to low authentication efficiency and inapplicability in a large-scale system. Tree-based approaches are proposed to improve authentication efficiency. For example, in [12], the keys of all tags are organized with a balanced tree. Each node of the tree stores a key and the keys in the path from the root to a leaf node are assigned to the tag related to the leaf node. However, each tag needs to store all keys from the root to leaf nodes. ACTION [13] employs a novel sparse tree architecture, such that the key of every tag is independent of one another. The common disadvantage of the above schemes lies in the high cost of authentication. They [11]–[13] need a large search time and employ an anti-collision algorithm to identify them before obtaining their hash values. Besides, the volume of authentication data is high due to the use of hash functions, leading to huge communication costs.

TABLE I
Comparison between related works and BatAu

Reference	[16]	[3]	[4]	[7]	[8]	[6]	BatAu
MLA	√	×	×	√	√	√	√
SAI	√	×	×	×	×	√	√
BA	×	×	×	×	×	×	√

MLA: machine learning avoidance; SAI: signal analyzer independence; BA: batch authentication supporting;
√:supported; ×:not supported;

To address the high cost of the hash function-based method, some probabilistic approaches aimed to authenticate the validity of a batch of tags. Different from the hash function-based approaches, a single echo-based batch authentication (SEBA) scheme [14] considers a batch of tags as a whole and authenticates the distribution of their replies. To overcome the scalability problem, Lin et al. [15] proposed a scheme called FISH to meet the requirement of prompting reliable batch authentications in large-scale RFID applications. However, these kinds of methods authenticate the validity of RFID tags with a probability of $1 - \delta$ if the number of fake tags is less than $n * \epsilon$ in a n tags system, where δ and ϵ are two security parameters. Meanwhile, the schemes proposed in [14] and [15] only focus on RFID systems and authenticate the group of tags sequentially within a specified time.

B. PLA Schemes

By extracting the physical layer features as fingerprints, a number of schemes have been proposed to identify or locate a BD. Founding the propagation difference regarding RSS between on-body and off-body BDs, Luo et al. [16] proposed a low-power authentication scheme for authenticating wearable BD. Zhao et al. [3] utilized unique phase features generated when a user touches the BD as a fingerprint. This kind of fingerprint can be extracted by a signal analyzer. With this approach, the device and its holder can be authenticated simultaneously with a machine learning (ML) based classifier. Li et al. proposed an RFID authentication scheme [4] by building a fully connected multi-class neural network for fingerprint classification. The reflection coefficient of each tag circuit is defined as the unique fingerprint for authentication. If two tags are placed in a close position, the backscattered

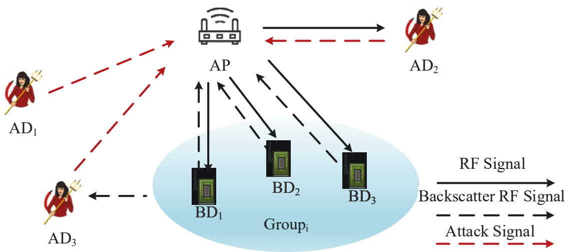

Fig. 1. System model and security model

signals of the pair of tags are much different from a single BD. The difference can be analyzed by deploying a professional signal analyzer. Butterfly [7] and Hu-Fu [8] utilize this kind of difference to authenticate a pair of tags. Wang et al. proposed a multi-stage authentication scheme named BCAuth [6] to authenticate a BD in both static and dynamic scenarios. By exploiting clustering-based analysis on RSS and ToA, BCAuth can detect the number of attackers and localize their positions. BCAuth also offers mutual authentication for capable BDs.

ML-based methods need adequate labeled data sets to train a classifier. In addition, deploying a sophisticated signal analyzer increases hardware costs, which causes limitations in the scenario of the schemes. Table I compares the above-related PLA works with BatAu in terms of ML avoidance (MLA), signal analyzer independence (SAI), and batch authentication (BA). We can see that although the existing PLA schemes have the potential for practical applications, there still lacks a general method for efficiently authenticating multiple BDs in a batch. BatAu shows a great advance in supporting batch device authentication. Besides, BatAu does not depend on an ML model and a signal analyzer.

III. BatAu Overview

In this section, we first introduce the system and security models of BatAu and then give a detailed description of its design. Furthermore, we theoretically analyze the security of BatAu.

A. System Model

Fig. 1 illustrates the system model of the proposed scheme. Equipped with omnidirectional antennas, AP can send RF signals to all BDs in order to authenticate them. The RF signals can carry information and energy simultaneously. Each BD contains a backscatter modulator, an information receiver, an RF energy harvester, and other modules (i.e., sensors) that can operate in two modes, backscattering mode and listening mode, respectively. In the backscattering mode, BDs transmit signals by reflecting incident signals and intentionally altering their information. In the listening mode, BDs decode information from a part of received signals while the remaining signals are used for energy harvesting. The harvested energy is used to power up the circuit and sensing elements. In SHN, BDs can be placed at different locations as sensors and can be grouped based on diverse functions. As a controller, AP can obtain the present condition of SHN by getting responses from BDs.

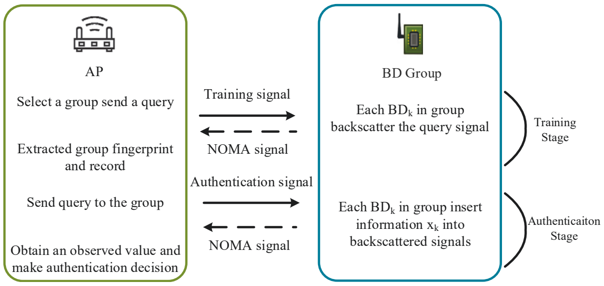
AP
Select a group send a query
Extracted group fingerprint and record
Send query to the group
Obtain an observed value and make authentication decision
Training signal
NOMA signal
Authentication signal
NOMA signal
BD Group
Each BD$_k$ in group backscatter the query signal
Each BD$_k$ in group insert information x$_k$ into backscattered signals
Training Stage
Authenticaiton Stage

Fig. 2. The procedure of BatAu

B. Security Model

In this paper, we consider AP as an honest and trusted party for all BDs in the system. BDs honestly transmit data only when inquired by the AP.

The attacker has two actions: eavesdropping and attacking. By eavesdropping, the attacker eavesdrops on the channel between the AP and a legal BD to acquire sensitive information. By attacking, the attackers intend to pass the authentication and transmit fake messages to AP to intrude on the SHN system. We define three kinds of attackers as follows:

An impersonate attacker, i.e. AD_1 in Fig. 1, has the ability to eavesdrop on the backscatter signals from a genuine BD or a group to obtain its or their identity information. Then the attacker impersonates the legal BD or the group with the identity to pass the authentication.

A replay attacker, AD_2 as shown in Fig. 1, records the backscatter signals from a legal group and replays identical signals of prior communication to the AP when the group is required by AP.

A relay attacker, namely AD_3 in Fig. 1, relays the signal of a legitimate group to the AP when the group is required for authentication.

We assume that the adversary cannot be very close to a legal BD and outside of the scope of a BD group. The correlation of fingerprints between two transmitters significantly reduces as the distance between the two transmitters increases. For example, in a wireless communication system with large multi-paths and rich scatters, the features of two transmitters with half wavelength distance can be treated as completely independent [17]. Thus, this assumption avoids attackers from getting highly correlated fingerprints and ensures they measure different channels with the legal BDs.

C. The Proposed Scheme

Herein, we describe the design of BatAu by utilizing mixed CSI from NOMA signals as the fingerprint of group BDs for authentication. As shown in Fig. 2, the scheme contains two stages: a training stage and an authentication stage.

Training stage. AP sends a training signal s_T with total power P to a certain group which contains n BDs, for example, $Group_i$, as shown in Fig.1. The received signal at BD_k, denoted as y_{k_T} can be expressed as

$$y_{k_T} = \sqrt{P} h_k s_T + N_k, \tag{1}$$

where h_k denotes the CSI between BD_k and AP, and N_k denotes additive white Gaussian noise (AWGN) at BD_k.

After receiving the signal, BD_k reflects the signal y_{k_T} with a power reflection coefficient (PRC) α_{ik}, but does not alter any information in the training stage. α_{ik} is preassigned by AP to the group member and satisfies $\sum\limits_{k=1}^{n} \alpha_{ik} = 1$. In order to decode information of each BD from mixed-signals by successive interference cancellation (SIC) strategy, the PRC of different BDs varies [18]. Then, the reflected signal y_k^T by BD_k is

$$y_k^T = \sqrt{\alpha_{ik}} y_{k_T}, \tag{2}$$

So the received superposition NOMA signal y^R at AP from the group $Group^*$ is

$$y^{R_T} = \sum_{k=1}^{n} h_k y_k^T + N_A = \sum_{k=1}^{n} (\sqrt{\alpha_{ik} P} {h_k}^2 s_T + I_k) + N_A, \tag{3}$$

where N_A denotes AWGN at AP and $I_k = \sqrt{\alpha_{ik}} h_k N_k$ denotes internal interference. AP extracts CSI in y^R as a group fingerprint e to form a white list for authentication, denote as

$$e = \sum_{k=1}^{n} \sqrt{\alpha_{ik}} {h_k}^2, \tag{4}$$

which is steady in a static situation.

Authentication stage. At the beginning of the authentication stage, the AP sends an authentication signal s with transmission power P to select a certain group of BDs to get responses, e.g., $Group_i$ in Fig. 1. The received signal at BD_k is similar to (1) and can be denoted as

$$y_{k_A} = \sqrt{P} h_k s + N_k. \tag{5}$$

Different from the training stage, the selected BD_k reflects the received signal by intentionally altering its information x_k with PRC. The reflected signal by BD_k in this stage is:

$$y_k^A = \sqrt{\alpha_{ik}} y_{k_A} x_k. \tag{6}$$

The mixed signals received at AP are also similar to 3, which is denoted as

$$y^{R_A} = \sum_{k=1}^{n} h_k y_k^A + N_A = \sum_{k=1}^{n} \sqrt{\alpha_{ik} P} {h_k}^2 s x_k + I_k + N_A. \tag{7}$$

Assuming all preamble in the authentication stage of the signals from different BDs are the same. Then, AP can obtain an observed value of the group fingerprint as

$$\hat{e} = \sum_{k=1}^{n} \sqrt{\alpha_{ik}} \hat{h_k}^2 \tag{8}$$

from the preamble of the mixed signals.

AP can make an authentication decision by measuring the difference between fingerprint e and the observed value $\hat{e}$ as

$$E = \left| e - \hat{e} \right|. \tag{9}$$

If the observed $\hat{e}$ is from a legal group, the results of $|e - \hat{e}|$ can be negligible. According to the security assumption, the attacker cannot get highly correlated fingerprints with any legal BDs, which leads to a substantial difference of E when the signals are not from a legal group. By formulating a hypothesis text with a threshold θ as

$$\mathcal{H}_0 : E \leq \theta, \tag{10}$$

AP can make an authentication decision. Selecting an appropriate value of the threshold is essential for the performance of the scheme. We can adjust the threshold by evaluating the detection error.

If this authentication is accepted, AP decodes this mixed signal with the SIC strategy. Since every BD_k in the group reflects the signal by altering its information x_k, AP can decode x_k in the mixed signals.

D. Security Analysis

1) Identity impersonation attacks: Assuming an identity impersonation attacker knows the authentication scheme. The attacker can obtain the identity of one legal BD and know which group it belongs to. The attacker muddles through by counterfeiting the legal BD in the group. Since the attacker cannot be very close to the legal BD, the independence of the Rayleigh fading channel causes the sent signals from the attacker to have uncorrelated CSI with the legal one. This leads to a remarkable difference for AP to reject the authentication. The situation is similar if a strong attacker can launch a group identity impersonation attack by owning multiple counterfeit BDs. It can also be detected by AP due to the difference of mixed CSI. Thus, identity impersonation attackers only with legal identities cannot succeed at AP.

2) Replay attacks: Assuming a replay attacker can intercept the authentication signals from a legal group of BDs, the attacker only replays the captured signal without any modification to raise a replay attack. The received signals at AP consist of the group signals with the CSI of the attacker mixed in it, which leads to an error value and causes an authentication failure. Therefore, BatAu is capable of defending against replay attacks.

3) Relay attacks: Assuming a relay attacker relays the authentication signal of a legal group to the AP. In this situation, AP receives both signals from the legal group and the attacker. The received signals at AP from the attacker have a significantly different fingerprint from the legal one. Hence, AP can directly detect relay attacks.

IV. Evaluation

In this section, we analyze and discuss the performance of BatAu with extensive simulations.

A. Simulation Setting

In our simulations, we consider a batch authentication system as illustrated in Fig.3 with two kinds of entities: an AP and six BDs. Six BDs with the same function are enough for deploying in an SHN. The distance from BD to the AP varies from BD to BD. These six BDs are grouped into five groups, and each group includes two to six BDs. Regarding the surroundings of SHN, it is unavoidable that obstacles may block the main channel between the AP and BDs. So we model the channel between AP and BDs with the Rayleigh channel model [19]. The channel gains are set as $10^{-2} d_k^{-2}$ according to [6], [20], where d_k denotes the distance between the BD_k and the AP. The uplink of the system is modeled as NOMA [18], where PRC for each BD_k in the group is set to different values. All PRC of the grouped BDs is preassigned

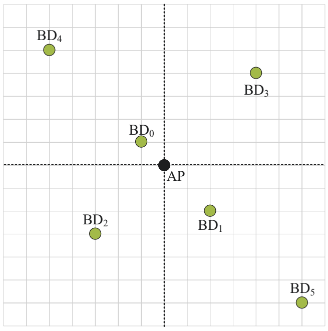

Fig. 3. Simulation setting

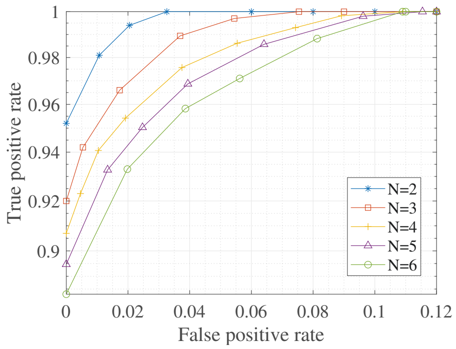

Fig. 4. ROC of authentication different groups

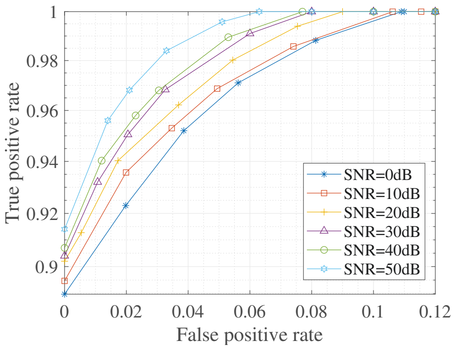

Fig. 5. ROC under different SNR

and satisfies α_{ik_n} larger than α_{ik_m} if n is smaller than m, which indicates that BD_n always holds a stronger PRC than BD_m in one group. The PRC of the attacker is selected by itself. We found that the smaller the PRC, the easier to perform an impersonation. But the imposter should at least hold the second smallest PRC in the selected group to keep its signal decoded by the SIC strategy of AP since the SIC strategy successively decodes the signals according to their powers from high to low.

B. Metrics

We use accuracy, latency, and availability to evaluate our proposed scheme.

Accuracy. Accuracy indicates the probability of correctly identifying a group, including accepting a legitimate group and rejecting an illegal group. We define the true positive rate (TPR) as the rate of a legal group accepted by BatAu, and the false positive rate (FPR) as the rate of an illegal group accepted by BatAu. A receiver operating characteristic (ROC) curve, a classical measure for describing the relationship between FPR and TPR, can show the resolving ability under varying thresholds.

Latency. Latency refers to the time spent in processing authentication. The main purpose of batch authentication is to improve the efficiency of BD authentication. The latency refers to the time spent from sending an authentication request to making an authentication decision.

Availability. Availability shows the performance of the proposed scheme under attacks. It indicates the accuracy of authentication when attackers launch different kinds of attacks.

C. Simulation Results

In this part, we show the performance of BatAu regarding the metrics above. Due to none of the work providing a solution for batch authentication in BC based on physical layer characteristics, we cannot set a comparison simulation with the existing work.

Fig. 4 shows the ROC curve of our proposed scheme when the signal-to-noise ratio (SNR) is 30dB regarding different numbers N of BDs in one group. When TPR grows, FPR also grows, as illustrated in Fig. 4, which indicates that by setting an appropriate hypothesis test threshold, the scheme can authenticate the legal group of BDs. Fig. 5 shows the ROC curve of the group consisting of four BDs under different SNR conditions. From Fig. 5, we observe that the higher the SNR, the better the authentication performance. Even though the noise could affect the authentication accuracy, BatAu has the capability to make a correct authentication decision by setting a proper threshold under poor communication conditions.

Fig. 6 shows the latency of the scheme with regard to different numbers N of BDs in the group and different SNR conditions. To avoid an experimental error, we measure the latency five times and take the average as the result. The latency of the scheme is highly related to the number N of BDs in the group. SNR conditions have little effect on latency.

Fig. 7 shows the ROC curve of the group consisting of four BDs under different numbers N' of identity impersonation attackers. As illustrated in Fig. 7, the bigger the number of imposters who launch attacks simultaneously, the better the performance of BatAu. Because a large number of attackers sneaking into a legal group leads to extracted observation fingerprints deviating from the original value recorded in a white list. It is indicated that it is easier for BatAu to detect attacks when more attackers exist.

Fig. 8 shows the bit error rates (BER) of the decoding signal from the BD that has the biggest PRC in the group containing N members. BatAu can obtain a more satisfactory BER under a higher SNR. However, when there are more than six BDs in the group, due to internal interference caused by NOMA, some received signals from BDs suffer from undesired BER, which causes meaningless communications. How to enhance the scalability of BatAu to support batch authentication in large-scale BD deployment scenarios is an interesting research topic worth further investigation.

V. Conclusion

In this paper, we proposed BatAu, a scheme for simultaneously authenticating multiple BDs deployed in an SHN. By exploiting physical layer features CSI from multiplexing NOMA signals, BatAu is capable of authenticating the eligibility of a group of BDs and defending against identity impersonation, replay, and relay attacks. We evaluate the performance of BatAu through extensive simulations with regard to accuracy, latency, and availability. The results showed that BatAu has a desirable performance and efficiency. However, BatAu only considers a static scenario and has an undesirable performance

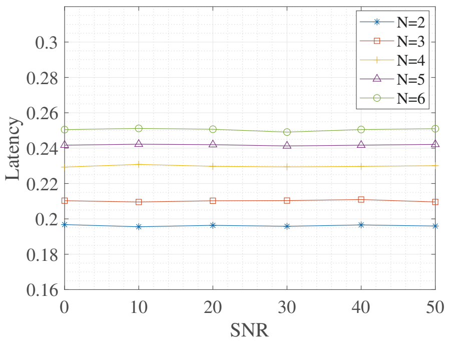

Fig. 6. Latency

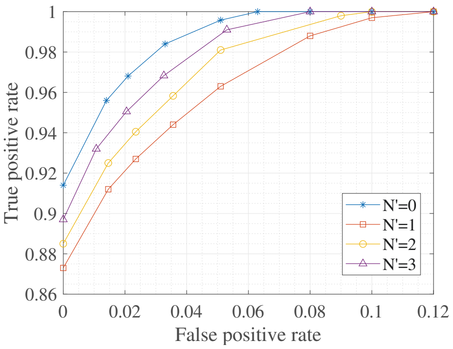

Fig. 7. ROC with different numbers of attackers

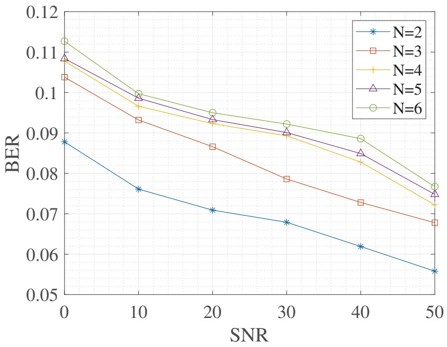

Fig. 8. BER under different SNR

facing a large-scale BD group. As our next work, we intend to investigate how to support mobility and achieve scalability in BatAu.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under Grant 62072351; in part by the Key Research Project of Shaanxi Natural Science Foundation under Grant 2023-JC-ZD-35; in part by the open research project of ZheJiang Lab under grant 2021PD0AB01; in part by the Academy of Finland under Grant 345072 and Grant 350464. (Corresponding author: Zheng Yan.)

References

[1] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," *IEEE Wireless Communications*, vol. 17, no. 5, pp. 56–62, 2010.

[2] Z. Luo, W. Wang, J. Xiao, Q. Huang, T. jiang, and Q. Zhang, "Authenticating on-body backscatter by exploiting propagation signatures," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 2, no. 3, sep 2018. [Online]. Available: https://doi.org/10.1145/3266002

[3] C. Zhao, Z. Li, T. Liu, H. Ding, J. Han, W. Xi, and R. Gui, "Rf-mehndi: A fingertip profiled rf identifier," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, 2019, Conference Proceedings, pp. 1513–1521.

[4] J. Li, A. Li, D. Han, Y. Zhang, T. Li, and Y. Zhang, "Rcid: Fingerprinting passive rfid tags via wideband backscatter," in *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*, 2022, pp. 700–709.

[5] Y. Huang, W. Wang, T. Jiang, and Q. Zhang, "Detecting colluding sybil attackers in robotic networks using backscatters," *IEEE/ACM Transactions on Networking*, vol. 29, no. 2, pp. 793–804, 2021.

[6] P. Wang, Z. Yan, and K. Zeng, "Bcauth: Physical layer enhanced authentication and attack tracing for backscatter communications," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2818–2834, 2022.

[7] 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, no. 4, pp. 1–21, 2018.

[8] G. Wang, H. Cai, C. Qian, J. Han, S. Shi, X. Li, H. Ding, W. Xi, and J. Zhao, "Hu-fu: Replay-resilient rfid authentication," *IEEE/ACM Transactions on Networking*, vol. 28, no. 2, pp. 547–560, 2020.

[9] S. Islam, N. Avazov, O. A. Dobre, and K. S. Kwak, "Power-domain non-orthogonal multiple access (noma) in 5g systems: Potentials and challenges," *IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 721–742, 2016.

[10] O. Maraqa, A. S. Rajasekaran, S. Al-Ahmadi, H. Yanikomeroglu, and S. M. Sait, "A survey of rate-optimal power domain noma with enabling technologies of future wireless networks," *IEEE Communications Surveys Tutorials*, vol. PP, no. 99, pp. 1–1, 2020.

[11] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in *1st International Conference on Security in Pervasive Computing*, 2004.

[12] T. Dimitriou, "A secure and efficient rfid protocol that could make big brother (partially) obsolete," in *Fourth Annual IEEE International Conference on Pervasive Computing and Communications (PERCOM'06)*, 2006, pp. 6 pp.–275.

[13] L. Lu, J. Han, R. Xiao, and Y. Liu, "Action: Breaking the privacy barrier for rfid systems," in *IEEE INFOCOM 2009*, 2009, pp. 1953–1961.

[14] L. Yang, J. Han, Y. Qi, and Y. Liu, "Identification-free batch authentication for rfid tags," in *The 18th IEEE International Conference on Network Protocols*, 2010, pp. 154–163.

[15] Q. Lin, L. Yang, and Y. Guo, "Proactive batch authentication: Fishing counterfeit rfid tags in muddy waters," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 568–579, 2019.

[16] 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, no. 3, pp. 1–22, 2018.

[17] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Communications Surveys Tutorials*, vol. 23, no. 1, pp. 282–310, 2021.

[18] J. Guo, X. Zhou, S. Durrani, and H. Yanikomeroglu, "Design of non-orthogonal multiple access enhanced backscatter communication," *IEEE Transactions on Wireless Communications*, vol. 17, no. 10, pp. 6837–6852, 2018.

[19] X. Li, M. Zhao, M. Zeng, S. Mumtaz, V. G. Menon, Z. Ding, and O. A. Dobre, "Hardware impaired ambient backscatter noma systems: Reliability and security," *IEEE Transactions on Communications*, vol. 69, no. 4, pp. 2723–2736, 2021.

[20] Y. S. Cho, J. Kim, W. Y. Yang, and C. G. Kang, *MIMO-OFDM wireless communications with MATLAB*. John Wiley & Sons, 2010.