A Secure and Private Authentication Based on Radio Frequency Fingerprinting

Chengchen Zhu*, Kunling Li *, Jianan Hong*, Cunqing Hua*, Futai Zou*
*School of Cyber Science and Engineering, Shanghai Jiao Tong University, China
Email: {zcc815107613, likunling.jingjing, hongjn, cqhua, zoufutai}@sjtu.edu.cn

***Abstract*—The technology development of wireless communication has brought about the rapid growth of various wireless devices, but also brings in many security threats. This paper focuses on the security and privacy problems in wireless authentication and proposes a novel authentication scheme based on the design of reusable fuzzy extractor (RFE) for device's radio frequency (RF) fingerprinting. Firstly, unlike the traditional authentication protocol, our scheme can accomplish the mutual authentication without the storage of long-term secret key, thus tackles with the key-compromise threats. Furthermore, although the scheme authenticates devices based on their RF fingerprint, it does not store RF fingerprinting information explicitly to safeguard it from eavesdroppers who may use it to impersonate the identity of valid users. Finally, our designed protocol relies on the correspondent peer to measure the fingerprint, rather than the device itself, thus is more secure against various adversaries. The security analysis shows the resiliency against theft of secret keys, wireless channel attacks and privacy disclosure. And the performance evaluation demonstrates that the design of RFE for device's RF fingerprinting is efficient in terms of recognition accuracy.**

***Index Terms*—Reusable Fuzzy Extractor (RFE), Radio Frequency (RF) fingerprinting, authentication.**

I. Introduction

The 5th generation standard for broadband cellular networks (5G) has developed significantly recently and it is not just limited to mobile broadband. 5G is designed to apply in a wide range of usage scenarios that fall into these categories: higher data rates for high-speed mobility, low data rate and low power devices, reliable and resilient network security, etc. [1]. The traditional mobile network system uses Subscriber Identity Module (SIM) cards for authentication and key agreement. However, especially in the field of Internet of Things (IoT), the increasing number of network devices brings in lots of deployment burden with such method and IoT connectivity has different requirements from typical end-user connectivity [2]. And much worse, there exist security threats by various attackers, including Man-in-the-Middle attack, the DoS attack and DNS spoofing [3]. Thus, 3GPP aims to eliminate the dependence on Subscriber Identity Module (SIM) cards in the scope of IoT and lots of network service providers are seeking for new techniques to substitute SIM based methods [4]. However, new methods will expose more threats, as the trusted management of keys no longer exists.

Radio frequency fingerprinting is one of the new techniques with the potential to provide effective authentication for wireless networks. Unlike traditional key-based authentication schemes that operate at the MAC layer and above [5], RF fingerprinting leverages tiny hardware-level imperfections at the physical layer. The hardware-level differences such as I-Q imbalance and PA nonlinearity [6] are introduced in the circuit design and production of devices, which is also inevitable for devices of the same model from the same manufacturer [7], [8], [9]. These hardware differences cause tiny distortions between the actual RF signal and the ideal signal, which can be leveraged through RF fingerprinting to analyze the received signal, extract the hardware features from these distortions, and complete device identification. Similar to Physical Unclonable Function (PUF), this technique is effective in resisting replay attacks as hardware-level imperfections cannot be imitated by adversarial devices. However, current schemes leak privacy: like other authentication schemes based on fingerprinting, it requires a database to compare the received fingerprint with the stored, which will raise critical privacy issues [10].

Fuzzy extractor (FE) can protect the privacy of fingerprints. It takes the noisy nonuniform information as input, e.g., iris, and outputs reliably reproducible, uniformly random strings. The extraction is error-tolerant because it is able to generate the same random strings even if the input is different, as long as it remains reasonably close to the origin [11]. Furthermore, if FE is reusable, i.e., reusable fuzzy extractor (RFE), it is able to generate different secret strings from the same source, which ensures the reuse of the same fuzzy secret and overcomes the major shortcoming in the case of biometric applications [12]. Despite the improvement of privacy preservation on fingerprinting-based authentication, current RFE schemes rely on the device itself to measure the fingerprint, which is not suitable: from the sight of verifier, it still uses key-based authentication. Thus, it cannot preserve most of the security properties from fingerprinting-based authentication.

In RF fingerprinting related areas, researchers tend to focus on improving the recognition accuracy. For instance, authors in [13] achieved better results to eliminate the effects of channel and in [14] carrier frequency offset on robustness was discussed. With respect to RFE related areas, there already exist some researches combing biometrics with RFE to implement authentication. In [15], authors present secure authentication for IoT devices that is based on the feature extraction of the biometrics and an effective key agreement scheme. In [16], authors propose a reliable authentication protocol for wireless medical sensor networks using PUF and RFE. However, now few researchers attempt to combine RF fingerprinting with RFE and the existing authentication schemes rely the

ICC 2024 - IEEE International Conference on Communications | 978-1-7281-9054-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICC51166.2024.10622361

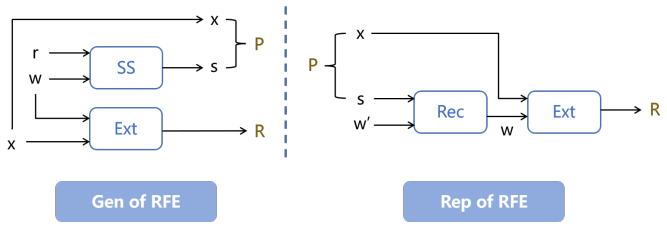


Fig. 1: Typical implementation of RFE

fingerprint owner to measure its features, which has the same threats in key-based authentication methods.

In this paper, we propose a new authentication scheme based on RF fingerprinting and RFE. In our scheme, RF fingerprinting is the authentication factor of the mobile device, and RFE is used to preserve the privacy of the RF fingerprinting information. Unlike existing schemes, the receiving node measures the RF fingerprinting and makes a mutual authentication between end device and the network, which is further analyzed to well resist various network attacks, such as Man-in-the-Middle attack, replay attack, etc. The main contribution of this paper can be summarized as follows:

1) It is the first that proposes a privacy preserving RF fingerprinting-based authentication scheme based on the idea of RFE. As the authentication relies on receiving node to measure the fingerprint, it tolerates more attacks compared with existing schemes.
2) We design a challenge/response-based protocol for the proposed fingerprinting-based authentication scheme. As a result, the device only needs to store a public key, while the related secret key is not stored in any peer, thus secures the security on a very high level.
3) Our further analysis shows the scheme can resist various attacks, with very slight computation and communication cost. Experiment results on public dataset show its feasibility for both recognition and false acceptance ratio.

The organization of the rest of the paper is as follows: Section II introduces some preliminaries about RFE and RF fingerprinting. Section III illustrates the system model and security requirements. Section IV shows our construction of the proposed protocol. Section V presents the security analysis of the protocol. The performance of the proposed protocols is demonstrated in Section VI followed by the conclusion in Section VII.

II. Preliminaries

A. Reusable Fuzzy Extractor

RFE is composed of two randomized procedures: Gen (generate) and Rep (reproduce). In the generation procedure, it inputs the fingerprint string W and then gets an extracted secret string R and a helper string P. In the reproduction procedure, it inputs a new fingerprint string W' and a previous saved string P. And if the difference between W and W' is small enough, RFE will reproduce the same secret string R

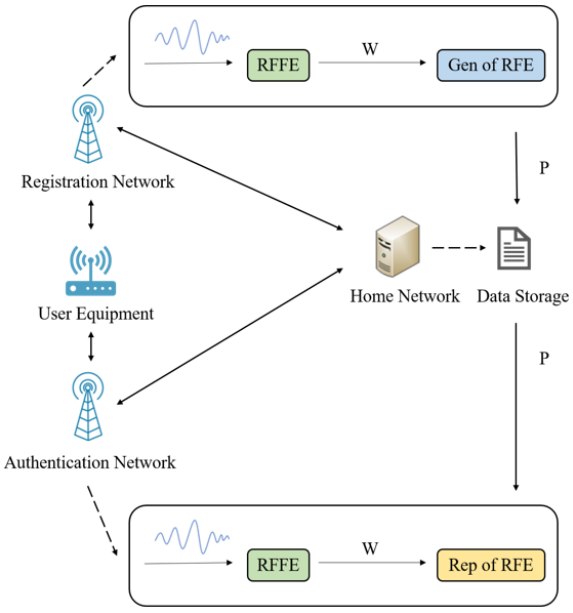


Fig. 2: System Model

[11]. The string R retains uniformly random even given P, so it can be used to generate symmetric or asymmetric keys without exposing the information of the fingerprint owner, which is suitable to build a biometric authentication protocol.

As shown in Fig. 1, the typical RFE usually uses secure sketch to realize Gen and Rep and a random number x to satisfy the reusable feature. In Gen, $sketch$ (SS) takes a random number r and fingerprint w as input and outputs a helper string s. In Rep, $recover$ (Rec) uses s and the new fingerprint w' to reproduce the original fingerprint w. And with a strong extractor Ext, it can extract the uniform randomness R if the input is the same.

B. Radio Frequency Fingerprinting

RF fingerprinting has the feature that even if the message content is the same, as long as the sender is different, the fingerprint information will be different. The generic methodology for RF fingerprinting can be divided into three parts: signal acquisition, preprocessing and fingerprint identification. In signal acquisition, the baseband transmitted signal will be processed by hardware components such as oscillator and power amplifier, which have their specific impairments. Then the received signal needs to be pre-processed before it can be used for fingerprint identification, including filtering, normalization, synchronization and target signal extraction. Finally the fingerprint identification algorithms are designed to identify wireless devices and detect invalid devices using the processed data, including supervised learning and unsupervised learning algorithms. In the sections below, we will use Radio Frequency Fingerprint Extractor (RFFE) to represent the whole process.

III. System Model

As shown in Fig. 2, our scheme works in a system consisting of User Equipment (UE), Registration Network (RN), Authentication Network (AN) and Home Network (HN). Their roles and our security assumptions are described as follows.

A. Architecture

In this architecture, RN and AN are maintained by HN. UE initiates the registration or authentication process ,but it is not trusted by the HN to store some sensitive secrets(e.g., private keys or passwords), just like the trust model as 5G AKA. When it sends a message, no matter what the content is, the RF fingerprint information will be included in it and then measured by the receiver.

In the registration phase, RN receives the message under a secure channel to extract the RF fingerprint with RFFE and uses it in RFE to generate the required data, which can be carried out during device production to ensure security and reliability. The required data will be stored in HN for later authentication. In the authentication phase, all messages between UE and AN are transmitted in public channels. AN triggers a request to obtain the data in HN, which is combined with the RF fingerprint information extracted from the message as the input of RFE to verify the device.

B. Trust Assumption and Security Requirements

In our scheme, UE and RN trust each other during the registration phase, which means the communication channel in registration is secure. However, UE and AN are uncertain whether the other party is valid during authentication and threats may exist throughout the authentication process. Such security assumption can well model the real-world communication, as registration should takes part in some controlled environment (e.g., Service Hall of the network service provider); whereas, the authentication should happen anywhere though insecure channels.

HN can be totally trusted to assist the mutual authentication between UE and AN. But as a single bottleneck point of the whole system, the adversaries will try their best to compromise it to retrieve some sensitive data stored there. Thus, the privacy issue should be taken into account.

We adopt the Dolev-Yao model as the attack model to the network. The security requirements below should be satisfied to realize a secure system.

- *Secret Key Secrecy.* Secret keys are often used in various authentication protocols and key leakage will cause serious security problems. An excellent authentication protocol should pay attention to the storage of keys and prevent key exposure.
- *Wireless Channel Protection.* Wireless channels are insecure and vulnerable to various attacks. It is noteworthy to consider how to resist various attacks like replay attacks or Man-in-the-Middle attacks.
- *Privacy Preserving.* The service provider usually stores a large amount of user data and it is vital to prevent users' privacy from leaking.

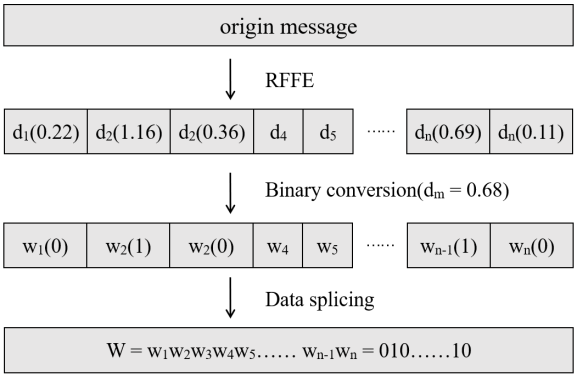


Fig. 3: RF Fingerprint Processing (d_m is the median)

IV. Construction

A. Overview

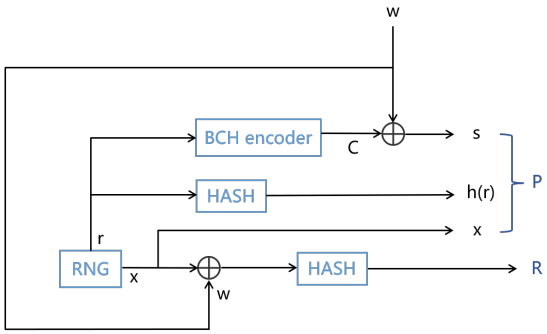
In our scheme, UE sends a request with its radio transmitter, which will automatically append some unclonable features. Then RN/AN controlled by HN will measure the features and use RFE to generate the keys for registration/authentication. The verifier measuring the features improves the security in key-based methods and RFE accomplishes the goal of protecting the privacy of the RF fingerprint. Also, when UE wants to start a mutual authentication procedure at some point, AN is able to use the receiving message from UE to reproduce the secret key. Table I below shows the descriptions and their meanings in this paper.

TABLE I: Notations and Descriptions

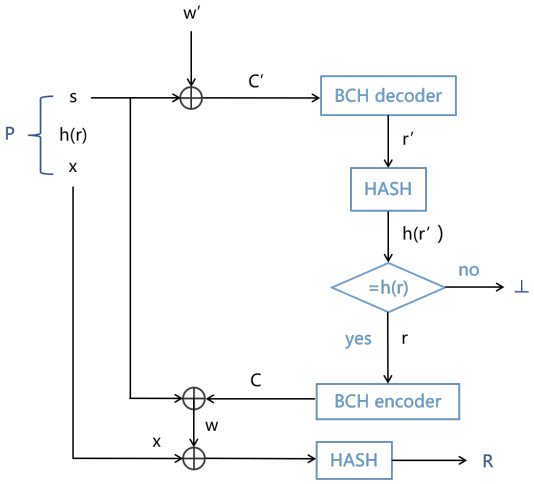
Notations	Descriptions
D	Initial RF fingerprint information
W	Processed RF fingerprint information
R	Secret string generated by RFE
P	Helper string generated by RFE
sk	Private key in a pair of asymmetric keys
pk	Public key in a pair of asymmetric keys
r	Origin random number
E	Encrypted random number
f	Message authentication function

B. RF Fingerprint Processing

The RFE adopted in our scheme uses Hamming distance to distinguish different inputs. However, the origin output of the RF fingerprinting is usually a multi-dimensional vector, which cannot be taken as the input of RFE directly. Thus, as illustrated in Fig. 3, we need several steps to get the final RF fingerprint W as input. When receiving the message, we can get the initial fingerprint information D by RFFE. D is an n dimensional vector, and each dimension value d_i is float-type data. We calculate the median of all data and get d_m. If d_i is greater than d_m, we converts it into 1, otherwise 0. Finally, each d_i is transformed into w_i and we can get the final result W by splicing them. Such a quantization process will bring



(a) Gen of RFE



(b) Rep of RFE

Fig. 4: Construction of RFE

about a loss of accuracy, but according to the later analysis, the improvement of the error tolerance of RFE can fill the loss and still achieve an ideal effect.

C. BCH based RFE

The RFE employed in our paper is based on [11]. In essence, we utilize BCH error-correcting codes, Random Number Generator (RNG) , and Secure Hash Algorithms (SHA) to construct a RFE that is amenable to practical implementation in real-world settings. The whole process is shown below in Fig. 4.

The primary concern in RFE is the construction of SS and we use the code-offset construction. In Gen, we input w and use it to output R and P. With an XOR operation $C \oplus w$, we get the output s, which gives it the error-tolerant ability for our second fingerprint input. In Rec, we decode r using C' if the hamming distance of w and w' is smaller than the error correction capability of the BCH code. Usually, the above construction is sufficient, but our scheme needs to check whether the correct R is generated. Thus, we add an additional $h(r)$ in P to verify the result in Rep. If the verification fails, RFE will output $\perp$.

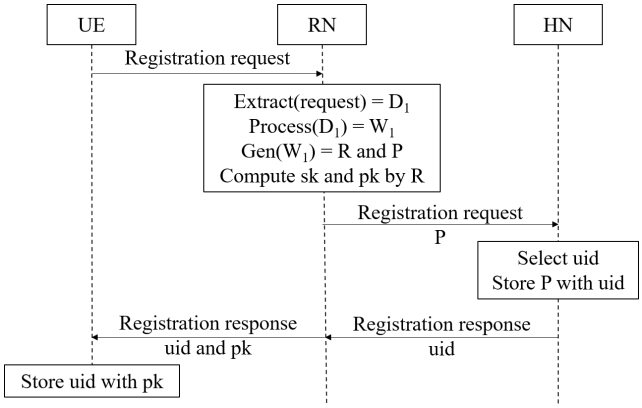


Fig. 5: Registration Phase

D. Registration Phase

This phase happens between UE, RN and HN to generate and store the necessary information for subsequent authentication. The registration phase is shown in Fig. 5.

Step-1: UE sends a registration request to RN and starts the registration process.

Step-2: After receiving the registration request, RN extracts the RF fingerprint information D_1 and processes it into W_1. RN uses W_1 as the input in Gen to generate R and P. Then it generates asymmetric key sk and pk using R and sends the registration request and P to HN.

Step-3: HN receives the registration request and selects a new user identifier uid. Then HN stores P with uid and sends the registration response containing uid to RN.

Step-4: RN receives the response and sends the response to UE with uid and pk.

E. Authentication Phase

This phase happens between UE, AN and HN to finish a mutual authentication process with the registration information. The authentication phase is shown in Fig. 6.

Step-1: UE selects a random number as r_u, searches the pk corresponding to HN and uses it to encrypt r_u. Then UE sends the encrypted E_u with uid to AN.

Step-2: AN receives the request and extracts the RF fingerprint information D_2. After processing it into W_2, AN forwards the request to HN to get the previously stored P.

Step-3: HN finds P with uid and passes it to AN.

Step-4: AN uses W_2 and P as the input in Rep to reproduce R and P. If R is generated successfully instead of invalid output $\perp$, AN authenticates UE successfully. Then AN regenerates asymmetric key sk and pk using R and decrypts E_u with sk. To calculate the session key and finish a mutual authentication, AN selects a random number as r_s. K and MAC will be calculated by r_s and r_u using different message authentication functions. At last, AN sends r_s and MAC to UE.

Step-5: After receiving the authentication response, UE calculates $XMAC$ and compares it with MAC. If they are

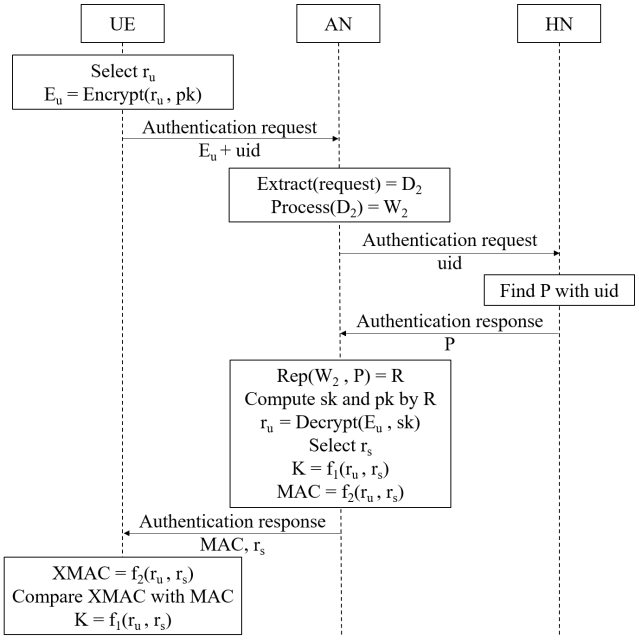


Fig. 6: Authentication Phase

the same, UE authenticates HN. Then UE calculates K and uses the session key for subsequent communication.

V. Security Analysis

A. Security in Insecure Wireless Channel

The proposed scheme resists various attacks in wireless channel, including identity forge, replay attack, man-in-the-middle (MitM) attacks. It is realized due to the usage of unclonable RF fingerprint. We allow the adversaries to try any attack methods (active or passive) to disturb the communication channel, but it cannot forge a physical-layer "impairments",which is regarded as the fingerprint characters for the the opposite side's measuring. Due to the above reason, it is impossible for the adversary to impersonate the UE's identity (by replay, MitM, or even more complex methods). On the other hand, it is also difficult for an attacker to impersonate the server's identity to become a fake base station. Nobody can regenerate the secret key without P, thus cannot complete the response of user's challenge in the authentication procedure.

B. Secret Key Secrecy

In key-based authentication schemes, security threat should be taken into account that the long-time secret keys may be hacked by adversaries. Luckily, our scheme stores no secret keys, either on UE or HN. The only stored data are the public key (on UE side) and the helper information (on HN side).

The public key storage is secure. On the one hand, the corresponding secret key is stored nowhere, instead, it is only generated via Rep function of RFE and cached temporarily. On the other hand, different devices (even registered in the same HN) stored diverse public keys (of course with different relevant secret keys), due to their different RF fingerprints. Thus, even a secret key is leaked unluckily during its caching time, the threat does not affect the other UEs.

The helper key P contains no knowledge of the secret information, even the associated secret keys.

In addition, in existing RFE schemes, the user generates the secret key by themselves by measuring its own biometrics, and this gives attackers an opportunity to take advantage of it to steal user's secret key. Especially when users are hijacked by attackers and their biometrics are leaked during a certain collection process. As a comparison, our scheme lets the AN directly measure the unclonable features to run RFE, thus resists such attack.

C. Privacy Preserving

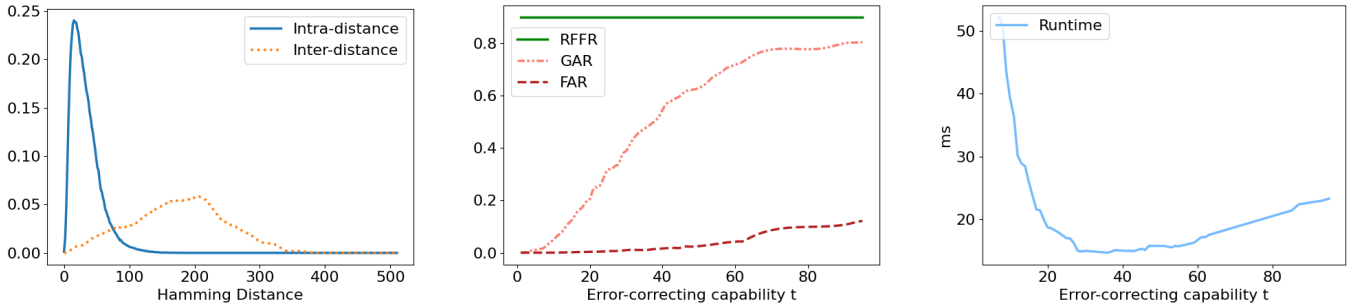
The proposed scheme preserves UE's privacy against potential HN compromise, which means all data stored in the HN can be known to the adversaries. We achieve it by using the secure RFE, which verifies an authentication by measuring RF fingerprint, but without storing any knowledge on real character. The helper string P stored in the HN leaks not one bit of the characters. Thus, even in the worst case, i.e., the server's database is invaded, the attacker cannot obtain any useful information about the user's identity.

VI. Performance Analysis

This section evaluates the feasibility in the real experiments. We use the data set and the training model from [13] to produce the initial data about RF fingerprinting. And the RFE adopted in our work is proposed in Section III-C. The initial RF fingerprinting data is 511-dimensional bitwise vector.

Initially, we focus on the performance of the quantized RF fingerprint data. Within the confines of our scheme, it is of paramount importance to differentiate distinct devices via their RF fingerprints. To put it another way, our objective is to minimize the hamming distance for same devices while simultaneously maximizing it for different devices, thereby effectively precluding any potential confusion. To be more specific, we employ the term "Intra-distance" to denote the hamming distance between same devices and "Inter-distance" to represent that between different devices. As shown in Fig. 7(a), the probability distribution of Intra-distance is concentrated below 50, while that of Inter-distance is concentrated above 100. This indicates that our current quantization method can effectively distinguish between the same and different devices through the hamming distance.

Next, we turn our attention to the performance of RFE accuracy when applied to RF fingerprints. The RFE we employ is based on BCH error-correcting codes, and as such, we will observe its specific performance by altering its error-correcting capability t. We focus on two indicators, Genuine Acceptance Rate (GAR) and False Acceptance Rate (FAR). GAR represents that we have correctly authenticated a legitimate user, while FAR represents that we have mistakenly authenticated an illegitimate user. And we should compare our performance of RFE with origin RF fingerprinting rate (RFFR). As shown in Fig. 7(b), as t increases, GAR and FAR



(a) Intra-distance and Inter-distance (b) Authentication Accuracy (c) Computational Overhead

Fig. 7: Evaluated Results on Critical Aspects

also increase and RFFR can be approximated by GAR. This result is in line with our expectations because the increase in t means that we have a higher tolerance for the differences between two fingerprint information inputs. This makes it easier to authenticate the same device, while some different devices with smaller Hamming distance differences can also be mistakenly authenticated. Thus, we need to select a suitable value for t to ensure that FAR remains low while obtaining a high GAR close to RFFR.

At last, we evaluate the computational overhead. As shown in Fig. 7(c), as t increases, our runtime increases initially and then decreases. For each value of t, we calculate its authentication success rate and determine the runtime by multiplying the expected number of authentication attempts by the duration of each individual attempt. Based on the data in the graph, we can obtain the lowest runtime at $t = 43$.

VII. Conclusion and Future Work

In this paper, we have proposed a mutual authentication scheme combining RF fingerprinting with RFE. The proposed scheme has been analyzed on its security functionality and it shows its advantage on stronger security compared with traditional schemes. Our future work is to strengthen trust level of authentication by implementing our proposed scheme in a multi-factor authentication. We are trying our effort to combine our RF fingerprinting-based authentication mechanism with 5G AKA architecture, which may be more reliable as current products.

Acknowledgment

This work was supported by National Key Research and Development Program of China (2022YFB2702302), and Natural Science Foundation of China (62171278, 62202290).

References

[1] M. Shafi, A. F. Molisch, P. J. Smith, T. Haustein, P. Zhu, P. De Silva, F. Tufvesson, A. Benjebbour, and G. Wunder, "5g: A tutorial overview of standards, trials, challenges, deployment, and practice," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 6, pp. 1201–1221, 2017.

[2] P. Annamalai, J. Bapat, and D. Das, "Emerging access technologies and open challenges in 5g iot: From physical layer perspective," in *2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2018, pp. 1–6.

[3] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196–248, 2020.

[4] B. A. Abdou, "Commercializing esim for network operators," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, 2019, pp. 616–621.

[5] A. Al-Shawabka, F. Restuccia, S. D'Oro, T. Jian, B. C. Rendon, N. Soltani, J. Dy, S. Ioannidis, K. Chowdhury, and T. Melodia, "Exposing the fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*. IEEE, 2020, pp. 646–655.

[6] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, 2008, pp. 116–127.

[7] M. Cekic, S. Gopalakrishnan, and U. Madhow, "Wireless fingerprinting via deep learning: The impact of confounding factors," in *2021 55th Asilomar Conference on Signals, Systems, and Computers*. IEEE, 2021, pp. 677–684.

[8] A. C. Polak and D. L. Goeckel, "Wireless device identification based on rf oscillator imperfections," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2492–2501, 2015.

[9] A. C. Polak, S. Dolatshahi, and D. L. Goeckel, "Identifying wireless users via transmitter imperfections," *IEEE Journal on selected areas in communications*, vol. 29, no. 7, pp. 1469–1479, 2011.

[10] X. Guo, Z. Zhang, and J. Chang, "Survey of mobile device authentication methods based on rf fingerprint," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2019, pp. 1–6.

[11] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *International Conference on the Theory and Applications of Cryptographic Techniques*, 2004.

[12] X. Boyen, "Reusable cryptographic fuzzy extractors," in *Proceedings of the 11th ACM Conference on Computer and Communications Security, CCS 2004, Washington, DC, USA, October 25-29, 2004*, 2004.

[13] G. Shen, J. Zhang, A. Marshall, and J. R. Cavallaro, "Towards scalable and channel-robust radio frequency fingerprint identification for lora," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 774–787, 2022.

[14] M. Cekic, S. Gopalakrishnan, and U. Madhow, "Wireless fingerprinting via deep learning: The impact of confounding factors," in *2021 55th Asilomar Conference on Signals, Systems, and Computers*. IEEE, 2021, pp. 677–684.

[15] A. Bentahar, A. Meraoumia, H. Bendjenna, S. Chitroub, and A. Zeroual, "Fuzzy extractor-based key agreement for internet of things," in *2020 1st International Conference on Communications, Control Systems and Signal Processing (CCSSP)*, 2020, pp. 25–29.

[16] W. Wang, Q. Chen, Z. Yin, G. Srivastava, T. R. Gadekallu, F. Alsolami, and C. Su, "Blockchain and puf-based lightweight authentication protocol for wireless medical sensor networks," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8883–8891, 2022.