Chang, Jingdong; Li, Jiajun; Yang, Yishan; Zhang, Yifan; Kaveh, Masoud; Yan, Zheng

APAuth: Authenticate an Access Point by Backscatter Devices

Published in:
ICC 2024 - IEEE International Conference on Communications

DOI:
10.1109/ICC51166.2024.10623058

Published: 13/06/2024

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

APAuth: Authenticate an Access Point by Backscatter Devices

Jingdong Chang, Jiajun Li, *Student Member, IEEE,* Yishan Yang, Yifan Zhang, Masoud Kaveh, Zheng Yan*, *Fellow, IEEE*

***Abstract*—Backscatter communication (BC) represents a wireless communication technology that facilitates the transmission of data by low-power devices, referred to as backscatter devices (BDs), through the modulation or reflection of pre-existing wireless signals, typically sourced from an access point (AP). The advent of the Internet of Things (IoT) has garnered significant attention and witnessed the widespread adoption of BC, primarily due to its exceptional energy-efficiency characteristics. Nevertheless, the security of BC systems faces substantial threats when deployed in practical scenarios due to their inherent openness. Specifically, wireless BDs, which directly engage with users, are susceptible to detrimental consequences in the event of interactions with counterfeit wireless APs. Owing to their non-authenticated and unconditional reflection properties, BDs are vulnerable to spoofing attacks orchestrated by malicious APs. Moreover, their limited computing capabilities make it challenging to employ intricate cryptographic algorithms. To tackle these challenges, we introduce APAuth, a lightweight authentication scheme that leverages the power value of BD to establish AP authentication. In this scheme, BDs and APs share a confidential key and engage in negotiations to determine a key generation algorithm. Subsequently, the current stored power value of BD is utilized to calculate the power value that must be delivered to BD from AP. If the computed charging power value aligns with the value determined by the key generation algorithm, the AP successfully passes the authentication of BD. We perform a thorough theoretical analysis of the security aspects inherent in our proposed scheme. We further conduct numerical simulations to validate the practical viability and desired performance of APAuth in diverse real-world scenarios.**

***Index Terms*—Backscatter Communication; Physical Layer Security; Device Authentication**

I. Introduction

Backscatter communication (BC) is a wireless communication method that empowers low-power devices, commonly referred to as backscatter devices (BDs), to convey data by either reflecting or modulating an existing wireless signal, typically originating from an access point (AP). BDs are typically low-power and low-cost devices that lack traditional radio transmitters. Instead, they communicate with other devices by reflecting or modulating radio frequency (RF) signals in the air from an RF source, such as an AP or a reader. As a result, BC offers many advantages. First, BDs are power-efficient, as they do not require a battery-powered transmitter. Second, they can operate for a long period consuming minimal energy. Additionally, BDs are relatively inexpensive, making them a cost-effective solution for various applications, such as environmental monitoring [1], smart agriculture [2], supply chain management [3], and healthcare [4], etc.

While BC offers numerous applications and advantages, it also poses security threats and vulnerabilities. In a wireless BC system, devices communicate by reflecting existing RF signals. This means that anyone with a suitable receiver can capture these signals and potentially eavesdrop on the communication or inject malicious data into the network. Without authentication, any device could potentially masquerade as an AP and communicate with BD to access sensitive information and privacy of the BDs. Therefore, authenticating the AP is crucial for maintaining the security and integrity of the BC system. By authenticating the AP, BD will prevent unauthorized access, data breaches, and system functionality disruptions. It establishes trust between BD and AP, ensuring that only legal and authorized communication takes place within the BC system.

Previous research studies such as RF-Rhythm [5], Tagora [6], and L-tag [7] discuss Radio Frequency Identification (RFID)-based identity authentication. Finger-print [8] explores authentication in BC, but focuses on BD authentication. SCBF [9] and BCAuth [10] can implement AP authentication, but both require support from an upper-layer protocol. In this paper, we present APAuth, a lightweight physical authentication scheme based on power value that allows BD to authenticate AP. The scheme contains three phases. In the initialization phase, BD and AP preload a secret and negotiate a key generation algorithm. In the preparation phase, BD sorts the APs according to the order of received messages. BD and legal AP substitute the power into the key generation algorithm negotiated in the initialization phase to get the power that needs to be charged and prepare for the authentication phase. In the authentication phase, the current power value of BD is used to calculate the power to be charged for BD, thus completing the authentication.

The main contributions of this article are as follows:

- We introduce APAuth, an authentication scheme based on power value that enables BD to authenticate AP. It provides resistance against eavesdropping attacks (EDA), replay attacks (RPA), relay attacks (RLA), and brute-force attacks (BFA).
- We enhance the scheme's security by considering the use of different frequencies of multi-channel to resist jamming attacks (JA), minimizing the possibility of security threats.
- We conduct theoretical analysis and perform numerous simulations under different parameters to demonstrate the strong security performance of APAuth.

II. Related Works

In this section, we review existing work on physical layer authentication related to AP authentication. We also

*Corresponding author

J. Chang, J. Li and Y. Yang are with the State Key Lab of ISN, School of Cyber Engineering, Xidian University, Xi'an, Shaanxi, 710026 China. (email: {jdchang, jiajunli1204, ysyangxd}@stu.xidian.edu.cn)

Y. Zhang and M. Kaveh are with the Department of Information and Communications Engineering, Aalto University, Espoo, 02150 Finland. (email: {yifan.1.zhang, masoud.kaveh}@aalto.fi)

Z. Yan (corresponding author) is with State Key Lab on Integrated Services Networks, School of Cyber Engineering, Hangzhou Institute of Technology, Xidian University, China. (email: zyan@xidian.edu.cn)

TABLE I: Summary and Comparison of Related Works

	Applicable Scenarios	Reverse Authentication	Mobility Support	Avoid Upper- Layer Support	Attack Resistance				
					EDA	RLA	RPA	BFA	JA
[5]	RFID	N	N	N	Y	Y	Y	N	N
[6]	RFID	Y	N	N	Y	Y	Y	N	N
[7]	RFID	Y	Y	Y	Y	Y	Y	Y	N
[8]	BD	N	N	N	Y	Y	N	N	N
[9]	BD	Y	Y	N	Y	Y	Y	Y	N
[10]	BD	Y	Y	N	Y	Y	Y	Y	Y
APAuth	BD	Y	Y	Y	Y	Y	Y	Y	Y

EDA: eavesdropping attack; RLA: relay attack; RPA: replay attack; BFA: brute-force attack; JA: jamming attack;
Y: supported; N: not supported.

compare the existing schemes with our scheme in Table I in terms of applicable scenarios, reverse authentication, mobility support, avoiding upper-layer support, and attack resistance.

Li *et al.* [5] proposed RF-Rhythm, which only addresses the authentication of RFID tags, and therefore does not support reverse authentication. As the devices need to maintain stability, the system does not support mobility. Additionally, since the analysis requires the assistance of a back-end server, the system requires support from an upper-level protocol. The RF-Rhythm system can withstand EDA, RLA, and RPA, but not JA. The article does not mention a defensive strategy for BFA.

Park *et al.* [6] proposed Tagora, which utilizes the unpredictable properties of the tag's collision responses at both layers. Similar to the previous article, Tagora enables mutual authentication between RFID readers tags, but can only resist EDA, RLA, and RPA.

Mehmood *et al.* [7] studied identity attacks on an RFID-based BC system. The challenge-response message exchange mechanism enables mutual authentication. This scheme can be completed at the physical layer without the need for upper-layer support, and it can also resist BFA, RLA and RPA.

Goki *et al.* [8] proposed a new method for network authentication, identification, and secure communication using the optical physical unclonable function Challenge-Response (PUF-CRPs) database protocol. This article addresses the BD authentication issue in the BC system, but it does not support reverse authentication. Additionally, it can only resist EDA and RLA.

Park *et al.* [9] utilized an unpredictable collision by applying a special type of data structure called Shifted Counting Bloom Filter (SCBF), which can reduce the overhead of BDs required for security. This scheme enables mutual authentication, but it requires support from an application layer protocol. In addition to JA, it can resist common types of attacks.

Wang *et al.* [10] proposed BCAuth, which innovatively achieves mutual authentication between AP and BD, and provides good resistance against various types of attacks. The measurement of angle and signal strength enables this scheme to support device mobility. However, this solution relies on support from the application layer.

In summary, RF-Rhythm, Tagora, and L-tag discuss RFID-based identity authentication. Finger-print studies authentication in BC, but focuses on BD authentication. SCBF and BCAuth can implement AP authentication, but both require support from an upper-layer protocol. The comparison results are summarized in Table I. We can easily see from the table that our scheme is the first one to resist various types of attacks without the support of the upper layer protocol.

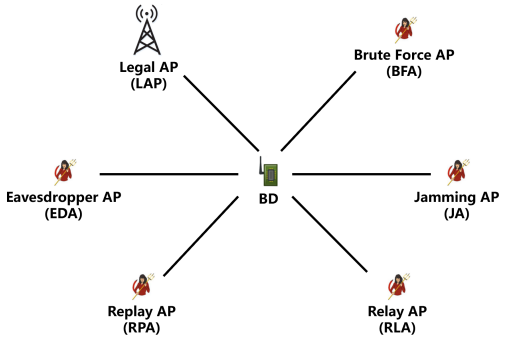


Fig. 1: System Model

III. Scheme Overview

In this section, we first introduce the system model and the security model and then provide an overview of APAuth.

A. System Model

Figure 1 illustrates the system model, which involves three types of devices: legal AP (LAP), fake APs (FAPs), and BD. FAPs can execute various types of attacks, including EDA, RPA, RLA, BFA, and JA.

The AP's position is fixed, while the BD can move within a spatial range. Additionally, the BD may receive signals from multiple APs. The BD separates the integrated signals and identifies different APs based on their signal characteristics. All APs within a BD's coverage area send signals to the BD in a time-division manner. In each time slot, the BD only receives signals from a specific AP, interacts with the AP in the environment, and determines the AP's legality based on the charging power value.

B. Security Model

Generally, the possible threats to the BC system mainly include EDA, RPA, RLA, BFA, and JA. Specifically, in an eavesdropping attack, the initiating FAP calculates the power value charged by the BD during each round of the authentication process by monitoring the signals in the environment and the BD's power value in real-time. The attacker then copies this power value to execute the attack.

In a BFA, the FAP repeatedly attempts to charge the BD with different battery values using violent enumeration and other methods to carry out the attack.

The FAP initiating the replay attack replicates the RF signal backscattered by BD to LAP, and replays the same

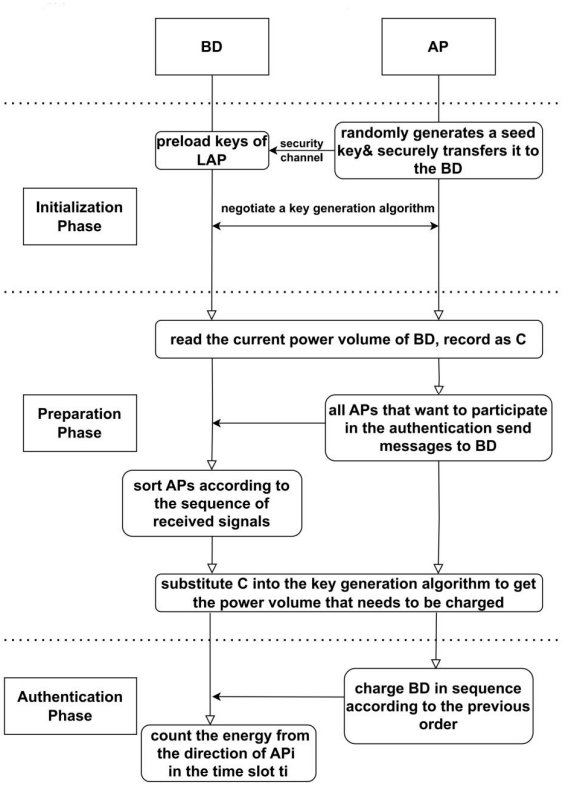


Fig. 2: Scheme Overview

signal to the BD in subsequent authentication. Specifically, in our system, this attacker monitors and intercepts the power value of the LAP charging the BD in the current time slot, and copies this power value to impersonate the LAP and charge the BD in the next time slot.

Compared to RPA, relay attackers simply involve forwarding backscattered signals from the BD to the LAP. To successfully impersonate a LAP, the attacker needs to be aware of the relative position of the LAP and the BD, and simulate itself as having the same position and angle as the LAP to forward signals to the BD, that is, the FAP relays the signal to the BD.

Furthermore, certain FAPs may launch JA by continuously emitting signals to interfere with the authentication process. In order to resist the above types of attacks, we first made the following basic assumptions on the model:

- The initialization phase is trustworthy, meaning the BD can preload secret information regarding the LAP. During the initialization phase, the LAP randomly generates a seed key, which is transmitted to the BD through a secure channel. A key generation algorithm is subsequently negotiated.
- The BD can differentiate between different APs based on received signals.
- A powerful attacker can intercept any communication between the LAP and the BD to obtain the AP's identity information.

The flowchart of our scheme can be seen as follows in Figure 2.

IV. Scheme Design

This section provides a detailed explanation of APAuth design, encompassing the initialization phase, preparation phase, and authentication phase. In response to the attack techniques outlined in Section III, we introduce random number (RN) into the key generation algorithm, using the seed key to encrypt the power value and an RN collectively to derive the round key. Additionally, to counter JA, we propose using orthogonal frequency division multiplexing (OFDM) to mitigate the problem.

A. Initialization Phase

Our authentication approach only accounts for situations where the BD and AP are in a stationary state. Although the BD's location can be moved, it must remain fixed during the authentication process. After determining the positions of the BD and AP in the system, all BDs must register with their authentic identities on the LAP, enabling the AP to obtain BD information. This algorithm incorporates specific information during verification, such as the RN, current power value, challenge-response, etc.

In accordance with the key generation algorithm presented by Li [11], a LAP randomly generates a seed key and securely transmits it to the BD. Subsequently, BD and FAP negotiate a key generation algorithm.

B. Preparation Phase

Following the initialization phase, the AP senses the existence of BDs in the environment, and the BD has negotiated the key generation algorithm to be used in subsequent rounds of authentication with the LAP. The key generation algorithm can be expressed as follows.

$$K = S \times (C + R), \tag{1}$$

where K represents the round key, S represents the seed key, C represents the current power value, and R symbolizes the RN. During the preparation phase, the BD authenticates the AP's identity by reading its own current power value. All APs intending to participate in the authentication process send messages to the BD. The BD then sorts these messages based on the order of received signals, resulting in a queue of APs $AP_n|n = [1, N]$. By substituting the power value into the key generation algorithm of the preparation phase agreed upon during the initialization phase, the BD and the LAP determine the power value to be charged.

In order to reduce the error between the actual charge and the calculated charge, AP needs to accurately control the power to charge BD. To achieve this, our solution employs the resource allocation optimization method [12] for AP charging of BD. The proposed scheme focuses on two key points: the algorithm should tolerate certain errors, and it should utilize the reverse estimate strategy. Specifically, when the AP sends an authentication request, BD responds with its current power value. Based on this response, the AP estimates the performance of the uplink and downlink, allowing it to adjust the charging power value and achieve accurate control. The specific implementation method is as follows.

The AP is an active device that can monitor the real-time power value of BD. The total power value q charged by the AP to BD within a given time range from 0 to t is represented by the integral equation:

$$q = \int_0^{t_0} I_t dt, \tag{2}$$

where I_t denotes the charging current from the AP to BD at time t. During the charging period, the AP can adjust its

charging speed (i.e., charging current i) based on the growth rate of BD power. This ensures that the total power received by BD is q within the time range from 0 to t_0.

C. Authentication Phase

BD authenticates each AP in sequence according to the AP queue arranged in the preparation phase. Specifically, when it is the turn of AP_i, BD reflects a start charging signal to AP_i. Only the energy from the direction of AP_i is counted in the subsequent time slot. The AP can estimate the signal loss in the transmission process by considering factors such as distance to adjust the signal strength during transmission. This ensures that the final power value charged to BD is within an acceptable range of the calculated power value from the formula. Consequently, a LAP is considered found.

Besides, in the scenario where three points are collinear, that is, two APs are on the same straight line with BD, BD provides feedback on messages sent by APs participating in the authentication. BD can differentiate two collinear APs based on the signal response time. The specific implementation method is as follows:

Assuming the distances between AP_1 and BD, and AP_2 and BD are l_1 and l_2 respectively ($l_1 \neq l_2$, and let $l_1 > l_2$). With the fixed propagation speed of electromagnetic waves in the air denoted as v_0, it follows that $l_1/v_0 \neq l_2/v_0$. BD starts timing from the moment it requires the AP to reflect the start charging signal sent by the AP that wants to participate in authentication. It stops timing upon receiving signals from AP_1 and AP_2, denoted as t_1 and t_2, where $t_1 \neq t_2$. Consequently, BD can distinguish between different APs from the different signal response time.

To prevent BD from reaching full power value after validating several APs, rendering subsequent validation impossible, a granular charge method can be employed. Taking into account the computational power of BD, the function is divided into three segments, with division points α and β. Within these three segments, multiply K by the coefficients 1, ξ_1, and ξ_2, where $\xi_2 < \xi_1 < 1$. The result is that the charging speed is fast when the battery is low and slows down as the battery level increases. Since our authentication method is based on the charging power value, the change of the power value determines the accuracy of authentication to a certain extent. In order to realize "fast charging at low power and slow charging at high power", we adopt the method of subsection charging, and the coefficient is small at high power. The coefficient is large when the power is low. Considering that the computational power of BD may not be applicable to overly complex rules, we divide the function into three sections. Assuming the round key calculated according to formula (1) is K and the current power value is C, the actual power value P to be charged in this round is determined as:

$$P = \begin{cases} K, & C < \alpha \\ K \cdot \xi_1, & \alpha \leq C \leq \beta \\ K \cdot \xi_2, & C \geq \beta \end{cases}$$

This transformation ensures that the battery cannot be fully charged during the authentication process. If the power value charged to BD is within an acceptable range of the calculated power value from the formula, a LAP is considered found.

V. Security Analysis

In this section, we provide a theoretical analysis of the security of AP against EDA, signal RLA, signal RPA, BFA, and JA.

A. Eavesdropping Attack

Proposition 1: The APAuth scheme can resist EDA.

Proof: During the initialization phase, both the BD and the LAP negotiate a seed key, denoted as S, and a key generation algorithm:

$$K = S \times (C + R), \tag{3}$$

where S represents the seed key, C represents the current power value, and R represents the challenge response. Since the attacker in an eavesdropping attack does not know S and R, if it calculates the round key using a wrong seed key $S^{'}$ and a wrong challenge response $R^{'}$, the round key would be:

$$K^{'} = S^{'} \times (C + R^{'}) \tag{4}$$

Obviously, $K^{'}$ is not equal to K, and thus the APAuth scheme can resist EDA.

B. Signal Replay Attack

Proposition 2: The APAuth scheme can resist signal RPA.

Proof: In a traditional signal replay attack, the attacker records the digital signals transmitted from the target BD and replays them to pass the authentication. In our system, the information copied by the FAP is not the message content, but the charging power value. Assuming we have not introduced the RN R, the formula would be:

$$K = S \times C \tag{5}$$

Since S is fixed, the same C would always result in the same K after calculation. The AP initiating the signal replay attack can conduct a series of experiments:

$$K_1 = S \times C_1; K_2 = S \times C_2; ...; K_n = S \times C_n \tag{6}$$

In this case, it is easy to guess the true S in the formula. To counter RPA, we introduce a challenge response obtained from the signal reflected from the BD into the original formula, as indicated in formula (1). Even if the current battery value C is the same, the resulting K would be different due to the different R values each time (let's take two examples: R_1 and R_2):

$$K_1 = S \times (C + R_1) \tag{7}$$

$$K_2 = S \times (C + R_2) \tag{8}$$

As seen, even if C is the same, the resulting K values differ due to the difference in R. Therefore, the APAuth scheme can resist signal RPA.

C. Signal Relay Attack

Proposition 3: The APAuth scheme can resist signal RLA.

Proof: Compared to RPA, RLA involves forwarding the backscattered signal from a legal BD to the AP. The AP conducting this attack needs to know the channel loss of the real AP and make compensation. However, in our system, the FAP cannot be aware of the channel loss of the LAP, making our system resistant to this type of attack.

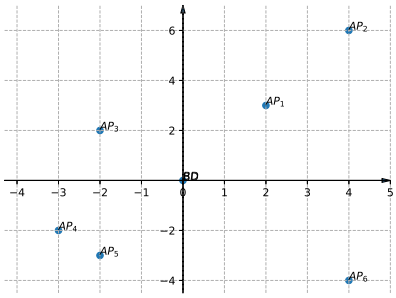


Fig. 3: Simulation Setting

D. Brute-Force Attack

Proposition 4: The APAuth scheme can resist BFA.

Proof: Let us assume that the electricity values at times T_1 and T_2 are both C_0. The corresponding calculated values, K_1 and K_2, at T_1 and T_2 are given by:

$$K_1 = S \times (C_0 + R_1) \tag{9}$$

$$K_2 = S \times (C_0 + R_2) \tag{10}$$

Since K_1 and K_2 are calculated using different values of R_1 and R_2, it follows that K_1 cannot be equal to K_2. Even if C_0 is the same, the calculated values of K will be different. Therefore, APAuth can resist BFA.

E. Jamming Attack

Currently, there is no research indicating that BD can utilize frequency hopping technology. However, if it becomes possible, we can consider using multiple channels with different frequencies to mitigate the problem.

In each round of authentication, a random channel is selected. If a FAP is jammed during this round, the next round will randomly jump to another channel, greatly reducing the probability of the FAP choosing the same channel again.

For example, suppose there are a total of 10 channels. During the first round of authentication, channel 5 is randomly selected for information exchange. If a FAP is jammed on the same channel, authentication cannot be completed. In the next round, a different channel is randomly selected, reducing the probability of being tracked twice to 1%. If it fails again, another random selection is made, reducing the probability of being tracked three times to 1%, and so on. This greatly reduces the success probability of JA.

VI. Performance Evaluation

In this section, we evaluate the performance of APAuth under various scenarios and parameters through extensive simulations.

A. Simulation Setting

In our simulation environment, we consider a BC system consisting of a BD and multiple APs. LAPs and several FAPs are randomly distributed within a radius of 0.5m around the BD. A plane rectangular coordinate system is established with the BD as the coordinate origin, as shown in Figure 3. Among them, AP_1 is a LAP, and the rest are FAPs.

In real-life scenarios, there are often obstacles between the BD and the APs. Hence, we model the simulated channel as independent complex Gaussian random variables (Rayleigh fading). The average power of the channel follows the contour [13], and the channel reciprocity is maintained within each time block of the coherent time. Referring to the works of [13] and [14], the forward and backward channel gain is set to $10^{-2}d^{-2}$, where d represents the distance between the BD and the AP [10].

B. Evaluation Metrics

We primarily consider two probability indicators, namely, the authentication rate (AR) and the false acceptance rate (FAR). The AR represents the true positive rate that a LAP is truly accepted by APAuth, while the FAR represents the false positive rate, which is the probability that a FAP is accepted by APAuth.

C. Simulation Results

In this section, we conduct three sets of experiments to investigate the performance of the system under different conditions: (i) varying the number of FAPs ($num_{FAP} = 0, 1, 2, ...$); (ii) fixing the number of FAPs to 5 and varying the average distance d between these six APs and the BD, evaluating the system's performance for different d values; (iii) assessing the performance of the BD when authenticating the AP under different electricity values. We use AR and FAR to quantitatively analyze the reliability of the system.

1) Performance under different numbers of FAPs: In our basic assumptions, we mentioned that there is only one LAP in the system. Hence, we set the number of FAPs num_{FAP} as 0, 2, 4, 5, 8. We evaluate the system performance for different numbers of FAPs, and the results are shown in Figure 4(a).

When the number of FAPs is 0, there is only one LAP in the environment, resulting in a 100% success AR, where both the AR and FAR values are 0. Figure 4(a) illustrates the gradual increase in AR and FAR with the increase in the number of FAPs. When the ratio of FAPs to LAP reaches 8:1, the AR and FAR values stabilize at approximately 15%.

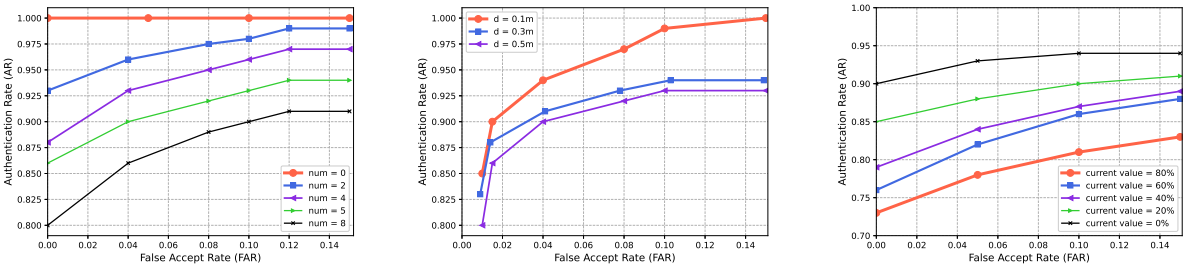
2) Performance under different average distances: In Experiment 2, we randomly place five FAPs and one LAP in the space. The average distance between the APs and the BD is denoted as d. The system performance was then evaluated under different average distances. The results are depicted in Figure 4(b).

From Figure 4(b), it can be observed that the AR and FAR values gradually increase with the average distance. When the average distance d reaches 0.5m, the AR and FAR values are approximately 15%.

3) Performance under different electricity values: In the third experiment, we investigated the performance of APAuth under various power values. As our scheme is based on charging power for authentication, different power values were examined. The results are shown in Figure 4(c).

From Figure 3(c), it is evident that the AR and FAR values gradually increase as the power value increases. When the power value approaches or reaches 100%, the AR and FAR values exceed 20%. However, in practical application scenarios, the BD equipment continuously consumes power, meaning that the power value will not remain near full power for an extended period.

We qualitatively compare APAuth with other related work. We found that APAuth is the first scheme that can authenticate AP without the help of a third-party server or upper-layer protocol. It can effectively resist EDA, RPA,



(a) Performance Under Different Number of FAPs

(b) Performance Under Different Average Distances

(c) Performance Under Different Electricity Values

Fig. 4: Simulation Results

RLA, and BFA. Our scheme has made great progress in active equipment authentication by passive equipment.

We try our best to compare its AR and FAR with the existing work [8], [9] and [10], all of which are applied in BC system. The parameters we set in the simulation are: the distance between BD and AP $d = 0.3m$, the signal power p=1, and the current power value of BD is 20%. From table II, we can see the comparison of AR and FAR of the two schemes. The larger the value of AR, the smaller the value of FAR, indicating the better performance of the system.

TABLE II: Comparison of AR and FAR

	[8]	[9]	[10]	APAuth
AR	72%	79%	85%	93%
FAR	8.7%	12%	6%	5.6%

From Table II, we can see that APAuth performs better than other schemes considering AR and FAR. Through the aforementioned experiments, it can be concluded that in most cases, our scheme can control the AR and FAR values within 10%, meeting the requirements of practical application scenarios. Considering the other advantages of APAuth, we believe that APAuth has substantial potential in real-world applications.

VII. Conclusion

This paper presented APAuth, an innovative authentication scheme to authenticate AP by a BD by measuring charged power value BD. The security of APAuth was analyzed. A series of experiments were conducted to verify the feasibility and performance of APAuth in different scenarios. The experimental results demonstrate that APAuth achieves expected performance without the assistance of a third party or an upper-layer protocol, and meets practical security requirements. Our future research will focus on verifying the performance of APAuth based on a prototype and improving its design towards practical application.

Acknowledgments

This work is supported in part by the National Natural Science Foundation of China under Grant U23A20300 and 62072351; in part by the Key Research Project of Shaanxi Natural Science Foundation under Grant 2023-JC-ZD-35; in part by the Academy of Finland under Grant 345072 and Grant 350464.

References

[1] M. Snellen, T. C. Gaida, L. Koop, E. Alevizos, and D. G. Simons, "Performance of multibeam echosounder backscatter-based classification for monitoring sediment distributions using multitemporal large-scale ocean data sets," *IEEE Journal of Oceanic Engineering*, vol. 44, no. 1, pp. 142–155, 2019.

[2] S. N. Daskalakis, S. D. Assimonis, G. Goussetis, M. M. Tentzeris, and A. Georgiadis, "The future of backscatter in precision agriculture," in *2019 IEEE International Symposium on Antennas and Propagation and USNC-URSI Radio Science Meeting*, 2019, pp. 647–648.

[3] 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," *Proceedings of the IEEE*, vol. 98, no. 9, pp. 1583–1592, 2010.

[4] M. Stanaćević, A. Ahmad, X. Sha, A. Athalye, S. Das, K. Caylor, B. Glisić, and P. M. Djurić, "RF backscatter-based sensors for structural health monitoring," in *2021 International Balkan Conference on Communications and Networking (BalkanCom)*, 2021, pp. 71–74.

[5] J. Li, C. Wang, A. Li, D. Han, Y. Zhang, J. Zuo, R. Zhang, L. Xie, and Y. Zhang, "RF-Rhythm: Secure and usable two-factor RFID authentication," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, 2020, pp. 2194–2203.

[6] H. Park, H. Roh, and W. Lee, "Tagora: A collision-exploitative RFID authentication protocol based on cross-layer approach," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3571–3585, 2020.

[7] A. Mehmood, W. Aman, M. M. U. Rahman, M. A. Imran, and Q. H. Abbasi, "Preventing identity attacks in RFID backscatter communication systems: A physical-layer approach," in *2020 International Conference on UK-China Emerging Technologies (UCET)*, 2020, pp. 1–5.

[8] P. N. Goki, T. T. Mulugeta, N. Sambo, R. Caldelli, and L. Potì, "Optical network authentication through rayleigh backscattering fingerprints of the composing fibers," in *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, 2022, pp. 2146–2150.

[9] H. Park, J. Yu, H. Roh, and W. Lee, "SCBF: Exploiting a collision for authentication in backscatter networks," *IEEE Communications Letters*, vol. 21, no. 6, pp. 1413–1416, 2017.

[10] 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.

[11] J. Li, P. Wang, L. Jiao, Z. Yan, K. Zeng, and Y. Yang, "Security analysis of triangle channel-based physical layer key generation in wireless backscatter communications," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 948–964, 2023.

[12] P. Wang, Z. Yan, N. Wang, and K. Zeng, "Resource allocation optimization for secure multidevice wirelessly powered backscatter communication with artificial noise," *IEEE Transactions on Wireless Communications*, vol. 21, no. 9, pp. 7794–7809, 2022.

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

[14] P. Wang, N. Wang, M. Dabaghchian, K. Zeng, and Z. Yan, "Optimal resource allocation for secure multi-user wireless powered backscatter communication with artificial noise," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, 2019, pp. 460–468.