Cross-layer Authentication Mechanism Model Combined with 5G Converged Channel Fingerprint

Wei Ao, Jian Wei, Yindong Li, Xiaolong Zhang,
Bin Yu and Kaiwen Hou*

Digital Research Branch of Inner Mongolia Power (Group) Co., Ltd, Hohhot, Inner Mongolia, China
E-mail: impcsyy_ao@163.com; wj272643132@icloud.com; impcsyy_lyd@163.com; 18847128476@163.com; joey8023@gmail.com; 15352845003@163.com
**Corresponding Author*

Received 14 August 2024; Accepted 23 October 2024

Abstract

In the actual communication environment, once the attacker successfully steals the legitimate channel information, the key information can be cracked according to the authentication response, so there is a security risk of key leakage. This paper combines the physical layer channel characteristics with the shared key, and combines it into a joint key to design a challenge-response physical layer authentication mechanism based on interpolation polynomial. Then, this method is applied to the EAP-AKA' authentication protocol of 5G network, and a cross-layer authentication mechanism for 5G converged channel fingerprint is proposed. Finally, using the captured high-level authentication challenge response data, a simulation environment is built in MATLAB and the feasibility and security of the scheme are verified. The experimental results show that the authentication mechanism has better

Journal of ICT Standardization, Vol. 12_3, 311–336.
doi: 10.13052/jicts2245-800X.1234

authentication performance and security performance. Compared with the traditional high-level authentication mechanism, it has certain advantages in computing overhead and can meet the 5G application scenarios of large-scale IoT terminals. Moreover, it combines physical layer authentication with high-level authentication, realizes mutual complementarity and mutual enhancement, and enhances the security performance of authentication.

Keywords: 5G, channel fingerprint, cross-layer, authentication mechanism.

1 Introduction

Wireless communication is accessed and transmitted in open space through electromagnetic waves. Compared with the wired connection of fixed access points, it is more vulnerable to illegal attacks by third parties, such as illegal eavesdropping, monitoring, information tampering, counterfeiting, replay and denial of service. The increase in the number of wireless communication terminals has brought about the transmission of a large amount of sensitive data, and daily items may also become the source of information security risks, leading to information leakage. Therefore, the security of wireless communication is facing severe challenges.

The important content of wireless communication security is wireless access security, and identity authentication is the primary task of wireless access security. Traditional wireless communication access authentication scheme has been widely used in existing communication systems, and it is usually carried out above the physical layer, and it uses IP address, MAC address [1], preset key, password and security certificate as the identity information of users. Even if the setting is complicated, there is a great risk of being copied and counterfeited, and the security of the whole system will be lost at this time. In addition, traditional access authentication schemes rely on complex cryptographic calculations, which consume a lot of computing resources and storage resources [2]. Complex operations are difficult to complete in a short time, which is easy to cause communication delay, and cannot meet the low delay requirements of future wireless communications. Therefore, there is an urgent need for an effective, low-latency and lightweight security scheme to guarantee the security of wireless communication.

Physical layer security technology is considered to be one of the most promising wireless access security enhancement schemes, especially radio frequency fingerprinting technology (RFF), also called specific emitter identification (SEI). Different from traditional security schemes based on complex

computation, RF fingerprinting is a scheme to study the inherent characteristics of the physical layer. RF fingerprint technology processes and analyzes the received signals, extracts the hardware characteristics reflected by these tiny distortions, thus forming RF fingerprints, identifying devices and realizing identity authentication. Meanwhile, radio frequency fingerprint technology has no additional computational burden on the device, and the main computation can be completed by the central device or remote server. It is a highly anticipated lightweight security solution.

This article attempts to find a breakthrough from the perspective of the physical layer, utilizing the inherent security elements in the wireless channel of the physical layer to authenticate communication entities. Due to the inability of third parties to obtain complete channel information, physical layer authentication can achieve a certain degree of information theory security. Moreover, compared to complex encryption and decryption operations, physical layer authentication operations are simpler. In addition, physical layer authentication technology also has high protocol architecture compatibility, which can be combined with high-level authentication to achieve a cross layer authentication mechanism of dual identity authentication, enabling high-level and physical layer to complement and enhance each other, and has significant research significance and application value.

The article proposes to combine physical layer authentication with EAP-AKA' authentication in 5G protocol, integrate wireless channel fingerprints into high-level authentication mechanism, and design a cross layer authentication mechanism for 5G fusion channel fingerprints. Firstly, the authentication response generated by the higher layer is used as the authentication credential, combined with the wireless channel characteristics to form a joint key. Based on the interpolation polynomial method, a curve equation is constructed, and the random number vector in the non joint key is substituted into the equation to generate a verification vector and form the authentication response, completing cross layer authentication. The proposed cross layer authentication mechanism utilizes channel characteristics to provide information entropy for high-level authentication. At the same time, this authentication mechanism utilizes channel characteristics to generate keys and encrypt authentication information, solving the problem of attackers using stolen authentication data to carry out forgery attacks and thereby pry into user privacy, enhancing the security performance of the authentication system.

This paper combines the physical layer channel characteristics with the shared key, and combines it into a joint key to design a challenge-response

physical layer authentication mechanism based on interpolation polynomial. Then, this method is applied to the EAP-AKA' authentication protocol of 5G network, and a cross-layer authentication mechanism for 5G converged channel fingerprint is proposed. Finally, using the captured high-level authentication challenge response data, a simulation environment is built in MATLAB and the feasibility and security of the scheme are verified.

The first part of this article is the introduction, which summarizes the research status and necessity of improving the cross layer authentication mechanism of 5G fusion channel fingerprint. The second part is the related work, which summarizes the existing research, analyzes the problems, and compares them with the research content of this article. The third part is the algorithm model part, which proposes the cross layer authentication mechanism system model of this article. The fourth part is the experimental part, which uses the QuaDRiGa simulation model to build a simulation environment on the MATLAB software platform to analyze the performance of this model. The fifth part is the conclusion part, which summarizes the research content of this article and analyzes the subsequent research.

2 Related Works

Unlike radio frequency fingerprint recognition technology that targets device characteristics, channel based authentication schemes verify the identity of unknown transmitters by observing the unique temporal and spatial features of Channel State Information (CSI). Reference [3] proposed a method based on channel frequency response and hypothesis testing to determine whether current and previous communications were conducted by the same sender. This algorithm combines channel detection with hypothesis testing to determine whether current and previous communications were conducted by the same user. Legitimate users can receive reliable authentication, while malicious users can be detected by reliable authentication. The author used the WiSEray tracing tool to simulate the spatial variation channel response in a real environment and analyzed the ability of the receiver to distinguish the transmitter based on its channel frequency response in a given communication environment [4]. By measuring 5 frequency response samples on a 100MHz bandwidth and using a transmission power of 100 mW, legitimate users can authenticate with 99% confidence, while malicious users with a confidence level of over 95% can be excluded. Reference [5] further proposes how to utilize the spatial variability of wireless channel response in a rich scattering environment to detect whether the current and

previous communication connections are made by the same transmitting terminal.

Reference [6] combines traditional message authentication mechanisms with physical layer authentication mechanisms, utilizing the temporal and spatial uniqueness of physical layer channel responses to achieve fast authentication while minimizing packet transmission overhead.

Reference [7] proposes an authentication scheme based on hypothesis testing, which is suitable for multiple input multiple output (MIMO) systems and OFDM modulated correlated fading multi eavesdropped channels. By allowing a certain degree of correlation between channels, the optimal attack strategy for single and multiple repeated attempts is provided.

In a rich scattering channel environment, channel impulse response can characterize the spatial geographic location information of wireless terminal devices. Although multi-path scattering clusters are independent of each other, they have high correlation over time. Therefore, the channel impulse response of multipath fading channels characterizes the spatiotemporal information related to the signal propagation environment. Reference [8] proposes a decision authentication mechanism based on the temporal correlation of channel impulse response, and derives the authentication threshold based on the probability distribution of the change in channel impulse response before and after time slots. However, this authentication scheme depends on the mobility of wireless terminals, noise, and the presence of channel estimation errors. In high latency and multipath fading channel environments, the performance of such authentication schemes will be greatly limited. Reference [9] combines the multipath delay characteristics of wireless channels with physical layer authentication based on channel impulse response to develop a two-dimensional quantization authentication scheme, which to some extent alleviates the impact of mobile terminal noise and channel estimation errors.

For static time invariant channel environments, reference [10] proposes a physical layer authentication scheme based on channel frequency response. Its basic principle is to use the spatial differences of signal propagation based on binary hypothesis testing theory to detect whether a communication network is attacked by a third eavesdropper. Reference [11] is based on the joint probability of the channel state information of the Alice Bob link and the Eve Bob link, and uses the difference in channel state information between two adjacent data frames to determine whether the channel state information of the current time slot is the same as that of the first legitimate transmitter. This method distinguishes between legitimate senders and eavesdroppers

at the cost of high false alarm rates, which can effectively resist channel estimation errors, but is not sufficient to resist simulated attacks on channel state information. Reference [12] proposed a physical layer authentication algorithm based on normalized likelihood ratio test statistic in frequency selective Rayleigh fading channel environment. Compared to wired communication networks, the channel changes rapidly and dynamically during wireless communication, and is more random. Accurately predicting channel information is a challenge. Reference [13] focuses on fast time-varying wireless channel propagation environments and uses time-varying carrier frequency offset based on binary hypothesis testing to achieve physical layer identity authentication. This scheme estimates the carrier frequency offset value of the previous time slot from the received signal at the receiving end, and then uses Kalman algorithm to predict the carrier frequency offset value of the current time slot. By establishing a test statistic for the predicted and estimated carrier frequency offset values, a decision can be made to determine whether the transmitted data information is sent by the legitimate sender. Experimental results show that this authentication algorithm can be well applied to multipath. Go into the environment. Reference [14] extends the physical layer authentication technique based on channel frequency response to Multiple Input Multiple Output (MIMO) systems

In the method of obtaining the RF fingerprint of wireless radio equipment, feature extraction can also be based on the steady-state response signal of the wireless device baseband obtained. From the perspective of research hotspots, the extracted steady-state response characteristics of RF equipment mainly include: carrier frequency offset value, SYNC synchronization signal correlation value, baseband I/Q two-way signal delay value, receiving end signal amplitude error and phase error, etc. Reference [15] estimated the frequency and phase deviation characteristics of the received signals in USRP2 and Zigbee devices under the IEEE802.15.4 standard to simulate the detection of attacks from unauthorized parties. Reference [16] extracted five unique features of the transmission state modulation signal, including "frequency error, synchronization correlation value (SYNC correlation), carrier feedthrough amplitude offset (I/Q offset), amplitude error, and phase error", for RF fingerprint recognition. The device was placed in different positions and IEEE802.11b data frames were captured using a vector signal analyzer for experiments. It was found that the extracted RF fingerprint did not change with different positions, which also indicates that the feature differences caused by defects in the RF device itself can be used as RF fingerprints.

Reference [17] tested the feasibility of a physical layer authentication scheme based on radio frequency fingerprints through simulated attacks and found that attackers only need to regenerate a signal after a certain period of attack training to obtain radio frequency fingerprint features, without the need for additional legitimate radio frequency devices to simulate third-party attacks. Therefore, physical layer authentication based on radio frequency fingerprints has lower security in simulated attack models. On the other hand, for RF fingerprint authentication, due to the very small differences in signals, physical layer authentication based on RF fingerprints requires extremely precise spectrum analyzers, high-speed samplers, large fingerprint databases, complex recursive algorithms, and low error probability density estimators to achieve. Meanwhile, the physical layer authentication scheme based on radio frequency fingerprints is greatly affected by environmental changes, resulting in poor recognition rates in dynamic propagation environments. To achieve more robust performance, it is necessary to extract radio frequency fingerprints in a relatively slow changing channel environment, which is also a limitation of the physical layer authentication technology based on radio frequency fingerprints [18].

Reference [19] proposed a new method for clustering channel estimates of different transmitters based on Gaussian mixture models. In the MC-MTC system based on physical layer security, the integrity and authenticity of information exchange between communication devices over the air are ensured.

Overall, although existing research schemes have shown good performance in physical layer identity authentication, most of the related studies on the extraction and recognition of RF fingerprint features are based on devices in fixed positions. In this case, the impact of time-varying channels on the RF fingerprint characteristics of the device is not significant. However, when the device is in a mobile state and the communication environment is constantly changing, the RF fingerprint will be more affected by the channel, thereby affecting the authentication performance; Although channel fingerprinting can effectively solve the problems encountered by RF fingerprinting, there is still an unresolved issue of channel fingerprinting stability. Therefore, the research objective of this article is to propose an access authentication method that can fuse RF fingerprint features and channel fingerprint features, and has adaptive capabilities for time-varying environments, in order to fill the gap in related research and better solve the security access authentication problem of RF fingerprint and channel fingerprint.

3 Model Algorithm

With the development of mobile communication systems, the security performance of communication mechanisms is constantly improving, but they are all implemented at higher logical layers of communication networks, and communication data is transmitted through wireless channels. The open nature of wireless channels makes them vulnerable to attacks. Although 5G has greatly enhanced security compared to 4G, there are still some security risks. Attackers can obtain some information about the key by stealing authentication responses. As the number of authentication attempts increases, the key entropy will continue to decrease. If the attacker obtains enough authentication data, it will threaten the security of the key. Therefore, this article analyzes the problem based on the actual situation and proposes reliable improvement strategies.

3.1 Problem Analysis

There are still security vulnerabilities in the 5G protocol. Malicious attackers can steal plaintext request authentication messages sent by SEAF (Security Anchor Function), use random challenge RAND and authentication token AUTN to conduct forgery attacks, and steal the authentication response of the target UE (User Equipment) and spy on its privacy information. The specific situation is shown in Figure 1, in which the red marked part shows that the attacker uses forgery attacks to spy on UE privacy information. Firstly, the attacker uses a sniffing tool to place it near the target UE, eavesdrops on the plaintext authentication request message sent to the target UE on the air interface, steals the RAND and AUTN data, and saves it locally.

Then, the attacker uses the stolen RAND and AUTN to forge the authentication request message, broadcast it in the place where the target UE may appear, and carry out the forgery attack. All UEs near the attacker will receive the request information and perform the authentication operation. After receiving the message, the UE verifies the message verification code MAC (Medium Access Control) and the Sequence Number SQN (Sequence Number). Since the attacker uses the stolen AUTN and RAND to forge the authentication request message, the target UE and other UEs will send different response messages, and the other UEs will not pass the MAC check and SQN check, and reply to the malicious attacker with a *MAC_ Failure* response message to end the authentication. The target UE will pass the MAC check but not the SQN check, and reply to the malicious attacker with a *Sync_ Failure* response message to perform resynchronization operations.

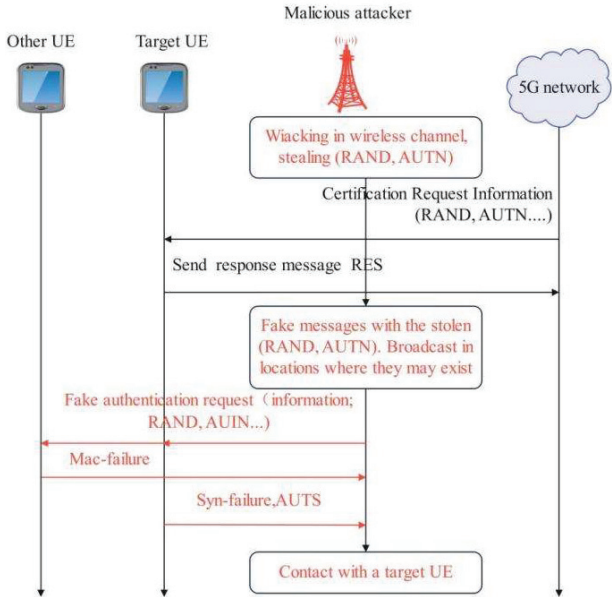


Figure 1 UE privacy risk caused by authentication response message.

The *CONC*∗ data in the authentication response message is only XOR encrypted by anonymous key AK. If the attacker makes two forgery attacks in a short time, AK encryption becomes meaningless. Then, the attacker snoops the privacy information of the target UE from the stolen SQN information to judge whether the target user is in a certain physical area, which seriously threatens the privacy security of the user.

The cross-layer recognition mechanism system model proposed in this paper is shown in Figure 2, where gNB is the base station equipment, UE is the user equipment, and Eve is the illegal attacker. The gNB and the UE are legal communication parties, and the communication channels are respectively represented by the downlink communication link *HDL* and the uplink communication link *HUL*, and both are TDL-D channel models, and the noise on the receiving side is white Gaussian noise. The attacker Eve is committed to eavesdropping on the legal channels of both parties in communication, stealing the data in the authentication process of both parties, hoping to crack the key information, or using the eavesdropping channel to generate the key, hoping to solve the stolen authentication data, and carrying out attacks such as forgery or replay, and seeking successful authentication, or using the response data of UE to snoop on private information.

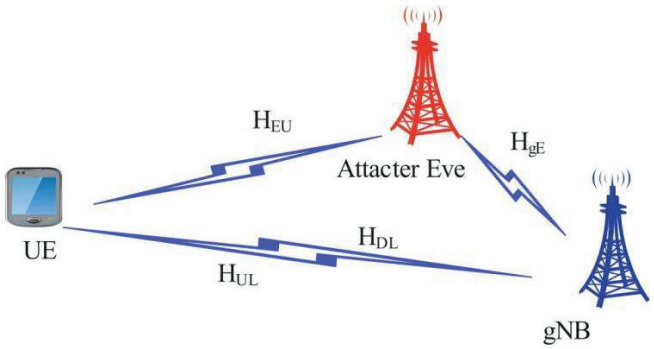


Figure 2 Cross-layer authentication mechanism system model.

3.2 Cross-layer Authentication Mechanism Process

In this paper, the physical layer authentication mechanism is combined with the EAP-AKA' authentication mechanism in 5G protocol, and a cross-layer authentication mechanism for 5G converged channel fingerprint is designed. The authentication process is shown in Figure 3.

Firstly, the UE and the serving network use the extracted channel features to realize physical layer authentication to ensure the security of the channel, and use the channel features to generate keys for subsequent encryption. Subsequently, the UE and the serving network execute an EAP-AKA' authentication mechanism, generate an authentication response, use the response as a trust credential, combine the response with the extracted channel characteristics into a joint key, and generate an authentication challenge and response in the cross-layer authentication mechanism by using an interpolation polynomial method. At the same time, the UE and the serving network use the channel characteristics to reconcile information and generate keys, encrypt the authentication challenge and response with the keys, and send them to the other party. Finally, after receiving the information, the authenticator uses the generated key to decrypt the information, obtains the specific authentication information, and sets the threshold according to the requirements to complete the cross-layer authentication.

The UE sets the authentication threshold Δ according to the authentication requirement, converts the authentication problem into a hypothesis testing problem, and uses the binary hypothesis testing method to match the results of Γ and Δ to judge the authentication result, as shown in formulas (1) and (2): a. a. The hypothesis H_0 indicates that if the statistical parameter Γ is less than the authentication threshold Δ, no attack is received in the

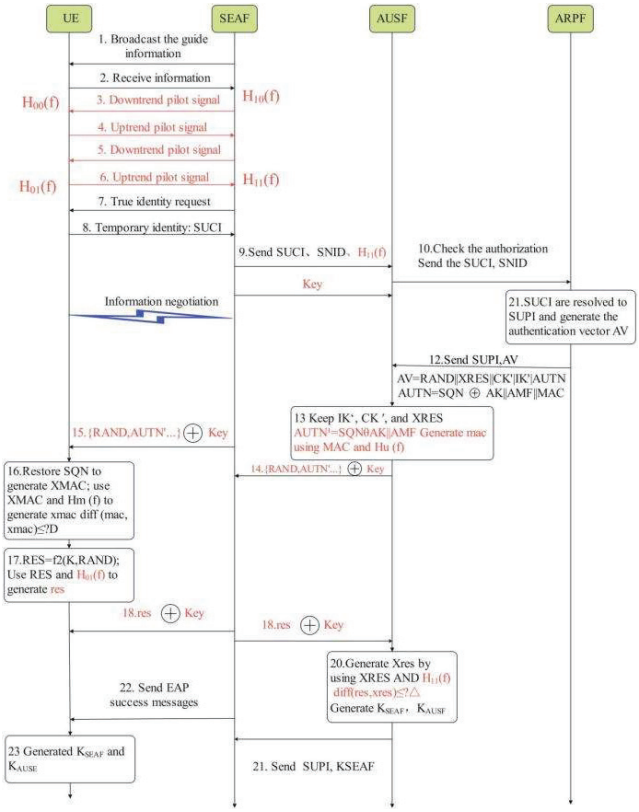


Figure 3 Cross-layer authentication process.

communication process and the base station is legal, and the authentication is successful. b. The hypothesis H_1 indicates that if the statistical parameter Γ is greater than the authentication threshold Δ, there may be an attack or a pseudo base station in the communication process, and the authentication fails.

$$H_0: \Gamma < \Delta \tag{1}$$

$$H_1: \Gamma > \Delta \tag{2}$$

In this paper, the key generation technology based on wireless channel is mainly divided into four steps: channel estimation, feature quantization, information harmonization and privacy amplification. The overall frame is shown in Figure 4. Among them, UE and gNB are legitimate communication

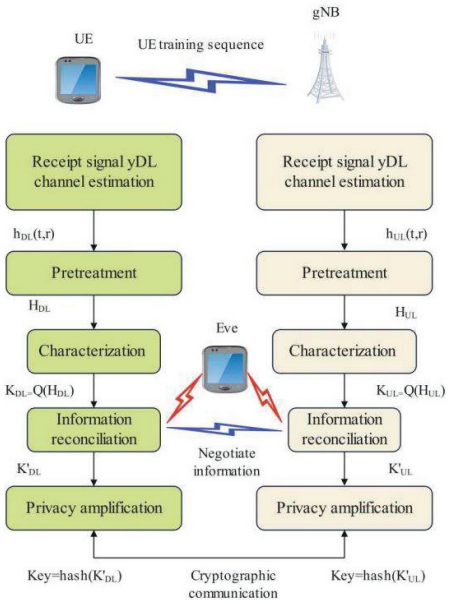


Figure 4 Key generation process.

parties, and Eve is a malicious attacker, eavesdropping on legitimate channel signals.

The specific steps are described as follows:

(1) Channel estimation involves measuring the channel using the received signal.
(2) Feature quantization refers to the process of quantifying estimated channel feature parameters into a bit stream. At present, there are quantization schemes such as single door limited quantity, double door limited quantity, and adaptive quantization threshold. This article uses the isomorphic quantization method to quantize the key bit stream.
(3) Information reconciliation is the process of correcting the quantized bit strings generated by both parties in communication, making them consistent and allowing both parties to have the same highly confidential key. This article uses Turbo codes for information harmonization.
(4) Privacy amplification, as the information reconciliation process requires negotiation between the communicating parties, attacker Eve can steal some information from the wireless air interface and analyze some key information from it. Privacy amplification is the process of discarding some key information that has been negotiated during the reconciliation

process, or compressing the negotiated key to prevent Eve from inferring key information, ensuring the security of the key.

Channel estimation refers to the measurement of a channel using a received signal. In the figure, the gNB transmits a downlink pilot signal $x_{DL}(t)$, which is represented by $y_{DL}(t)$ after UE receives it. After t time, the UE transmits an uplink pilot signal $x_{UL}(t)$, which is represented by $y_{UL}(t)$ after gNB receives it. Among them, τ is less than the coherence time *TC*. The channel impulse response can be expressed as $h(t,\tau) = \sum_{i=0}^{N(t)} \alpha_i(t)\delta(t-\tau_i(t))$, and the uplink and downlink received signals can be expressed as:

$$y_{DL}(t) = x_{DL}(t)h_{DL}(t,\tau) + n(t) \tag{3}$$

$$y_{UL}(t) = x_{UL}(t)h_{UL}(t,\tau) + n(t) \tag{4}$$

Among them, the downlink channel response of the gNB to the UE may be expressed as:

$$h_{DL}(t,\tau) = \sum_{i=0}^{N(t)} \alpha_i(t)\delta(t-\tau_i(t)) \tag{5}$$

According to the channel reciprocity characteristic, the uplink channel characteristic of the UE to the gNB can be expressed as:

$$h_{UL}(t,\tau) = h_{DL}(t,\tau) = \sum_{i=0}^{N(t)} \alpha_i(t+\tau)\delta(t+\tau-\tau_i(t)) \tag{6}$$

Since the training sequence process is in coherent time, $h(t,\tau)$ is almost the same as $h(t+\tau,\tau)$. Subsequently, the communication parties use fast Fourier transform to preprocess, and convert the channel impulse response into channel frequency responses H_{UL} and H_{DL}, which are respectively expressed as:

$$H_{DL} = Pr\ e(FFT(h_{DL})) \tag{7}$$

$$H_{UL} = Pr\ e(FFT(h_{UL})) \tag{8}$$

Among them, $Pr\ e$ is the preprocessing function, and FFT is the fast Fourier transform.

Feature quantization refers to quantizing an estimated channel feature parameter into a bit stream. At present, quantization schemes include single-gate limiting, double-gate limiting, adaptive quantization threshold, etc.

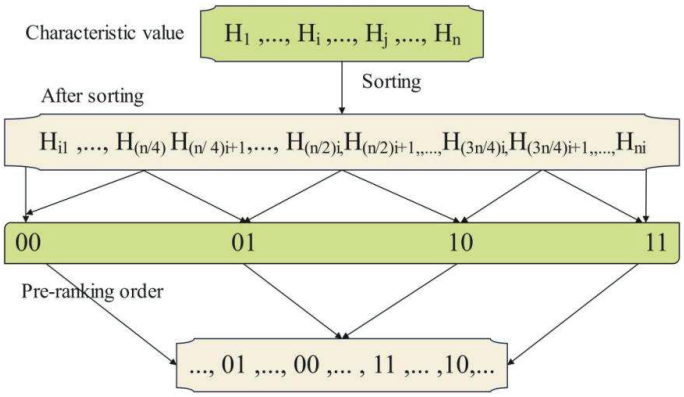


Figure 5 Quantization method.

In this paper, the equal probability quantization method is used to quantize the key bit stream.

The operation mode is shown in Figure 5. Both parties of legal communication first sort the eigenvalues, distribute the areas according to the quantization order, and the eigenvalues of the same area are the same number of bits, then use Gray code to reduce the key inconsistency rate, and finally obtain the key bit stream according to the original sequence. The respective key bitstreams of the UE and the gNB, both parties to the legitimate communication, are expressed as K_{DL} and K_{UL}.

In the EAP-AKA' authentication process, the authentication data is based on the bit stream, and once there is an errata of one bit in it, the whole authentication process will suffer failure. Without increasing verification or error correction, the bit error rate can be used to express the probability of authentication failure, and the bit error rate is affected by the signal modulation mechanism. Therefore, this paper selects three typical modulation methods for analysis, namely BPSK, QPSK and 2DPSK, and their bit error rates are as follows:

$$P_{e\_BPSK} = \frac{1}{2} erfc \frac{\sqrt{2}a}{2\sigma_n} = \frac{1}{2} erfc\sqrt{r} \tag{9}$$

$$P_{e\_QPSK} = 1 - \left[1 - \frac{1}{2} erfc \frac{a}{2\sigma_n}\right] = 1 - \left[1 - \frac{1}{2} erfc\sqrt{\frac{r}{2}}\right] \tag{10}$$

$$P_{e\_2DPSK} = erfc \frac{\sqrt{2}a}{2\sigma_n} = erfc\sqrt{r} \tag{11}$$

Among them, $r = a^2/(2\sigma_n^2)$ represents the signal-to-noise ratio at the input terminal, $a^2/2$ is the signal power and σ_n^2 is the noise power. EAPAKA' authentication modulates 128-bit authentication response data using the above modulation method, and the modulation corresponds to 128, 64, and 64 symbols respectively. In this paper, the false alarm rate is also used to express the authentication failure caused by the occurrence of bit error. Because of the bit error rate, the false alarm rate when the signal modulation mechanism is adopted can be expressed by formula (12):

$$F = 1 - (1 - P_e)^N \tag{12}$$

Among them, P_e is the bit error rate after modulation and N is the number of symbols. Because the proposed cross-layer authentication mechanism takes the physical layer channel characteristics as one of the authentication parameters and the curve fitting degree as the judgment parameter, it does not require the equation curves constructed by both authentication parties to be completely consistent, and has certain fault tolerance. Moreover, the fault tolerance performance is related to the setting of threshold value, the larger the threshold value is, the higher the fault tolerance performance, and the fault tolerance performance can also be characterized by the authentication success rate. At this time, the false alarm rate is the probability of authentication failure.

4 Experimental Study

4.1 Test Method

In this paper, QuaDRiGa simulation model is used to build a simulation environment on MATLAB software platform. The system configuration information is shown in Table 1. QuaDRiGa is a model developed by FraunhoferHHI and used for system-level simulation of mobile wireless networks, and it can generate real wireless channel impulse responses, and MIMO radio channels can be modeled for specific network configurations (e.g. indoor, satellite or heterogeneous networks).

In this paper, a 3D scattering simulation environment is created by using the QuaDRiGa model, in which the legal communication parties are Tx and Rx, which represent the base station gNB and the user UE respectively. When the gNB sends a signal, because the randomly generated scatterer is set in the simulation environment, the signal will pass through different scattering paths and finally reach the UE. The UE communicates with the gNB using the 5G

Table 1 System configuration

System Configuration	Contents
Operating system	Windows 10
Processor	Intel Core i99900KF Processor 16M Cache up to 5.00 GHz
RAM	64.0 GB
MATLAB Version	MATLAB R2024a
QuaDRiGa version	V 2.8. 1

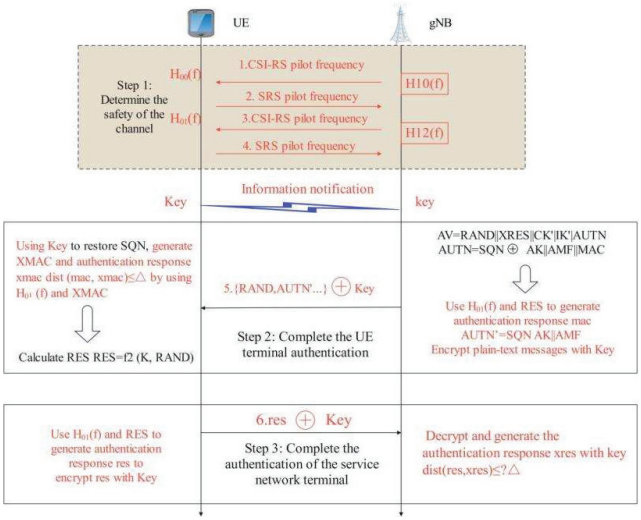


Figure 6 Flow of experimental steps.

reference signal, the gNB transmits signal status information CSI-RS to the UE via the downlink, and the UE transmits sounding reference signal SRS to the gNB via the uplink. Flow of experimental steps as shown in Figure 6.

4.2 Results

In this paper, the key inconsistency rates of both legal communication parties using different quantization orders in the feature quantization stage are compared, as shown in Figure 7.

The information entropy obtained when the authentication response information takes different response lengths is compared, as shown in Figure 8.

This paper compares the performance of the EAP-AKA' authentication mechanism with the cross-layer authentication mechanism under this condition setting, as shown in Figure 9.

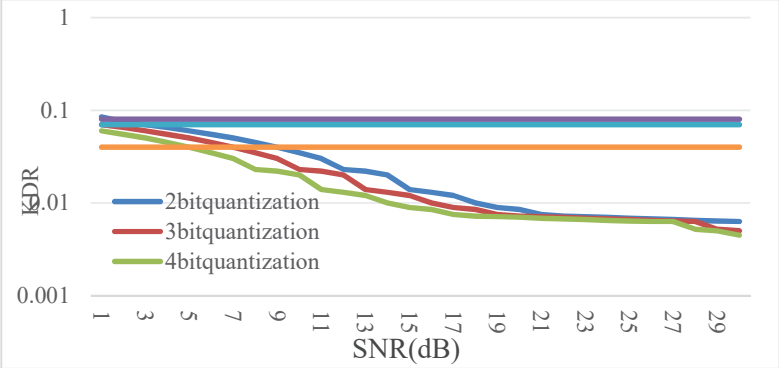


Figure 7 Relationship between key inconsistency rate, quantization order and correlation coefficient.

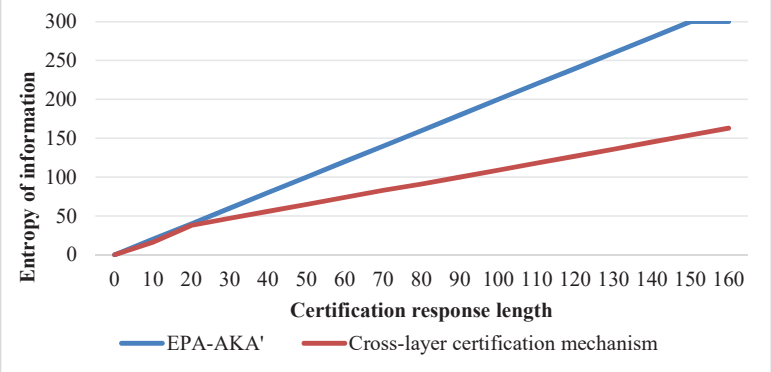


Figure 8 Comparison of information entropy.

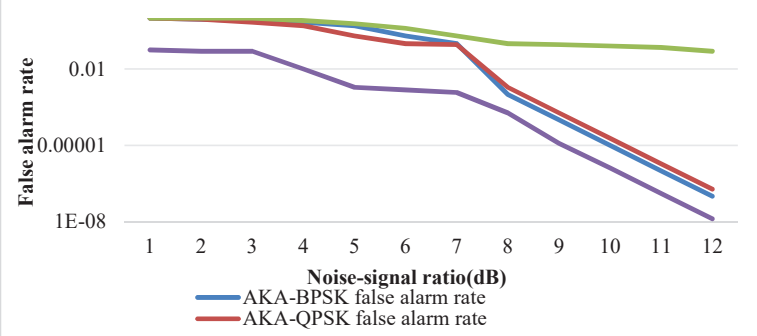


Figure 9 Relationship between false alarm rate and signal-to-noise ratio.

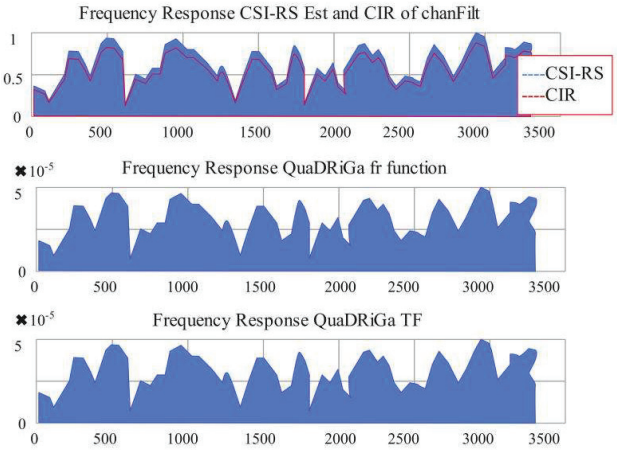
The gNB transmits a downlink CSI-RS (Channel State Information-Reference Signal) pilot signal, and after receiving the pilot signal, the UE estimates a channel characteristic from the pilot signal, which is denoted as H00 (f). At the same time, the UE transmits an uplink SRS (Sounding Reference Signal) pilot signal to the gNB. Figure 10(a) is a diagram of frequency response pairs of CSI-RS pilot signals transmitted by gNB, and they are respectively from bottom to top:

1. The frequency response diagram obtained by Fourier variation of impulse response;
2. The frequency response diagram calculated by impulse response through QuaDRiGa's own function;
3. The display diagram obtained by comparing the frequency response obtained by channel estimation using the CSI-RS reference signal in the communication process with the frequency response obtained by the equivalent channel filter using the impulse function CIR.

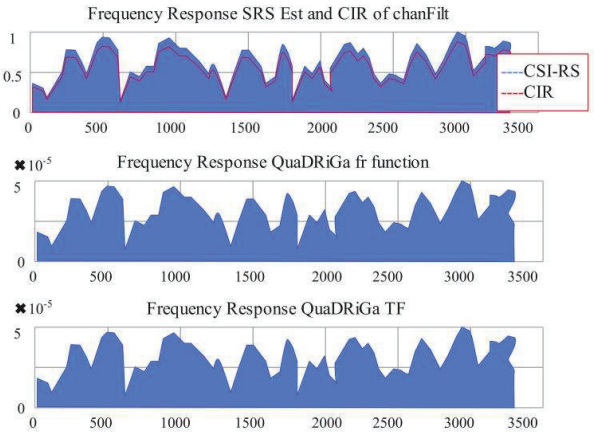
After receiving the signal, the NB extracts the channel feature H10 (f) therefrom. The frequency response diagram of the SRS pilot signal received by the gNB is shown in Figure 10(b).

4.3 Analysis and Discussion

This paper proposes a cross-layer authentication mechanism for 5G converged channel fingerprints, which realizes the superimposed enhancement of physical layer authentication and high-layer authentication. The wireless channel fingerprint and the authentication data generated by high-layer authentication form a joint key, and new authentication challenge and response information are generated based on interpolation polynomial method to realize cross-layer authentication. The proposed cross-layer authentication scheme uses the time-varying characteristics of wireless channel fingerprints to provide information entropy for higher layers, which enhances the security performance. At the same time, the cross-layer authentication mechanism uses the channel characteristics of the physical layer to generate the key, and encrypts the authentication challenge and response through the key, thus solving the problem that the attacker uses the stolen authentication data to carry out forgery attacks and snoop the user's privacy, enhances the security performance of authentication, and realizes the mutual complementarity and mutual enhancement of the physical layer and the high layer.



(a) CSI-RS frequency response



(b) SRS frequency response

Figure 10 Frequency response.

From the simulation results in Figure 6, it can be found that the quantization order is proportional to the key inconsistency rate. When the quantization order is larger, the key inconsistency rate is higher. In order to reduce the key inconsistency rate, the quantization order adopted in this paper is 2.

This paper also compares the key inconsistency rate between Eve (Eavesdropper) channel and legitimate communication channel, which shows the influence of the correlation between Eavesdropper channel and legitimate communication channel on the key inconsistency rate. From the simulation results, it can be found that when the quantization order is 2, the larger the correlation coefficient ρ, the key inconsistency rate of Eavesdropper channel decreases, but there is still a big gap between Eavesdropper channel and legitimate communication channel.

It can be seen from Figure 8 that the information entropy of the proposed cross-layer authentication mechanism is greater than that of the EAP-AKA' authentication mechanism, which increases the difficulty of attacking malicious attackers. In the 5G protocol, the authentication challenge and response information generated by the EAP-AKA' authentication mechanism, such as MAC and RES, are 64 and 128 bits in length respectively, and correspond to the information entropy of 64 and 128 bits respectively. The proposed cross-layer authentication mechanism can achieve the same information entropy of authentication challenge or response length are set, and can achieve 131 bits of information entropy when the same 64-bit authentication response length is set. Therefore, the cross-layer authentication mechanism after fusing the physical layer channel fingerprint can increase the information entropy of EAP-AKA' in the original 5G protocol and enhance the security performance of the authentication system.

In Figure 9, the false alarm rate changes with the change of signal-to-noise ratio. It can be found that as the signal-to-noise ratio increases, the false alarm rate decreases. The false alarm rate of the cross-layer authentication mechanism is always lower than that of the modulated EAP-AKA' authentication mechanism under the condition of 1–12 dB and has better authentication performance.

It can be found from Figure 10(a) that the three results are the same, which proves the accuracy of channel estimation in the experiment. Comparing Figures 10(a) and 10(b), it is found that the frequency responses of the uplink and downlink reference signals are almost the same, satisfying channel reciprocity. At this time, the UE moves 1/4 wavelength distance, and the gNB transmits the CSI-RS pilot signal again.

With the practical implementation of 5G communication systems and the widespread application of technologies such as Massive MIMO and millimeter wave communication, communication methods have become more diverse and wireless channel resources have become more abundant, providing a broader space for research on physical layer authentication. This

article mainly studies the use of wireless channel characteristics to enhance authentication security performance, proposes targeted solutions, and verifies the effectiveness of our model through experimental research.

Overall,this paper uses the 5G experimental platform and the built MATLAB simulation environment in the subject to verify the feasibility and security of the cross-layer authentication mechanism that integrates channel fingerprints. The experimental results show that the proposed cross-layer authentication mechanism has good authentication performance and security performance.

5 Conclusion

This paper studies the cross-layer authentication mechanism for 5G converged channel fingerprints, and proposes corresponding solutions to the existing physical layer authentication problems, so as to provide ideas for the high-security, high-reliability, and high-flexibility authentication mechanism required in 5G application scenarios. Aiming at the hidden danger of key leakage in physical layer challenge-response authentication, a physical layer challenge-response authentication mechanism based on interpolation polynomial is proposed, and its performance is analyzed by simulation to solve the hidden danger of key leakage. In addition, in view of the problems that the current high-level authentication mechanism leaks privacy, the key entropy decreases with the increase of authentication times, and the joint design of physical layer authentication and high-level authentication protocols has received less attention, this paper combines physical layer authentication with EAP-AKA' authentication protocol in 5G networks to design a cross-layer authentication mechanism that integrates channel fingerprints. From the experimental analysis, it can be seen that the model proposed in this article has good performance in enhancing the security performance of the authentication system and better authentication performance, as well as good performance in channel estimation accuracy. It solves the potential security risks existing in the current protocol from the perspective of physical layer, and provides key entropy for the higher layer by using the channel characteristics of physical layer, thus enhancing the security performance of authentication.

Finally, this paper uses the 5G experimental platform and the built MATLAB simulation environment in the subject to verify the feasibility and security of the cross-layer authentication mechanism that integrates channel fingerprints. The experimental results show that the proposed cross-layer

authentication mechanism has good authentication performance and security performance. The next research plan is to collect real 5G channel characteristics in real 5G scenarios to verify the feasibility and security of the cross-layer authentication mechanism proposed in this paper.

Acknowledgment

This paper is supported by the "Research and Application of Key Technologies for 5G Network Security in Terminal Access for New Power System" (Neidian Kechuang [2024] No. 5) ,which funded by the Science and Technology Program of Inner Mongolia Power (Group) Co., Ltd.

References

[1] Xu, D., Yu, K., and Ritcey, J. A., 'Cross-layer device authentication with quantum encryption for 5G enabled IIoT in industry 4.0', IEEE Transactions on Industrial Informatics, 18(9), 6368–6378, 2021.

[2] Lee, Y., Yoon, J., Choi, J., and Hwang, E., 'A novel cross-layer authentication protocol for the Internet of Things', IEEE Access, 8(1), 196135–196150, 2020.

[3] Liu, X., Wang, J., Guo, S., and Wang, H., 'A Survey on Cross-Layer Authentication in Wireless Communication Networks', Journal of Networking and Network Applications, 4(1), 21–30, 2024.

[4] Wang, M., Zhao, D., Yan, Z., Wang, H., and Li, T., 'XAuth: Secure and privacy-preserving cross-domain handover authentication for 5G HetNets', IEEE Internet of Things Journal, 10(7), 5962–5976, 2022.

[5] Zhao, D., Yan, Z., Wang, M., Zhang, P., and Song, B., 'Is 5G handover secure and private? A survey', IEEE Internet of Things Journal, 8(16), 12855–12879, 2021.

[6] Nagamani, K., and Monisha, R., 'Physical Layer Security Using Cross Layer Authentication for AES-ECDSA Algorithm', Procedia Computer Science, 215(2), 380–392, 2022.

[7] Zhao, H., Xu, M., Zhong, Z., and Wang, D., 'A fast physical layer security-based location privacy parameter recommendation algorithm in 5G IoT', China Communications, 18(8), 75–84, 2021.

[8] Parween, S., Hussain, S. Z., Hussain, M. A., and Pradesh, A., 'A survey on issues and possible solutions of cross-layer design in Internet of Things', Int. J. Comput. Networks Appl, 8(4), 311–320, 2021.

[9] Solaija, M. S. J., Salman, H., and Arslan, H., 'Towards a unified framework for physical layer security in 5G and beyond networks', IEEE Open Journal of Vehicular Technology, 3(1), 321–343, 2022.

[10] Cui, Q., Zhu, Z., Ni, W., Tao, X., and Zhang, P., 'Edge-intelligence-empowered, unified authentication and trust evaluation for heterogeneous beyond 5G systems', IEEE Wireless Communications, 28(2), 78–85, 2021.

[11] Salahdine, F., Han, T., and Zhang, N., 'Security in 5G and beyond recent advances and future challenges. Security and Privacy, 6(1), e271–e280.

[12] Ramadan, M., Liao, Y., Li, F., and Zhou, S., 'Identity-based signature with server-aided verification scheme for 5G mobile systems', IEEE Access, 8(2), 51810–51820, 2020.

[13] Boodai, J., Alqahtani, A., and Frikha, M., 'Review of Physical Layer Security in 5G Wireless Networks', Applied Sciences, 13(12), 7277–7287, 2023.

[14] Sun, Y., Tian, Z., Li, M., Zhu, C., and Guizani, N., 'Automated attack and defense framework toward 5G security', IEEE Network, 34(5), 247–253, 2020.

[15] Wu, T., Guo, X., Chen, Y., Kumari, S., and Chen, C., 'Amassing the security: An enhanced authentication protocol for drone communications over 5G networks', Drones, 6(1), 10–17, 2021.

[16] Han, S., Lee, Y., Choi, J., and Hwang, E., 'Lightweight physical layer aided key agreement and authentication for the Internet of Things', Electronics, 10(14), 1730–1738, 2021.

[17] Sodhro, A. H., Pirbhulal, S., Sodhro, G. H., Muzammal, M., Zongwei, L., Gurtov, A., ... and de Albuquerque, V. H. C., 'Towards 5G-enabled self adaptive green and reliable communication in intelligent transportation system', IEEE Transactions on Intelligent Transportation Systems, 22(8), 5223–5231, 2020.

[18] Al-Aqrabi, H., Johnson, A. P., Hill, R., Lane, P., and Alsboui, T., 'Hardware-intrinsic multi-layer security: A new frontier for 5G enabled IIoT', Sensors, 20(7), 1963–1972, 2020.

[19] Hao, Y., and Qiu, X., 'MIMO cross-layer secure communication algorithm for cyber physical systems based on interference strategies', IEEE Access, 8(5), 226797–226810, 2020.

Biographies

Wei Ao, holds a Master's degree in Engineering and is a senior engineer. He is a member of the Communist Party of China and graduated from Inner Mongolia University with a bachelor's degree in Computer Science and Technology in July 2004. In the same year, he started working at Inner Mongolia Power Information and Communication Company. In June 2014, he graduated with a Master's degree in Engineering from North China Electric Power University with a major in Industrial Engineering. In September 2023, he became the Deputy General Manager of Inner Mongolia Power Digital Research Company, responsible for scientific and technological innovation and production operation management. He has won three technical innovation achievements in the autonomous region's power industry, one second prize in group company level management innovation achievements, five third prizes in scientific and technological progress awards, and four utility patents.

Jian Wei graduated from Changchun Institute of Technology in July 2015 with a bachelor's degree. From July 2012 to November 2023, he worked at the Information and Communication Branch of Inner Mongolia Electric Power (Group) Co., Ltd. From November 2023 to present, he has been working

at the Digital Research Branch of Inner Mongolia Electric Power (Group) Co., Ltd. His current main research directions are information technology construction, artificial intelligence, etc.

Yindong Li graduated from Inner Mongolia University of Technology with a Bachelor's degree in Computer Science and Technology in 2007. He worked at the Information and Communication Branch of Inner Mongolia Electric Power (Group) Co., Ltd. from September 2007 to November 2023, and at the Digital Research Branch of Inner Mongolia Electric Power (Group) Co., Ltd. from November 2023 to present. His current main research direction is network security.

Xiaolong Zhang graduated from the Computer Science and Technology program at Inner Mongolia University in July 2021, where he obtained a Master of Engineering degree. From September 2021 to the present, he has been working at the Inner Mongolia Power Digital Research Company. His current primary research focus is on network security and network architecture.

Bin Yu, male, Mongolian, born in Jining, Inner Mongolia in February 1993. He started working in August 2016 and joined the Jiusan Society in December 2022. He holds a master's degree in business administration and is a senior engineer. He is a member of the Chinese Society of Electrical Engineering and the Chinese Computer Society.

From September 2012 to June 2016, studied Communication Engineering at the School of Information Engineering, Wuyi University; 2016.08–2023.11 Assistant Engineer, Engineer, and Senior Engineer at the Information and Communication Branch of Inner Mongolia Electric Power (Group) Co., Ltd. (during which: Master's degree in Business Administration at the School of Economics and Management, Inner Mongolia University from August 2019 to June 2022); From March 31, 2023 to present, Senior Engineer at the Digital Research Branch of Inner Mongolia Electric Power (Group) Co., Ltd.

Kaiwen Hou graduated from Inner Mongolia Agricultural University in July 2011 with a Bachelor's degree in Engineering. From October 2011 to November 2023, he worked at the Information and Communication Branch of Inner Mongolia Electric Power (Group) Co., Ltd. From November 2023 to present, he has been working at the Digital Research Branch of Inner Mongolia Electric Power (Group) Co., Ltd. His current main research areas are power information system construction, network security, artificial intelligence, etc.