Enhancing Wi-Fi Device Authentication Protocol Leveraging Channel State Information

Bing Chen[1,2,3], Yubo Song[1,3(✉)], Tianqi Wu[1,3], Tianyu Zheng[1,3], Hongyuan Chen[1,3], Junbo Wang[2,3], and Tao Li[1,3]

[1] School of Cyber Science and Engineering, Key Laboratory of Computer Network Technology of Jiangsu Province, Southeast University, Nanjing, China
[2] School of Information Science and Engineering, Southeast University, Nanjing, China
[3] Purple Mountain Laboratories, Nanjing, China
songyubo@seu.edu.cn

Abstract. Wi-Fi device authentication is crucial for defending against impersonation attacks and information forgery attacks. Most of the existing authentication technologies rely on complex cryptographic algorithms. However, they cannot be supported well on the devices with limited hardware resources. A fine-grained device authentication technology based on channel state information (CSI) provides a non-cryptographic method, which uses the fingerprint extracted from CSI for authentication since CSI can uniquely identify the device in a limited time. But maintaining a fingerprint database for fingerprint matching is a challenging work. Firstly, the fingerprints extracted from the CSI are time-sensitive, which means that the fingerprint database must be updated in real time; Secondly, the authentication device may collect false fingerprints under the attack of identity-based attackers, which means that the authenticity of the fingerprint used to update the database must be checked. In this paper, we propose an enhancing Wi-Fi device authentication protocol based on CSI to implement the fingerprint database update and the device authentication. We provide a viable method of database update and an authentication algorithm based on Local Outlier Factor (LOF). We also present a complete authentication process. In addition, we evaluate the performance of our CSI-based authentication algorithm and database updating method. The experiments showed that the accuracy of the authentication algorithm is up to 97.1% and our database updating method can help the system maintain high accuracy.

Keywords: Wi-Fi device authentication · Channel state information (CSI) · Local outlier factor (LOF) · Wireless physical fingerprintfing

J. Xiong et al. (Eds.): MobiMedia 2021, LNICST 394, pp. 33–46, 2021.
https://doi.org/10.1007/978-3-030-89814-4_3

1 Introduction

Nowadays, Wi-Fi has become one of the most important association technologies. However, there are serious security problems in Wi-Fi association. Attackers can get other devices' identity information through wireless sniffing, and then use the information to disguise themselves as legitimate devices [7,8]. Attackers can steal confidential data or attack the internal websites after getting authorization [1], or they can control other devices by sending spurious instructions [14]. Therefore, the authentication of Wi-Fi devices is indispensable. 802.11i provides some cryptographic-based device authentication method, but has proven security weaknesses [2,3,12]. What's more, a part of Wi-Fi devices does not have enough hardware resources to support these authentication schemes, which brings challenges to the usage of cryptographic-based device authentication technology.

In recent years, people tried to use wireless channel characteristics for device authentication. One of the methods is to extract fingerprints that can identify the device from CSI and use fingerprint matching to verify devices' identity [4,8,13]. The principle of this method is that under the influence of multipath and environmental fading, the amplitude and phase of each sub-carrier contains unique spatial information, which means devices at different locations have different CSI. Some existing CSI-based device authentication schemes can do identify matching with high accuracy [5,6,9–11]. [12] provides an identification scheme and authentication protocol in detail, and it also gives a framework to defend against attackers. As we all know, device authentication is a long-term work, and the channel state will change over time. Thus, the CSI of the device will also change and cause the current CSI and the fingerprints in database to not match, and the legal device will be rejected. Maintaining a valid fingerprint database in the authentication device during the long-term work is significant for device authentication. However, all the authentication system given above do not provide a solution for fingerprint database update.

In this paper, we propose an enhancing Wi-Fi device authentication protocol. We focus our attention on two application scenarios, including the authentication in access phase and the authentication in association phase. In two scenarios, we provide different fingerprint database updating method and authentication processes. Based on the fact that CSI can uniquely identify devices [7], our protocol extracts fingerprints from CSI and uses them to verify the identity of unknown devices by fingerprint matching.

The main contributions of this paper are as follows:

- We propose an enhancing Wi-Fi device authentication protocol based on CSI.
- We provide a method of fingerprint database update, which can update the fingerprint database effectively in both access phase and association phase. It can help to maintain a low false rejection rate during long-term work, and it can effectively detect the identity-based attackers on the other hand.
- We provide a complete Wi-Fi device authentication framework, which covers the authentication process and the fingerprint database updating method in both access and association phase.

This paper is organized as follows: Sect. 2 gives an overview of the authentication framework. Section 3 provides an authentication method based on CSI; Sect. 4 gives a detailed description of our fingerprint database updating method; In Sect. 5, we introduce the enhancing Wi-Fi device authentication protocol. Section 6 gives the evaluation. Section 7 concludes the paper.

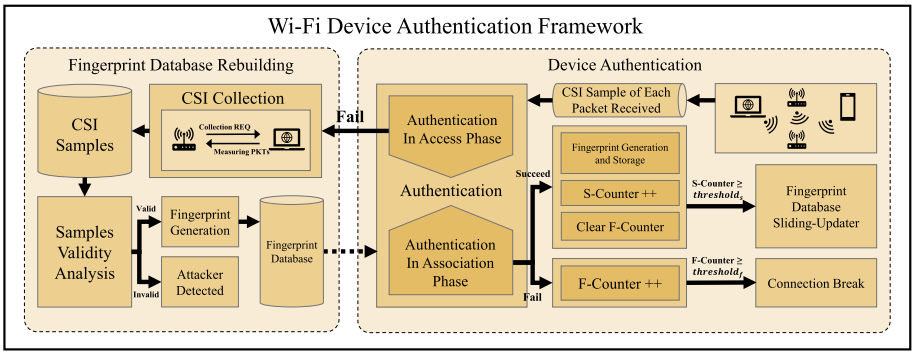


Fig. 1. The framework of our Wi-Fi device authentication system

2 Framework Overview

We design a Wi-Fi device authentication framework to provide device authentication service in both access phase and association phase, as shown in Fig. 1. The framework is mainly implemented on the Wi-Fi Access Point (AP). Some working steps that require signaling interaction between the AP and the working station (STA) can be completed by installing our authentication protocol on the both devices.

It can be seen in Fig. 1 that the Wi-Fi device authentication framework is mainly composed of two parts, including the device authentication and the fingerprint database rebuilding. But according to the logical function, the framework should be divided into two parts including device authentication and fingerprint database update. The device authentication mainly completes two tasks. The first task is to verify the identity of the STA in access phase and decide whether to allow access. The second task is to check the identity of data frames sent by the STA during the association phase. The third task is to extract fingerprints from the received data packets and use them to update the fingerprint database. The fingerprint database update is mainly responsible for the rebuilding and the sliding-updating of the fingerprint database.

We describe the whole authentication framework by simulating the device authentication process in two application scenarios, including the access phase and the association phase.

2.1 Authentication in Access Phase

According to the access process of the 802.11 device, the STA needs to send an authentication request to the AP. The AP first extracts CSI sample from the request frame, and then sends it to the authentication module. At the same time, the fingerprints belonging to this STA in the fingerprint database will be sent to the authentication module (shown with the dotted line), and the module will check if the CSI sample is an outlier in the fingerprints based on LOF. If the sample is not an outlier, it means that the access request is indeed from the STA, and the AP accepts the access request and informs the STA that the authentication is successful. If the sample is checked to be an outlier, the AP will return an authentication failure signal to the STA to deny access. The AP will start to rebuild the fingerprint database after detecting the authentication failure event in access phase. Firstly, the AP sends a collection request named Collection REQ to the STA. The STA then returns the Measuring PKTs, which are used to measure the CSI. After the AP collects enough CSI samples, it sends them to the samples validity analysis module to detect whether the CSI samples really comes from the STA. If the sample set is valid, it used to generate fingerprints and rebuild the fingerprint database. Otherwise, the fingerprint database will not be changed.

2.2 Authentication in Association Phase

For each data packet from the STA, the AP extracts the CSI and sends it to the authentication module. The authentication process of the module is the same as the authentication in access phase, but some follow-up processing should be finished according to different authenticating results. It can be seen from Fig. 1 that after successful authentication, the AP uses the CSI samples to generate a new fingerprint and store it in a buffer. The AP maintains a counter called S-Counter to record the number of data packets that have been successfully authenticated since the last update of the fingerprint database. If the value is greater than or equal to the $threshold_s$, it will update the fingerprint database with the fingerprints in the buffer. We provide a fingerprint database sliding-updater to maintain the database. Meanwhile, The AP also maintains a counter called F-Counter. It records the number of the frames that continuously fail the authentication. When the authentication fails, the F-Counter is updated, and the AP determines whether the connection should continue according to whether the $threshold_f$ is reached.

3 Authentication Leveraging CSI Fingerprint

In this section, we focus on the device authentication based on CSI fingerprint. We first explain the basic idea of how to do authentication using CSI fingerprint, and then we describe the algorithm of device authentication.

3.1 Basic Idea

CSI includes the amplitude and phase of all sub-carriers used to transmit data. These values will vary with factors such as channel fading and the multipath effect. We know that the channel between two Wi-Fi devices are unique, which means that the CSI measured by the two devices is also unique. In the light of this idea, the AP can uniquely mark the device by extracting and recording the CSI of the STA. Figure 2 shows the amplitude image of the CSI obtained from three devices placed in different positions. We can see that the CSI images of the same device are concentrated, while the CSI images between different devices are very different.

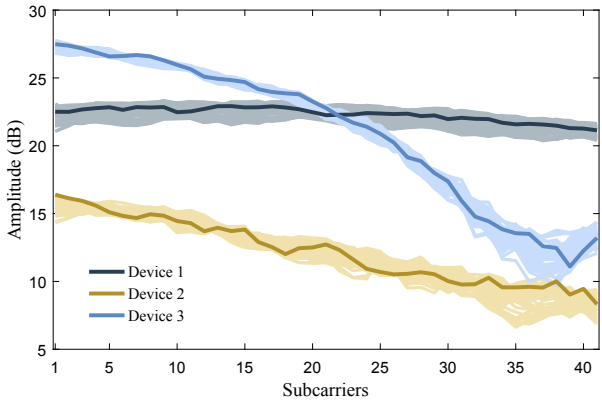


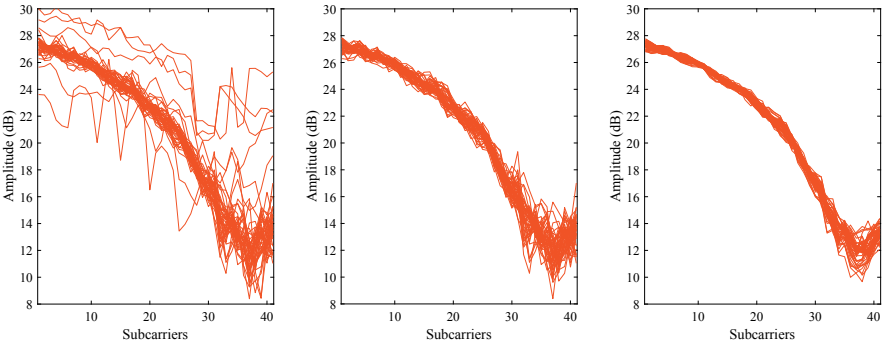
Fig. 2. CSI samples of three devices placed in different locations

In the realistic authentication work, we need to match an unknown CSI sample with the local fingerprint set, and determine the result of the authentication based on the matching result. Inspired by the feature of the CSI images in Fig. 2, we consider using the Local Outlier Factor (LOF) algorithm to do CSI matching. We use the samples in the local fingerprint set as the reference sample group, and calculate the LOF of the unknown sample in the reference sample group to determine whether it is an outlier, thereby obtaining the matching result.

We found in the test that there are often values that far exceed the expected numerical fluctuation range, as shown in Fig. 3(a). They do not contain any information of device identity and will reduce the accuracy of system. Therefore, we use the Hampel Identifier to exclude these outliers. In addition, the CSI samples of the same device will change under noise interference. Even though the CSI images of the same device still have the same trend, but the dispersion increases. The local outlier factor describes the difference between samples based on the Euclidean distance. It means the noise will cause the reference sample group become discrete and reduce the probability of abnormal CSI being detected. Therefore, we smooth the CSI samples in the time domain.

3.2 Algorithm Description

Fingerprint Generation. The Fingerprint generation algorithm consists of two stages, including the outlier elimination and the smoothing.



(a) Before processing (b) After removing outliers (c) After smoothing

Fig. 3. CSI samples in different processing stage

Outlier Elimination. We perform outlier detection on each subcarrier individually. Let the k-th CSI sample from device D be $C_D^k = \{C_{D,1}^k, ..., C_{D,N}^k\}(k = 1, ..., K)$, where N is the number of subcarrier and K is the number of samples obtained from device D. We arrange the amplitude samples of n-th subcarrier in chronological order, which can be presented as $L_{D,n} = (C_{D,n}^1, ..., C_{D,n}^K)$. We select the median of the window composed of $C_{D,n}^I$ and its $2l$ surrounding samples. We use the absolute deviation of each sample to estimate the standard deviation of the samples in the window. The standard deviation is shown as follows:

$$\sigma_{D,n}^I = \frac{1}{\gamma} median\left(\mid C_{D,n}^i - C_{D,n}^I \mid\right), \tag{1}$$

where $C_{D,n}^I$ indicates the median of the window , $C_{D,n}^i$ is the sample in the window. We use $\gamma = \sqrt{2}erfinv(0.5)$, where $erfinv$ on behalf of the inverse error function.

We then perfrom the following numerical substitution on each amplitude sample to exclude the outlier:

$$C_{D,n}^i = \begin{cases} C_{D,n}^i & \mid C_{D,n}^i - C_{D,n}^I \mid \leq \eta\sigma_{D,n}^I \\ C_{D,n}^I & \mid C_{D,n}^i - C_{D,n}^I \mid > \eta\sigma_{D,n}^I, \end{cases} \tag{2}$$

where η is a threshold used to judge whether the sample is outlier.

We repeat the above work on each subcarrier. Figure 3(b) shows the CSI amplitude images after removing the outliers.

Smoothing. We smooth the amplitude of each sub-carrier in the time domain to reduce this effect. The smoothing process is described as follows:

$$\widetilde{C}_{D,n}^{k} = \frac{1}{w} \sum_{max(0,k-\lfloor \frac{w}{2} \rfloor)}^{min(K,k+\lfloor \frac{w-1}{2} \rfloor)} C_{D,n}^{k}, \tag{3}$$

where w indicates the length of smoothing window. Figure 3(c) shows the CSI amplitude images after smoothing.

Fingerprint Matching. In the sample space S_D composed of the local fingerprints of Device D and the new sample with $D's$ identity, we define the distance between the k-th and the r-th sample as:

$$d_{k,r} = \left(\sum_{n=1}^{N} \left(C_{D,n}^{k} - C_{D,n}^{r} \right)^2 \right)^{\frac{1}{2}}. \tag{4}$$

We define $d_p(k)$ as the distance between the k-th sample and the p-th farthest sample. Also, we define the p-distance neighborhood of the k-th sample as the set of samples whose distance from it is less than or equal to $d_p(k)$, and denote it by $N_p(k)$. In addition, we define the p-reachable distance from the k-th and the r-th sample as:

$$rech_p(k,r) = max(d_p(r), d_{k,r}). \tag{5}$$

Therefore, the local reachable density of the k-th sample can be expressed as:

$$lrd_p(k) = \frac{\mid N_p(k) \mid}{\sum_{r \in N_p(k)} rech_p(k,r)}. \tag{6}$$

Finally, we get the local outlier factor of the k-th sample:

$$LOF_p(k) = \frac{\sum_{r \in N_p(k)} lrd_p(r)}{\mid N_p(k) \mid \cdot lrd_p(k)}. \tag{7}$$

The Fig. 1 tells us that if the k-th sample does not belong to device D, then it will be far away from the surrounding samples, and the local reachable density of it should be small. On the contrary, if the samples around the k-th sample are clustered together, the local reachability density of them will be very large. It is reflected on the LOF that if the k-th sample belongs to device D, the LOF of it is approximately 1; if it does not belong to device D, the LOF is a larger value. Thus, We do the following judgement to verify the identity:

$$\begin{cases} LOF_p(u) \leq mean\left(LOF_p(f)\right) + 10 * std\left(LOF_p(f)\right) & success; \\ LOF_p(u) > mean\left(LOF_p(f)\right) + 10 * std\left(LOF_p(f)\right) & failure, \end{cases} \tag{8}$$

where u indicates the new CSI sample with D's identity, f represents D's fingerprint in local database, $mean\left(LOF_p(f)\right)$ indicates the mean of $LOF_p(f)$ and $std\left(LOF_p(f)\right)$ indicates the standard deviation.

The Fig. 4 shows the LOF obtained from two different devices. We use 44 CSI samples obtained from a device to generate a fingerprint database, and collected 44 CSI samples of this device and another device at an adjacent time. Blue bar represents the LOF of the fingerprints in the library, red bar represents the LOF of the samples collected from the same device, and yellow bar is the LOF of the CSI samples from another device. The blue dashed line shows the threshold, and it can be seen that only 1 sample was wrongly judged.

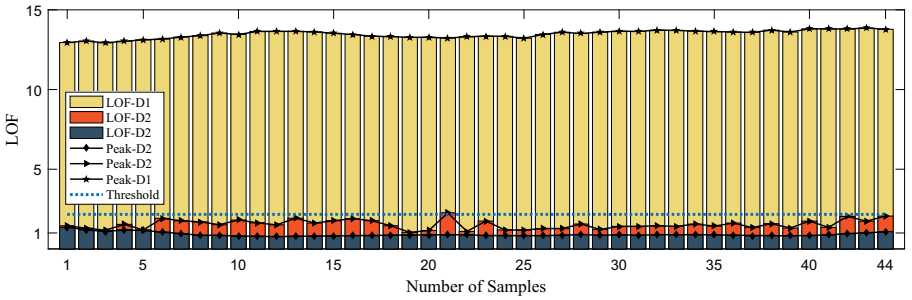


Fig. 4. The LOF of the samples collected from two devices

4 CSI Fingerprint Update

In this section, we will focus on the method of the fingerprint database update. Fingerprint database update is important because if the fingerprints in the database become outmoded, any access request sent from STA will be refused because the CSI of the STA is different with the fingerprints in AP's database. The updating method of fingerprint database presented in this paper can improve this problem without compromising the safety of the system. We will describe this method from two application scenarios.

4.1 CSI Fingerprint Update in Access Phase

In the initial state, the STA is not connected. At this time, the fingerprints of the STA stored in the AP may or may not be able to match with the current CSI. If the matching succeeds, the access work can be finished without maintaining the fingerprint database. Therefore, we will only discuss the updating method in the case of matching fails.

We discuss the algorithm in two situations: 1) the STA requests access; and 2) the attacker requests access.

The STA Requests Access. When the STA requests access, the AP uses an invalid fingerprint for authentication, which causes the authentication to fail. The AP then sends the CSI collection request, and the STA sends CSI measurement packets after receiving the request. If there is no attacker or the attacker does

not do any response, the master device collects a true and effective CSI sample set. It then uses the sample set to generate fingerprints and overwrite the original data in the fingerprint database. If the attacker exists and sends measurement frames at the same time, the CSI sample set collected by the AP will contain two distinct group of samples. We use the mean of samples as the center, Fig. 2 shows that when the samples come from one device, all the samples are concentrated in the narrow band at the center. When the samples come from two different devices, it can be expected that most of the samples are far away from the center. We use the standard deviation of samples to quantify this dispersion:

$$\sigma = \left[\frac{1}{K} \sum_{k=1}^{K} \left(C_D^k - C_D \right)^2 \right]^{\frac{1}{2}}, \tag{9}$$

where C_D is the mean of all samples.

We set a threshold for estimate. If the standard deviation exceeds the threshold, the sample set is judged to be invalid and the fingerprint database will not be maintained. Regardless of whether the fingerprint database is successfully maintained, the child device will continue to request access. If the update is successful, the STA can be successfully accessed in the next request. Otherwise, the STA must wait until the attacker stops attacking before it can successfully access.

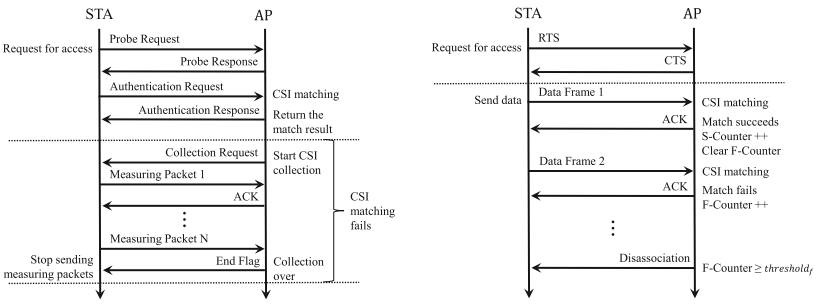
The Attacker Requests Access. When an attacker requests access, authentication will fail and CSI collection will start. In our working environment, the STA being impersonated will also receive the measurement request and send the measuring packets to the AP. Similarly, we consider two possibilities. If the attacker does not send measuring packets, the AP will update the fingerprint database with the CSI of the real device, and the attacker still cannot be accessed. If the attacker sends measuring packets, it cannot pass the sample validity check, and thus cannot construct a false fingerprint database in the AP.

4.2 CSI Fingerprint Update in Association Phase

We assume that the STA has been successfully connected and starts to transmit data. The successful access of the STA means that the fingerprints in the AP is valid, which means that we can successfully authenticate the data sent by the STA. The key for updating the fingerprint database in association phase is that we will store the CSI samples of data packets and use them to generate a new fingerprint set to update the fingerprint database (as described in Sect. 2). We propose a simple fingerprint database sliding-updater, which uses the new fingerprints to replace the $threshold_f$ earliest generated fingerprints in the database (just like a sliding-window). Through the updater, we ensure that the fingerprints in database and the CSI samples obtained from packets received recently are always highly correlated.

However, the real-time update of the fingerprint database is based on the active communication between the AP and the STA. When the STA is in sleeping mode, keeping the CSI collection will cause greater power consumption and increase the network burden, so this is not recommended. After a device returns to be active, the fingerprints stored in the authenticator may become invalid. In order to reestablish the fingerprint database, we disconnect after $threshold_f$ consecutive data packets fail the authentication (see Sect. 2), at this time the update of the fingerprint database will return to the first situation.

In addition, we must also consider the existence of the attacker. When an attacker uses a forged identity to send a data packet, the AP will get the failed authentication result and discard the packet. If the AP continuously receives $threshold_f$ packets from the attacker, the connection is broken. We can find that the attacker cannot attack the AP effectively during this whole process.



(a) Access phase (b) Association phase

Fig. 5. The procedure of CSI-based authentication protocol

5 The CSI-based Authentication Protocol

It can be seen from the previous section that the association and cooperation between the AP and the STA are the key to do device authentication and fingerprint database update in both the access and the association phase. Therefore, we present an enhancing Wi-Fi device authentication protocol in this section, which is designed based on the existing Wi-Fi association process.

5.1 The Authentication Procedure in Access Phase

This subsection shows the authentication procedure in access phase. As shown in Fig. 5(a), the process includes an authentication stage and a CSI collection stage, where the CSI collection stage is triggered only when the identity authentication fails. The steps are shown as follows:

- STA sends Probe Request to request access to the network. AP responds with Probe Response after listening to the request, indicating that it can provide access service and is ready for authentication.

- STA then sends Authentication Request for the authentication. AP extracts CSI from the control frame and performs CSI matching. Then AP returns Authentication Response to inform STA of the authentication result.
- If the matching is successful, the access authentication ends. If the match fails, AP sends Collection Request to STA, requesting to start CSI collection.
- After receiving the request, STA starts to send Measuring Packets with a fixed data length of 24 bytes. After receiving the data packets, AP responds with ACK to tell STA to continue or stop.

5.2 The Continuous Authentication in Association Phase

Figure 5(b) shows the continuous authentication in association phase. In Wi-Fi association, CSMA/CA is used to avoid the collisions among packets. The STA exchanges RTS/CTS with the AP before starting to transmit data to inform other devices to remain silent. After exchanging RTS/CTS, the AP performs CSI matching on each received data frame, and judges whether the current connection is valid according to the matching situation, and decides whether to continue association or not (as shown in Sect. 2).

- STA sends RTS to tell AP that it is going to send data. AP responds with CTS after receiving the request, indicating that it is ready receiving and clearing the channel.
- STA starts to send Data Frames. When AP receives a Data Frame, it responds with ACK. AP extracts the CSI of the frame and performs CSI matching. If the match is successful, the S-Counter is increased by 1, and the F-Counter is cleared. If the match fails, the F-Counter is increased by 1.
- If F-Counter reaches $threshold_f$, AP sends Disassociation to STA to disconnect.

6 Performance Evaluation

In this section, we evaluate the performance of two parts of our authentication framework. The first part is the authentication algorithm based on LOF. The CSI samples used in this process is obtained within a short time interval. The second part is the fingerprint database sliding-updater. To evaluate the performance of our sliding-updater, we simulate the long-term working scenario by collecting CSI within a long time interval.

In our experiments, the STAs were fixedly placed in different locations in the laboratory. They transmitted frames at a rate of 100 pkt/sec in a 20 MHz wireless channel. The AP was also placed in a fixed location and listened to the frames sent by STAs. Since the AP will received irrelevant frames from other unknown Wi-Fi devices, we set the MAC of each STA and filter the frames by MAC checking. For each valid frame received, the AP got CSI information from it and saved.

To evaluate the performance of the fingerprint database sliding-updater, we first used a fixed fingerprint database to do authentication. Then we updated the fingerprint database during authentication to see the improvement of performance.

We use three metrics: false rejection rate (FRR), false acceptance rate (FAR) and accuracy rate (ACC) to quantify the performance of the system. FRR is the probability of matching failure for samples from legal device. FAR is the probability of successful matching for samples from attackers. ACC is equal to the proportion of correctly matching samples in the total sample set. We use the samples collected in the same time on the same device. After successively authenticating 100 samples, we obtain the authentication accuracy of the 100 samples as the accuracy of the current system.

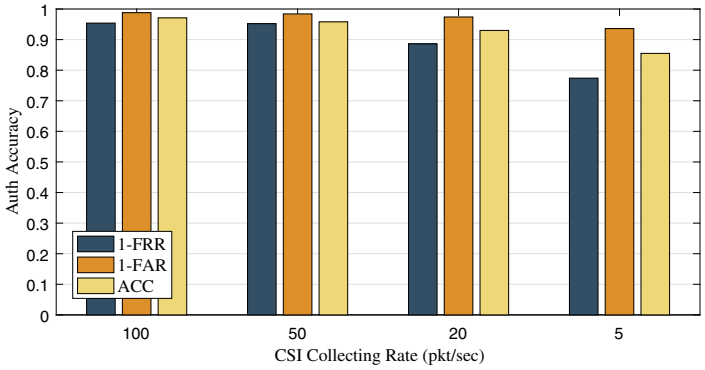


Fig. 6. The value of each metrics with different CSI collecting rate

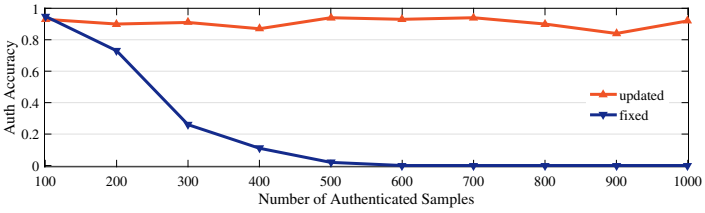


Fig. 7. The accuracy of the authentication systerm tested with updated and fixed fingerprint database

In the experiments, we got more than 96,000 CSI samples using four devices (ETTUS USRP B210) in our laboratory. In the first phase, we evaluated our authentication algorithm based on LOF. We got the three metrics in four different packet sending rates. We set the size of the local fingerprint database to 100, and did authentication on more than 1,000 CSI samples. The Fig. 6 shows the test results. To observe the results more clearly, we use $1 - FRR$ and $1 - FAR$ to represent the test results. The results show that when the data packet rate is at its maximum, the three indicators all reach their maximum values, with the maximum values being 95.4%, 98.8% and 97.1%. It can be seen from it that when the data packet rate decreases, FRR and FAR increase accordingly. The accuracy of authentication also decreases, but it remains above 85%. This is because

when the packet rate decreases, the time difference between each CSI sample increases, so the correlation between samples will decrease. In particularly, we can see that FRR is growing faster than FAR in the Fig. 6.

In the second stage, we evaluated the performance of the fingerprint database sliding-updater. The two sets of data shown in the Fig. 7 are the accuracy of system with updating the database and not updating. We can see that when the system uses the sliding-updater to continuously update the fingerprint database during the test, the accuracy of the system is maintained above 80%, and the highest accuracy is 94%. When the fingerprint database is fixed, the accuracy of the system decreases rapidly during the authentication, and it is almost 0 after authenticating the 600th CSI sample.

We obtained good results in both experiments. However, the high accuracy of the system may be due to the over-fitting of the data and the stability of the test environment considering that our experiment has limited data and single test environment.

7 Conclusion

In this paper, we propose an enhancing Wi-Fi device authentication protocol. We also give a complete Wi-Fi device authentication framework. The framework mainly contains two parts, including the device authentication and the fingerprint database update. Our protocol works on two application scenarios, including the authentication in access phase and the authentication in association phase. We provide different fingerprint database updating method and authentication processes in two scenarios. In the first scenario, we reestablish the fingerprint database after authenticating fails with new CSI samples. We use the standard deviation of the new CSI sample set to decide whether there is an attacker. In the second scenario, we use the database sliding-updater to update the fingerprints. We also provide a fingerprint generating method and an authentication method based on LOF. The evaluation shows that our authentication method has a good performance as well as the sliding-updater.

Acknowledgment. This work is supported by Frontiers Science Center for Mobile Information Communication and Security, Southeast University, Nanjing, China. This work is also supported by Zhishan Youth Scholar Program Of SEU, Nanjing, China.

References

1. Alshudukhi, J.S., Mohammed, B.A., Al-Mekhlafi, Z.G.: An efficient conditional privacy-preserving authentication scheme for the prevention of side-channel attacks in vehicular ad hoc networks. IEEE Access **8**, 226624–226636 (2020). https://doi.org/10.1109/ACCESS.2020.3045940
2. Chatterjee, U., Sadhukhan, R., Mukhopadhyay, D., Subhra Chakraborty, R., Mahata, D., M.Prabhu, M.: Stupify: A hardware countermeasure of kracks in wpa2 using physically unclonable functions. In: Companion Proceedings of the Web Conference 2020, WWW 2020, pp. 217–221. Association for Computing Machinery, New York (2020). https://doi.org/10.1145/3366424.3383545

3. Elhigazi, A., Razak, S.A., Hamdan, M., Mohammed, B., Abaker, I., Elsafi, A.: Authentication flooding dos attack detection and prevention in 802.11. In: 2020 IEEE Student Conference on Research and Development (SCOReD), pp. 325–329, September 2020. https://doi.org/10.1109/SCOReD50371.2020.9250990
4. Liao, R., Wen, H., Pan, F., Song, H., Xu, A., Jiang, Y.: A novel physical layer authentication method with convolutional neural network. In: 2019 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), pp. 231–235, March 2019. https://doi.org/10.1109/ICAICA.2019.8873460
5. Liu, H., Wang, Y., Liu, J., Yang, J., Chen, Y.: Practical user authentication leveraging channel state information (csi). In: Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security, ASIA CCS 2014, pp. 389–400. Association for Computing Machinery, New York (2014). https://doi.org/10.1145/2590296.2590321
6. Liu, M., Mukherjee, A., Zhang, Z., Liu, X.: Tbas: Enhancing wi-fi authentication by actively eliciting channel state information. In: 2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), pp. 1–9, June 2016. https://doi.org/10.1109/SAHCN.2016.7733021
7. Liu, S.: Mac spoofing attack detection based on physical layer characteristics in wireless networks. In: 2019 IEEE International Conference on Computational Electromagnetics (ICCEM), pp. 1–3, March 2019. https://doi.org/10.1109/COMPEM.2019.8779180
8. Madani, P., Vlajic, N., Sadeghpour, S.: Mac-layer spoofing detection and prevention in iot systems: Randomized moving target approach. In: Proceedings of the 2020 Joint Workshop on CPS&IoT Security and Privacy, CPSIOTSEC 2020, pp. 71–80. Association for Computing Machinery, New York (2020). https://doi.org/10.1145/3411498.3419968
9. Rocamora, J.M., Ho, I.W.H., Mak, M.W.: Fingerprint quality classification for csi-based indoor positioning systems. In: Proceedings of the ACM MobiHoc Workshop on Pervasive Systems in the IoT Era, PERSIST-IoT 2019, pp. 31–36. Association for Computing Machinery, New York (2019). https://doi.org/10.1145/3331052.3332475
10. St. Germain, K., Kragh, F.: Multi-transmitter physical layer authentication using channel state information and deep learning. In: 2020 14th International Conference on Signal Processing and Communication Systems (ICSPCS), pp. 1–8, December 2020. https://doi.org/10.1109/ICSPCS50536.2020.9310034
11. St. Germain, K., Kragh, F.: Physical-layer authentication using channel state information and machine learning. In: 2020 14th International Conference on Signal Processing and Communication Systems (ICSPCS), pp. 1–8, December 2020. https://doi.org/10.1109/ICSPCS50536.2020.9310070
12. Troya, A.S., Astudillo, J.J., Romero, C.G., Sáenz, F.G., Díaz, J.: Vulnerability detection in 802.11i wireless networks through link layer analysis. In: 2014 IEEE Latin-America Conference on Communications (LATINCOM), pp. 1–6, November 2014. https://doi.org/10.1109/LATINCOM.2014.7041875
13. Wang, Q., Li, H., Zhao, D., Chen, Z., Ye, S., Cai, J.: Deep neural networks for csi-based authentication. IEEE Access **7**, 123026–123034 (2019). https://doi.org/10.1109/ACCESS.2019.2938533
14. Yan, C., Ge, J.: Synchronous control of master-slave manipulator system under deception attacks. In: 2020 Chinese Control And Decision Conference (CCDC), pp. 1778–1782 August 2020. https://doi.org/10.1109/CCDC49329.2020.9164635