AKA-PLA: Enhanced AKA Based on Physical Layer Authentication

Jing Yang[1], Xinsheng Ji[1,2], Kaizhi Huang[1], Ming Yi[1] and Yajun Chen[1]
[1] China National Digital Switching System Engineering and Technological R&D Center
Zheng Zhou, 450002 - P.R. China
[e-mail: yangjingFi@163.com]
[2] National Mobile Communications Research Laboratory, Southeast University
Nan Jing, 211189 - P.R. China
[e-mail:jxs@ndsc.com.cn]
*Corresponding author: Jing Yang

Received December 17, 2016; revised March 9, 2017; revised April 13, 2017; accepted April 27, 2017; published July 31, 2017

Abstract

Existing authentication mechanisms in cellular mobile communication networks are realized in the upper layer by employing cryptographic techniques. Authentication data are broadcasted over the air in plaintext, enabling attackers to completely eavesdrop on the authentication and get some information about the shared secret key between legitimate nodes. Therefore, reusing the same secret key to authenticate several times results in the secret key's information leakage and high attacking rate. In this paper, we consider the most representative authentication mechanism, Authentication and Key Agreement (AKA), in cellular communication networks and propose an enhanced AKA scheme based on Physical Layer Authentication (AKA-PLA). Authentication responses generated by AKA are no longer transmitted in plaintext but masked by wireless channel characteristics, which are not available to adversaries, to generate physical layer authentication responses by a fault-tolerant hash method. The authenticator sets the threshold according to the authentication requirement and channel condition, further verifies the identity of the requester based on the matching result of the physical layer authentication responses. The performance analyses show that the proposed scheme can achieve lower false alarm rate and missing rate, which are a pair of contradictions, than traditional AKA. Besides, it is well compatible with AKA.

Keywords: Authentication, channel characteristics, cross-layer, false alarm rate, missing rate

This research was supported by China's High-Tech R&D Program (863 Program) SS2015AA011306; Natural Science Foundation of China 61379006 and 61521003, and National Science Fund for Excellent Young Scholars 61501516.

https://doi.org/10.3837/tiis.2017.07.024 **ISSN : 1976-7277**

1. Introduction

Identity authentication is the process of verifying users' validity, which is the first step for secure communication [1][2]. After successful authentication, the communication nodes agree on the same symmetric key to secure subsequent communication. Therefore, authentication data such as challenge and response are mostly transmitted over the air in plaintext which are available to adversaries [3]. On the other hand, existing authentication mechanisms in cellular networks are realized in the upper layer by employing cryptographic techniques [1-4], whose security depend on the computational complexity [5]. Attackers are usually assumed to have limited storage and computing capability which is not always true for high-capacity computers such as quantum computers. It was commonly believed that adversaries can get some information about the secret key according to the eavesdropped authentication data and resuing the same shared secret key results in the secret key's information leakage and high attacking rate [6] [7]. [6] has demonstrated in theory that the successful attacking rate is lower bounded by $P \geq 2^{-I(K;X^n,Y^n)/n}$ after n rounds of eavesdropping, where X^n and Y^n are the challenge and response data. It is also believed that attackers with enough computational and storage power can crack the shared key by force at least in theory [7], which poses a big threat to wireless authentication.

In recent years, the inherent and unique characteristics of wireless channels have been considered as potential complements to enhance authentication security [8][9]. Wireless channels are location-specific due to path loss and channel fading, making any wireless link between two communication nodes unique and unclonable [10]. It is difficult for an adversary to get the information about the legitimate channel as long as its distances to legitimate communication nodes are larger than $\lambda/2$ (half of a wavelength) [11]. In addition, wireless channels are time-varying but short-term reciprocal, which means the two communication nodes can observe and extract the same channel characteristic within the channel coherence time [12]. These properties of wireless channels are the fundamental theoretical foundation of physical layer security [13][14], including physical layer authentication (PLA).

In [15-17], the unique wireless channels decided by users' locations are used as their fingerprints to achieve light-weight and fast authentication (which we call fingerprints-based PLA) by comparing the similarity of channel characteristics extracted from two successive data packets. If the channel characteristics are highly correlated, the sender can be regarded as the original one, otherwise, it is assumed to be an intruder. It is lightweight to decide whether current and prior communication attempts are made by the same user. [18-21] provide a novel idea to exploit wireless channels to achieve identity authentication using Challenge-Response mechanism (which we call CR-based PLA). Channel characteristics are exploited to mask the authentication challenge and secret key to generate the authentication response. Since the two communication nodes can extract similar channel characteristics, they can generate similar responses.

Physical layer authentication exploits the naturally available random and location-specific characteristics of wireless channels hence very hard to mimic. Besides, it is lightweight and easy to implement since channel estimation is indispensable in mobile communication. However, they can not be applied independently since they are susceptible to channel variations and noises. It is pointed out that cross-layer authentication combing the upper layer and physical layer is of great theoretical and practical significance and value [9][14].

Authors in [22-24] propose cross-layer authentication schemes by combining fingerprints-based PLA with traditional upper-layer authentication in which the identity authentication is achieved in the upper layer while the verification of subsequent data packets is achieved at the physical layer by comparing successive channel characteristics. In [7], a CR-based PLA scheme is integrated into AKA to achieve enhanced AKA. Only when the CR-based PLA and AKA are all passed, the authentication is successful.

Though cross-layer methods mentioned above can achieve enhanced authentication, they are still exposed to the problem of secret key's information leakage since the realization of the upper-layer authentication has not been changed. This means that after several rounds of eavesdropping, attackers could still get some information about the secret key and launch a successful attack.

In this paper, we consider the most representative authentication mechanism, AKA, in cellular networks and propose an enhanced AKA scheme based on Physical Layer Authentication (AKA-PLA) by integrating AKA and CR-based PLA. The employed PLA scheme in this paper was proposed in our previous work and interested readers can refer to [21] for detailed information. The responses generated in AKA do not need to be transmitted over the air, but are used as the keys for physical layer authentication. The wireless channel characteristics are extracted and bound with the keys to generate PLA responses using a fault-tolerant hash method. Different from existing cross-layer schemes achieving authentication in the upper layer and physical layer separately, we integrate them. Verification is only executed in the physical layer according to the matching result of the PLA responses. The performance analyses show that the proposed authentication scheme can achieve lower false alarm rate as well as missing rate than AKA. It is worth noting that our idea can also be applied to LTE and other communication networks which employ symmetric cryptosystem to achieve authentication.

The rest of the paper is organized as follows. In Section 2, we analyze the problem of key information leakage of AKA. In Section 3, we describe in detail the proposed enhanced AKA based on PLA. The performance analyses of our proposed method compared to AKA are derived in Section 4, and finally, conclusions are drawn in Section 5.

2. Problem Overview

Fig. 1 illustrates the general process of AKA. The authentication entities involved are the user (UE), the base station (BS), the Visitor Location Register (VLR) and Home Location Register (HLR). The HLR stores the identity key K of the UE, which is only known by the UE and HLR and used to uniquely identify the UE.

The BS sends a request for real identity to the UE when received an access request from the UE. The UE then sends the real identity to the BS and the latter forwards it to the HLR via VLR. The HLR generates authentication vector (AV) composed as follows: $AV = RAND \| XRES \| CK \| IK \| AUTN$ and transmits to the VLR and BS. $RAND$ is the authentication challenge which is usually a random number. $XRES$ is the expected authentication response used by the network to verify the UE, CK and IK are respectively the cipher key and integrity key. $AUTN$ is the authentication token composed as follows in (1),

$$AUTN = SQN \oplus AK \| AMF \| MAC \tag{1}$$

where MAC is the authentication code used by the UE to verify whether the network is legal. MAC, $XRES$, CK, IK are generated by hash functions specified by 3GPP with the challenge $RAND$ and the secret key K as the inputs and their lengths are all 128 bits.

The BS transmits $RAND$ and $AUTN$ to the UE and the latter employs the same hash methods to generate authentication responses $XMAC$ and RES, and then compares whether MAC is same with $XMAC$. Similarly, RES is transmitted to the network to authenticate the UE by comparing RES and $XRES$.

During the process, authentication challenge $RAND$ and responses (RES, $XRES$, MAC, $XMAC$) are all transmitted in plaintext. Attackers can completely eavesdrop on them and get some information about the secret key, i.e., $H(K \mid RAND, RES) > 0$. Therefore, the information entropy of the secret key decreases as the authentication times increases, resulting in high attacking rate. It has been demonstrated in [6] in theory that the successful attacking rate is lower bounded by $P \geq 2^{-I(K;RAND,XRES)/n}$ after n rounds of eavesdropping.

Researches on message authentication [25][26] and identity authentication [6] have pointed out that channel noises can help to prevent the secret key's information leakage and lower the attacking rate. But they did not give concrete examples about how channels noises can be exploited to improve authentication performance. This paper presents a concrete illustration of how channel characteristics can be used as a kind of noise to prevent the secret key's information leakage.

3. AKA-PLA: Enhanced AKA Based on Physical Layer Authentication

In this section, we describe our proposed enhanced authentication AKA-PLA in detail. **Fig. 1** shows the whole authentication flow of AKA and AKA-PLA , where the steps in red color are the improvements based on AKA, namely the parts related to PLA. AKA is firstly performed and the generated responses are used as the keys for PLA. The UE and the BS extract wireless channel characteristics and bind them with the keys by a fault-tolerant hash method to generate PLA responses and further judge according to the decision threshold.

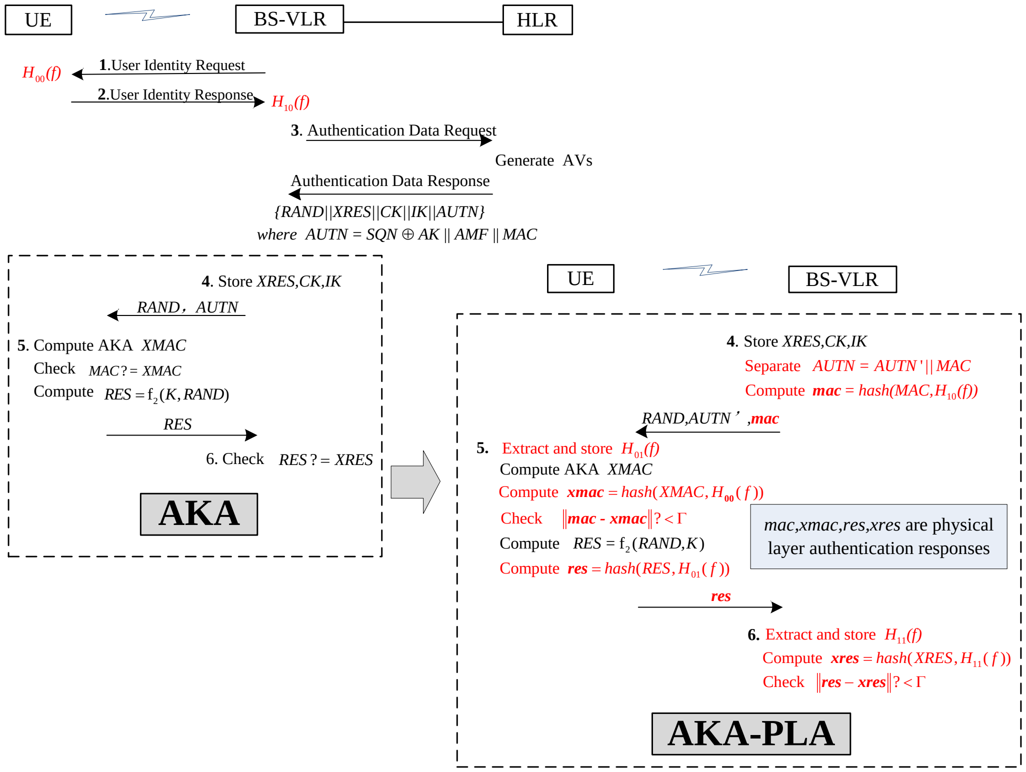

UE
BS-VLR
HLR
$H_{00}(f)$
1.User Identity Request
2.User Identity Response
$H_{10}(f)$
3. Authentication Data Request
Generate AVs
Authentication Data Response
{RAND||XRES||CK||IK||AUTN}
where AUTN = SQN ⊕ AK || AMF || MAC
4. Store XRES,CK,IK
RAND，AUTN
5. Compute AKA XMAC
Check MAC ? = XMAC
Compute $RES = f_2(K, RAND)$
RES
6. Check RES ? = XRES
AKA
UE
BS-VLR
4. Store XRES,CK,IK
Separate AUTN = AUTN '|| MAC
Compute mac = hash(MAC,$H_{10}(f)$)
RAND,AUTN ’ ,mac
5. Extract and store $H_{01}(f)$
Compute AKA XMAC
Compute xmac = hash(XMAC, $H_{00}(f)$)
Check ||mac - xmac|| ? < Γ
Compute $RES = f_2(RAND, K)$
Compute res = hash(RES, $H_{01}(f)$)
mac,xmac,res,xres are physical layer authentication responses
res
6. Extract and store $H_{11}(f)$
Compute xres = hash(XRES, $H_{11}(f)$)
Check ||res − xres|| ? < Γ
AKA-PLA

Fig. 1. Authentication flows of AKA and AKA-PLA

(1) Steps 1-3

These steps are exactly same with AKA except that during steps 1-2, the UE and BS measure and store the channel frequency responses according to the pilot signals of each other. Due to the noises, they will store noisy versions of the channel responses. The channel characteristic extracted by the UE in step 1 can be expressed as:

$$H_{00}(f)=\overline{H_{00}(f)}+N_{00}(f) \tag{2}$$

where $\overline{H_{00}(f)}$ and $N_{00}(f)$ are respectively the true channel frequency response and the noise. $H_{00}(f)$ and $N_{00}(f)$ are modeled as complex Gaussian distributions with zero mean and variances σ_H^2 and σ_N^2, i.e., $H_{00}(f) \sim CN(0,\sigma_H^2)$, $N_{00}(f) \sim CN(0,\sigma_N^2)$ (CN denotes the complex Gaussian distribution). For simplicity, all the noises are modeled with the same distribution without loss of realism. The BS measures and stores the extracted channel characteristic $H_{10}(f)$ with the same method.

(2) Step 4

The BS forwards the authentication data to the UE to verify the network. The way of transmitting the authentication data is the main difference between AKA and the proposed AKA-PLA. Different from AKA where $AUTN$ is transmitted directly to the UE, the BS separates the authentication code MAC out and uses a fault-tolerant hash method $hash(\cdot)$ proposed in our previous work [24] to bind MAC and $H_{10}(f)$ to generate physical layer response $\boldsymbol{mac}$ in (3),

$$\boldsymbol{mac} = hash(H_{10}(f), MAC) \tag{3}$$

The hash process consists of the following steps:

a) $H_{10}(f)$ is N-point sampled to get sequence $\boldsymbol{H}_{10}$. Assuming that the sampling size N is appropriately set to ensure that every sample is complex Gaussian distributed with zero mean and variance σ_H^2. MAC is mapped to a complex Gaussian process $\boldsymbol{MAC}$ with the distribution of $CN(0,\sigma_H^2)$ [27] with length of L which is similar to the synthetic fingerprints in [28][29]. Different $MACs$ are mapped to different fingerprints. $\boldsymbol{H}_{10}$ and $\boldsymbol{MAC}$ are concatenated to get the initial authentication information $\boldsymbol{AUC}$ by (4).

$$\boldsymbol{AUC} = [\boldsymbol{H}_{10}, \boldsymbol{MAC}] \tag{4}$$

Then $\boldsymbol{AUC}$ can be regarded as a synthetic curve and the authentication can be converted into the process of curve matching.

b) The hash method in 3D curve matching [30] is employed to map $\boldsymbol{AUC}$ into a hash vector $\boldsymbol{mac}:(P_1, P_2 \ldots P_{\mathrm{M}})$ with length of M which will be used as the authentication response. Every element $P_m (1 \le m \le M)$ in the vector is calculated by (5),

$$P_m = a\sum_{i=1}^{N+L} AUC_i \cdot \cos(2\pi m(i-1)/(N+L)) \tag{5}$$

where $a(a>0)$ is a fixed real parameter, $m = 1, 2 \cdots M$. Since every element in $\boldsymbol{AUC}$ is complex Gaussian distributed with zero mean and variance σ_H^2, it can be deduced that $P_m \sim CN(0, a^2\eta\sigma_H^2)$, where $\eta = \sum_{i=1}^{N+L} (\cos\frac{2\pi m(i-1)}{N+L})^2 = \frac{N+L}{2}$. It has been proved that the hash method is fault-tolerant and irreversible, which means that the two legitimate nodes can generate similar responses despite the noises and attackers can not crack the authentication data reversely. Interested readers can refer to our previous work [24] for detailed derivation and proof.

Then the BS sends $AUTN' := SQN \oplus AK \| AMF$, the random number $RAND$ and the physical layer response $\boldsymbol{mac}$ to the UE.

(3) Step 5

After receiving the authentication information from the BS, the UE measures and stores the updated wireless channel characteristic $H_{01}(f)$.

The UE demodulates the received signal to get $RAND$, $AUTN'$ and further generates the authentication code $XMAC$ which will be same to MAC if the network is legal. Then the UE generates PLA response $\boldsymbol{xmac}$ by (3) with $H_{00}(f)$ and $XMAC$ as the inputs. The test statistic Z defined in (6) is employed to get the matching degree of the PLA responses,

$$Z = \boldsymbol{zz}^H = (\boldsymbol{mac} - \boldsymbol{xmac})(\boldsymbol{mac} - \boldsymbol{xmac})^H = \|\boldsymbol{mac} - \boldsymbol{xmac}\| \tag{6}$$

where $\boldsymbol{z} = \boldsymbol{mac} - \boldsymbol{xmac}$. The UE employs binary hypothesis test (7) to authenticate the network according to the matching result based on the threshold. If the test statistic Z is smaller than a specific threshold Γ, authentication is successful. The network is regarded to be legal and the wireless channel is not under attack. On the contrary, when Z is larger than Γ, the hypothesis H_1 is accepted and the authentication fails. The BS is supposed to be illegal or the wireless channel is under attack.

$$\begin{aligned} H_0 &: Z < \Gamma \\ H_1 &: Z > \Gamma \end{aligned} \tag{7}$$

After successful authentication of the network, the UE uses the random number $RAND$ and the shared key K to update the authentication response RES of AKA,

$$RES = \mathrm{f}_2(K, RAND) \tag{8}$$

Then the extracted channel characteristic $H_{01}(f)$ and RES are used to generate PLA response $\boldsymbol{res} = hash(H_{01}(f), RES)$, which is then sent to the BS.

(4) Step 6

After receiving $\boldsymbol{res}$, the BS extracts the channel characteristic $H_{11}(f)$ and employs $H_{11}(f)$ and $XRES$ to generate the PLA response $\boldsymbol{xres}$. $\boldsymbol{res}$ and $\boldsymbol{xres}$ are compared by (7) and judged by (8).

After successful authentication of each other, both sides use AKA key generation schemes to generate the cipher key CK and integrity key IK to secure transmission of subsequent communications.

4. Performance Analysis

Since it is impossible to quantitatively calculate $H(K \mid RAND, RES)$, the conditional entropy of the secret key according to the challenge and response, we choose to analyze the ideal case in which attackers can get nothing about the key, i.e., $H(K \mid RAND, RES) = 0$. The performance of our scheme can be proved if it still outperforms AKA in this case.

4.1 Entropy Comparison

The entropy of authentication data in our proposed scheme has been improved since authentication data are physical layer signals instead of traditional binary bit streams.

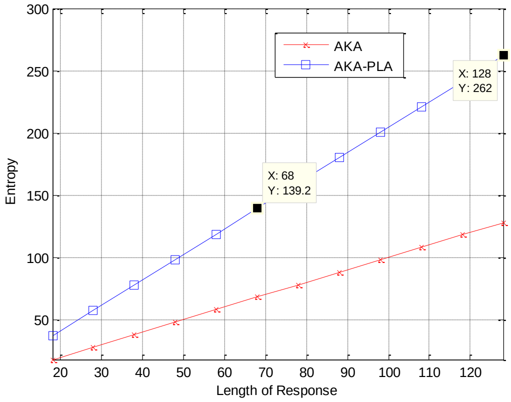


Fig. 2. Entropy comparison of AKA and AKA-PLA

When the attacker knows nothing about the secret key, the information entropy of every element in AKA response can be calculated as $H_{AKA} = -2 \times 1/2 \times \log(1/2) = 1(bit)$. While the responses in our proposed scheme AKA-PLA are complex Gaussian distributed and the probability density functions are expressed as $p(x) = 1/\sqrt{2\pi\sigma_H^2}\exp(-x^2/2\sigma_H^2)$ when the samples of the channel frequency response are uncorrelated. Then the information entropy can be calculated by,

$$
\begin{aligned}
& H_{AKA-PHY} = -\int_{-\infty}^{\infty} p(x)\log p(x)dx \\
& = -\int_{-\infty}^{\infty} p(x)\log(1/\sqrt{2\pi\sigma_H^2})dx - \int_{-\infty}^{\infty} p(x)\log(\exp(-x^2/2\sigma_H^2))dx \\
& = \log\sqrt{2\pi\sigma_H^2}\cdot\int_{-\infty}^{\infty} p(x)dx + \log(e)/2\sigma_H^2\cdot\int_{-\infty}^{\infty} x^2 p(x)dx \\
& = \log\sqrt{2\pi\sigma_H^2} + \log\sqrt{e} = 1/2\log(2\pi e\sigma_H^2)(bit)
\end{aligned}
\tag{9}
$$

Fig. 2 shows the entropy comparison of authentication information between AKA and AKA-PLA under different response lengths where σ_H^2 is normalized to be 1. As can be seen, the information entropy of AKA-PLA is larger than AKA, making attacks more difficult. It can achieve 128-bit entropy in AKA while 262 bits in our proposed AKA-PLA. When AKA-PLA is required to achieve the same information entropy strength as AKA, the required response length is 63 which is only half of AKA. Therefore, AKA-PLA can reduce the communication overhead and improve communication efficiency.

4.2 Security Comparison

Authentication data in AKA are binary bit streams, which are not fault-tolerant. That means a single-bit error in authentication data will result in authentication failure. When no extra overhead considered (such as using channel coding), the probability of authentication failure can be characterized by the bit error rate which is affected by modulation schemes. Different modulation schemes such as Binary Phase Shift Keying (BPSK), Quadrature Phase Shift Keying (QPSK), 8 Phase Shift Keying (8PSK) are considered here whose bit error rates p_{e_BPSK}, p_{e_QPSK}, p_{e_8PSK} are $1/2\mathrm{erfc}\sqrt{r}$, $1-[1-1/2\mathrm{erfc}\sqrt{r/2}]^2$, $\mathrm{erfc}(\sqrt{r}\sin(\pi/8))$ [31] and 128, 64 and 43 symbols are required for 128 bits, respectively. The probability of authentication failure is denoted by the false alarm rate α, which means one communication node refuses the other legitimate side. Since the authentication will fail as long as there is a single-bit error, the FAR when employing BPSK can be characterized by the bit error rate,

$$\alpha_{AKA\_BPSK} = 1-(1-p_{e\_BPSK})^{128} \tag{10}$$

Similarly, the false alarm rates employing QPSK and 8PSK can be obtained, $\alpha_{AKA\_QPSK} = 1-(1-p_{e\_QPSK})^{64}$, $\alpha_{AKA\_8PSK} = 1-(1-p_{e\_8PSK})^{43}$.

The probability of successful attacks is denoted by the missing rate β, which means the two communication nodes fail to detect the attacks. Since attackers launch attacks by guessing, the attacking rates when employing different modulation methods are same,

$$\beta_{AKA} = 2^{-128} \tag{11}$$

AKA-PLA employs physical layer signals as authentication parameters and the distance as the decision parameter which does not require the responses to be exactly the same. When the authentication threshold is set to be Γ, the false alarm rate and missing rate can be expressed as (12),

$$\begin{aligned} \alpha_{AKA-PLA} &= P_{H_0}(Z > \Gamma) \\ \beta_{AKA-PLA} &= P_{H_1}(Z_{Eve} < \Gamma) \end{aligned} \tag{12}$$

where Z_{Eve} is the test statistic obtained by the authenticator when there exists an attacker. When the UE is legal, the m-th element of $\boldsymbol{z}$ can be derived from (5) as,

$$\begin{aligned} z(m) &= RES(m) - XRES(m) \\ &= a \cdot \sum_{i=1}^{N+L} (\cos\frac{2\pi m(i-1)}{N+L} \cdot (AUC_{Ai} - AUC_{Bi})) \\ &= a\sum_{i=1}^{N} (\cos\frac{2\pi m(i-1)}{N+L} \cdot (\Delta H_i)) \end{aligned} \tag{13}$$

It has been proved that $z(m) \sim CN(0, a^2\eta_1 \cdot 2\sigma_N{}^2)$, where $\eta_1 = \sum_{i=1}^{N}(\cos\frac{2\pi k(i-1)}{N+L})^2$, in our previous work [24]. Let $\lambda_1 = a^2\eta_1\sigma_N{}^2$, then $\frac{Z}{\lambda_1}$ is chi-square distributed with $2M$ degrees of freedom, i.e., $\frac{Z}{\lambda_1} \sim \chi^2(2M)$. For a fixed threshold Γ, the false alarm rate can be expressed as:

$$\begin{aligned} &\alpha_{AKA-PLA} = P\{Z > \Gamma \mid H_0\} \\ &= \mathrm{P}_r\{\frac{Z}{\lambda_1} > \frac{\Gamma}{\lambda_1} \mid H_0\} = 1 - \mathrm{F}_{\chi^2_{2M}}(\frac{\Gamma}{\lambda_1}) \end{aligned} \tag{14}$$

Similarly, $z_{Eve}(m) = RES_{Eve}(m) - XRES(m) \sim CN(0, 2a^2\eta\sigma_H^2)$. Let $\lambda_2 = a^2\eta\sigma_H^2$, then $\frac{Z_{Eve}}{\lambda_2} \sim \chi^2(2M)$. The missing rate can be expressed as:

$$\beta_{AKA-PLA} = P\{Z_{Eve} < \Gamma \mid H_1\} = F_{\chi^2_{2M}}(\frac{\Gamma}{\lambda_2}) \tag{15}$$

When given a specific false alarm rate α_0, the corresponding authentication threshold Γ_0 can be denoted as (16) according to (14),

$$\Gamma_0 = \lambda_1 \mathrm{F}_{\chi^2_{2M}}{}^{-1}(1 - \alpha_0) \tag{16}$$

Then the corresponding missing rate can be expressed as:

$$\beta_{AKA-PLA} = P\{Z_{Eve} < \Gamma \mid H_1\} = F_{\chi^2_{2M}}(\frac{\lambda_1}{\lambda_2} F^{-1}_{\chi^2_{2M}}(1 - \alpha_0)) \tag{17}$$

When BPSK, QPSK and 8PSK are employed, the values of M will be 128, 64 and 43, respectively. When the false alarm rate for AKA-PLA remains unchanged (assign $\alpha_0 = 0.00005$ here), the corresponding missing rates under different modulation schemes can be obtained from (17). **Fig. 3** shows the authentication performance of AKA and AKA-PLA under different signal-to-noise ratios (SNRs) when $\alpha_0 = 0.00005$. We can find that the missing rates for AKA under different modulation schemes are same, since the attacker can only launch an attack by guessing. It is the minimum probability of successful attacks for AKA. While for the proposed AKA-PLA, the missing rate decreases as the SNR increases. When the SNR is greater than a certain threshold, the false alarm rate and missing rate of AKA-PLA can be both lower than AKA. We can set the authentication threshold properly to ensure that both the missing rate and false alarm rate are lower than AKA and we try to search for the threshold area by following.

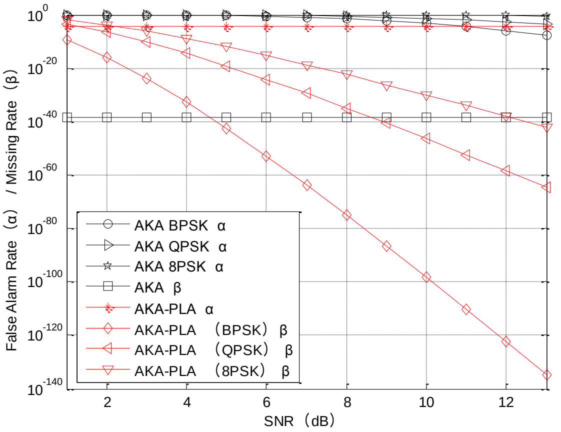


Fig. 3. Authentication performance under fixed false alarm rate ($\alpha_0 = 0.00005$)

Two requirements presented in (18) should be satisfied in order to make the false alarm rate and missing rate lower than AKA,

$$\begin{aligned} &\alpha = P\{Z > \Gamma \mid H_0\} = 1\text{-}\mathrm{F}_{\chi^2_{2M}}(\frac{\Gamma}{\lambda_1}) < \alpha_{AKA} \\ &\beta = P\{Z_{Eve} < \Gamma \mid H_1\} = F_{\chi^2_{2M}}(\frac{\Gamma}{\lambda_2}) < \beta_{AKA} \end{aligned} \tag{18}$$

The constrained area of Γ can be expressed as

$$\lambda_1 \mathrm{F}^{-1}_{\chi^2_{2M}}(1 - \alpha_{AKA}) < \Gamma < \lambda_3 \mathrm{F}^{-1}_{\chi^2_{2M}}(\beta_{AKA}) \tag{19}$$

Fig. 4 shows the threshold areas (the shaded areas) satisfying the constraint (19) when BPSK, QPSK, 8PSK are employed. We can see that when the SNRs are larger than 2dB, 6dB and 8dB, respectively, the false alarm rate and missing rate of AKA-PLA under different modulation schemes can be both lower than AKA. We further select the average thresholds in the constrained areas to analyze the authentication performance under different SNRs, shown in **Fig. 5**.

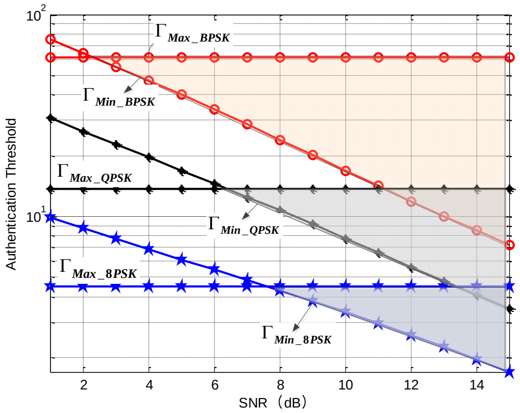


Fig. 4. Constrained area of Γ when the false alarm rate and missing rate of AKA-PLA are lower than AKA

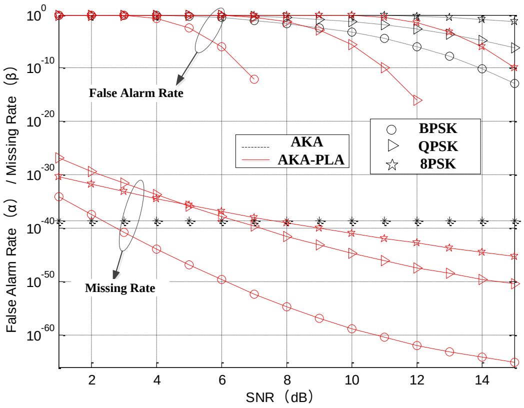


Fig. 5. Authentication performance when Γ is in the constrained area

We can find that as the SNR increases, both the false alarm rate and missing rate decrease. When the SNRs are larger than 2dB, 6dB, and 8dB under BPSK, QPSK and 8PSK, respectively, the false alarm rate and missing rate, which are a pair of contradictions, can be both lower than AKA, matching with the analysis results in **Fig. 4**. These SNR requirements can be easily satisfied in actual communication environments. When the SNR is lower, only one of the two parameters will be better than AKA. We can set the threshold according to the authentication requirements to guarantee the false alarm rate or missing rate.

In traditional AKA authentication, extra communication overhead, such as channel coding, are needed to improve authentication performance. When the (7, 4) linear block code [31] is employed here, 128-bit authentication data are divided into 32 groups with 7 bits in each group. Since the performance of 8PSK modulation is affected by encoding methods which is somewhat complex, we only analyze the performance of BPSK, QPSK modulations which require 224 and 112 carriers, respectively. Since the (7,4) linear block code can only correct one error, when more than one error in a group of seven bits occurs, the data can not be recovered correctly and the authentication will fail. For a 7-bit code, the probability that can not be correctly decoded can be expressed as:

$$p_{e\_BPSK}'=1-(1-0.5erfc(\sqrt{r}))^7-C_7^1(0.5erfc(\sqrt{r}))(1-0.5erfc(\sqrt{r}))^6 \tag{20}$$

The QPSK signal can be regarded as two BPSK signals and demodulated in two coherent demodulators and the bit error rate of each branch can be expressed as $0.5erfc(\sqrt{r/2})$. Then the probability that can not be correctly decoded under QPSK can be expressed as:

$$p_{e\_QPSK}'=1-(1-0.5erfc(\sqrt{r/2}))^7-C_7^1(0.5erfc(\sqrt{r/2}))(1-0.5erfc(\sqrt{r/2}))^6 \tag{21}$$

The probability of authentication failure using BPSK modulation is:

$$\alpha_{BPSK}'=1-(1-p_{e\_BPSK}')^{32} \tag{22}$$

Similarly, the false alarm rate for QPSK can be expressed as $\alpha_{QPSK}'=1-(1-p_{e\_QPSK}')^{32}$. When an attacker attempts to launch an attack, the probability of zero error and one-bit error in a 7-bit code is $(0.5)^7$ and $C_7^1(0.5)^7$, respectively. Then the probability of successful decoding can be expressed as $C_7^1(0.5)^7+(0.5)^7=(0.5)^4$. Since there are 32 pairs of 7-bit codes, the probability of successful attacks can be denoted as $(0.5)^{128}$, which is same to that when no channel coding techniques are employed.

The authentication performance of AKA-PLA is calculated through (14) and (15) as well while the corresponding degrees of freedom are changed to be 224 and 112.

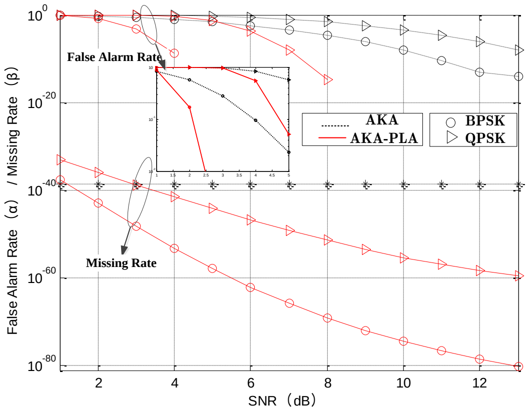


Fig. 6. Authentication performance comparison when AKA employs the (7,4) linear block code

The corresponding authentication performance is shown in **Fig. 6**. It can be seen that the false alarm rate and missing rate under BPSK and QPSK are both lower than AKA when the SNRs are larger than 1dB and 3dB, respectively. That means, even when AKA employs error correction codes to improve authentication performance, AKA-PLA still outperforms AKA. It is obvious that AKA-PLA can achieve the same authentication strength with AKA with less communication overhead, which improves communication efficiency.

4.3 Overhead Analysis

Our proposed authentication scheme combines AKA and PLA to form an enhanced authentication scheme, which can improve the security but increases the computation overhead. The increased computational overhead lies in the steps of generating PLA responses. The PLA responses are generated by a fault-tolerant hash method taking the AKA responses from the upper layer and the channel characteristics in the physical layer as the inputs. However, the increased computation process only involves in multiplication whose calculation is easy, making the increased overhead acceptable.

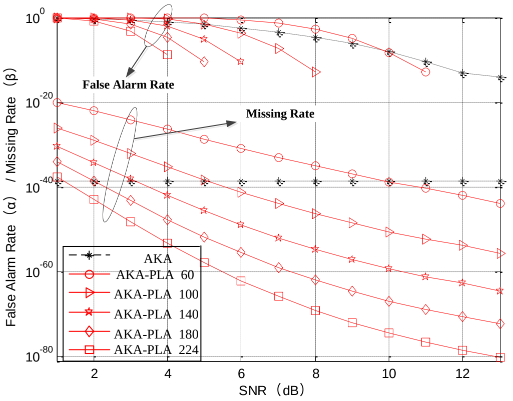


Fig. 7. Comparison of communication efficiency

Besides, AKA-PLA can achieve the same authentication strength with AKA with less communication overhead, improving the communication efficiency. **Fig. 7** shows the performance comparison of AKA and AKA-PLA under different carriers when AKA employs the (7, 4) linear block code and BPSK modulation.

We can find that the authentication performance of AKA-PLA becomes better as the number of carriers increases. When the SNRs are larger than specific values, the performance of AKA-PLA is better than AKA. For example, when the SNR is greater than 2dB, only 180 carriers are needed to achieve the same authentication strength of AKA which requires 224 carriers, reducing the carrier overhead by 19.6%.

4.4 Practicability Analysis

The responses in AKA are transmitted in plaintext and the secret key is reused due to the difficult distribution and refreshment of keys, resulting in the secret key's information leakage and high attacking rate. In our proposed scheme, the AKA responses are masked by wireless channel characteristics which are not available at the side of adversaries as long as their distances to legitimate nodes are larger than $\lambda/2$. Attackers can not crack the AKA responses according to the received physical layer responses, let alone getting the information of the secret key. The distance of $\lambda/2$ can be easily satisfied in actual communication environment which makes the proposed scheme practical. Even when the channel information is captured by attackers, it will not cause a severe impact on the performance, since PLA responses are generated by a physical layer hash process which we have proved to be irreversible and attackers cannot crack the authentication data reversely. Even under the worst case when attackers are extremely powerful to track all the authentication processes and capture all the channel characteristics, the performance of the proposed scheme is not fatal. It just degrades to traditional AKA since attackers can only get the AKA responses. They need to pay a heavy price further to get some information about the secret key. Moreover, attackers cannot employ the captured channel characteristics to forge PLA responses since they are not aware of correct AKA responses.

Besides, authentication in the upper layer employs cryptographic techniques which are not fault-tolerant. To guarantee the authentication performance, channel coding or other techniques are required, resulting in the increase in communication overhead. The proposed method employs physical layer channel information to hide AKA response which is fault-tolerant, requiring less communication overhead to achieve the same authentication strength with AKA. The authentication strength is also adjustable according to different requirements by setting different authentication thresholds. In addition, the proposed method involves in small changes which can be well compatible with AKA.

4.5 Comparisons with other authentication schemes

In this section, we will give comparisons between our proposed method and other related authentication schemes. **Table 1** gives the comparison of the proposed AKA-PLA with other cross-layer authentication schemes employing channel characteristics.

Table 1. Comparison with other cross-layer authentication schemes

	PLAA-SC in [24]	**[7]**	**Our scheme**
Realization	Upper layer authentication+ fingerprints-based PLA	AKA+CR-based PLA	AKA+CR-based PLA
Responses Transmission	In plaintext	In plaintext	Encrypted by channel characteristics
Advantages	Lightweight to secure every data packet	Two-factor authentication on identity and channel	Two-factor authentication, prevent key's information leakage
Disadvantages	Fails under fast-varying channels or burst transmission	Additional hash methods and steps	Involves in physical layer hash process
Information Leakage	Yes	Yes	No

Table 2 below gives the comparison of advantages and disadvantages of AKA and AKA-PLA.

Table 2. Comparison between AKA and AKA-PLA

	AKA	**AKA-PLA**
Advantages	● Standardized, widely used ● Not susceptible to channel condition by channel coding	● Prevents secret key's information leakage ● Requires less authentication overhead
Disadvantages	● Secret key's information Leakage ● Requires channel coding	● Susceptible to channel condition and noises ● Requires additional computation overhead to generate PLA responses

5. Conclusion

Aiming at the problem that the entropy of the secret key decreases as the authentication times increase in AKA, an enhanced AKA scheme based on physical layer authentication (AKA-PLA) is proposed. The authentication responses generated by AKA are protected by physical layer authentication using a fault-tolerant hash method and the authenticator sets the threshold according to the requirement and the wireless channel condition. The performance analyses show that the proposed authentication scheme can achieve lower false alarm rate as well as missing rate. To achieve the same authentication strength with AKA, AKA-PLA requires less communication overhead, improving communication efficiency. Since the authentication does not change the process and parameters of AKA, it has good compatibility with AKA. In actual communication scenarios, we can use AKA or AKA-PLA according to specific communication environments and authentication requirements. The proposed method provides an innovative idea for enhanced cross-layer authentication for the next-generation network.

References

[1] X Li, J Niu, J Liao and W Liang, "Cryptanalysis of a dynamic identity-based remote user authentication scheme with verifiable password update," *International Journal of Communication Systems*, vol. 28, no. 2, pp. 374-382, January 2015. Article (CrossRef Link)

[2] J Cao, M Ma, H Li, Y Zhang and Z Luo, "A survey on security aspects for LTE and LTE-A networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 283-302, April, 2014. Article (CrossRef Link)

[3] X Li, J Niu, S Kumari, J Liao and W Liang, "An Enhancement of a Smart Card Authentication Scheme for Multi-server Architecture," *Wireless Personal Communications*, vol. 80, no. 1, pp. 175-19, August 2015. Article (CrossRef Link)

[4] X Li, J Niu, MK Khan, J Liao and X Zhao, "Robust three-factor remote user authentication scheme with key agreement for multimedia systems," *Security & Communication Networks*, vol. 9, no. 13, pp. 1916-1927, September, 2016. Article (CrossRef Link)

[5] U M Maurer, "Authentication theory and hypothesis testing," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1350-1356, July, 2000. Article (CrossRef Link)

[6] F Zheng, Z Xiao, S Zhou, J Wang and L Huang, "Identity Authentication over Noisy Channels," *Entropy*, vol. 17, no. 7, pp. 4940-4958, July 2015. Article (CrossRef Link)

[7] X Wu, Z Yan, C Ling and XG Xia, "A Physical-Layer Authentication Assisted Scheme for Enhancing 3GPP Authentication," *Mathematics*, 2015.(to be published)

[8] E Jorswieck, S Tomasin and A Sezgin, "Broadcasting Into the Uncertainty: Authentication and Confidentiality by Physical-Layer Processing," in *Proc. of the IEEE*, vol. 103, no. 10, pp. 1702-1724, October, 2015. Article (CrossRef Link)

[9] Kai Zeng, K Govindan and P Mohapatra, "Non-cryptographic authentication and identification in wireless networks," *Wireless Communications*, vol. 17, no. 5, pp. 56-62, October 2010. Article (CrossRef Link)

[10] N Patwari and S K Kasera, "Temporal link signature measurements for location distinction," *IEEE Transactions on Mobile Computing*, vol. 10, no. 3, pp. 449-462, March, 2011. Article (CrossRef Link)

[11] W C Jakes and D C Cox, "Microwave Mobile Communications," *New Jersey*, *Wiley-IEEE Press*, pp. 13-39, 1994. Article (CrossRef Link)

[12] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 733-742, May, 1993. Article (CrossRef Link)

[13] B. Li and Z. Fei, "Robust artificial noise-aided secure beamforming in wireless-powered non-regenerative relay networks," *IEEE Access*, vol. 4, pp. 7921-7929, November 2016. Article (CrossRef Link)

[14] Y Liu, H H Chen and L Wang, "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347-376, August 2016. Article (CrossRef Link)

[15] Liang Xiao, L J Greenstein, N B Mandayam and W Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2571-2579, July, 2008. Article (CrossRef Link)

[16] Liang Xiao, L J Greenstein, N B Mandayam and W Trappe, "Channel-Based Detection of Sybil Attacks in Wireless Networks," *IEEE Transactions on Wireless Communication*, vol. 4, no. 3, pp. 492-503, September, 2009. Article (CrossRef Link)

[17] P Baracca, N Laurenti and S Tomasin, "Physical Layer Authentication over MIMO Fading Wiretap Channels," *IEEE Transactions on Wireless Communications*, vol. 11, no. 7, pp. 2564-2573, July, 2012. Article (CrossRef Link)

[18] Dan Shan, Kai Zeng, Weidong Xiang and P Richardson, "PHY-CRAM: physical layer challenge-response authentication mechanism for wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1817-1827, September, 2013. Article (CrossRef Link)

[19] Xianru Du, Dan Shan, Kai Zeng and L Huie, "Physical layer challenge-response authentication in wireless networks with relay," in *Proc. of IEEE International Conference on Computer Communications*, pp. 1276-1284, April 27-May 2, 2014. Article (CrossRef Link)

[20] Xiaofu Wu and Yan Zhen, "Physical-layer authentication for multi-carrier transmission," *IEEE Communications Letters*, vol. 19, no. 1, pp. 74-77, January 2015. Article (CrossRef Link)

[21] Xinsheng Ji, Jing Yang, Kaizhi Huang and Ming Yi, "Physical layer Authentication Scheme Based on Hash Method," *Journal of Electronics and Information Technology*, vol. 38, no 11, pp. 2900-2907, July, 2016. Article (CrossRef Link)

[22] H Wen and P H Ho, "Physical layer technique to assist authentication based on PKI for vehicular communication networks," *KSII Transactions on Internet & Information Systems*, vol. 5, no. 2, pp. 440-456, February, 2011. Article (CrossRef Link)

[23] H Wen, Y Wang, X Zhu, J Li and L Zhou, "Physical layer assist authentication technique for smart meter system," *IET Communications*, vol. 7, no. 7, pp. 189-197, February, 2013. Article (CrossRef Link)

[24] H Wen, "Physical Layer Assisted Authentication for Distributed Ad Hoc Wireless Sensor Networks," *IET Information Security*, vol. 4, no. 4, pp. 390-396, December 2011. Article (CrossRef Link)

[25] L Lai, H E Gamal and H V Poor, "Authentication Over Noisy Channels," *Mathematics*, vol. 55, no. 2, pp. 906-916, February 2008. Article (CrossRef Link)

[26] F Zheng, Z Xiao, S Zhou, J Wang and L Huang, "Message Authentication over Noisy Channels," *Entropy*, vol. 17, no. 1, pp. 368-383, January 2015. Article (CrossRef Link)

[27] A Swaminathan, Yinian Mao and Min Wu, "Robust and secure image hashing," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 215-230, June, 2006. Article (CrossRef Link)

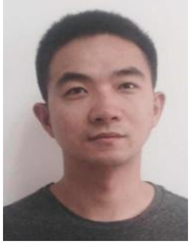
[28] N Goergen, T C Clancy and T R Newman, "Physical layer authentication watermarks through synthetic channel emulation," in *Proc. of IEEE Symposium on New Frontiers in Dynamic Spectrum*, pp. 1-7, April 6-9, 2010. Article (CrossRef Link)

[29] N Goergen, W S Lin, K J Liu and TC Clancy, "Authenticating MIMO transmissions using channel-like fingerprinting," in *Proc. of Global Telecommunications Conference*, pp. 1-6, December 6-10, 2010. Article (CrossRef Link)

[30] Ke LV, Guo-hua GENG and Ming-quan ZHOU, "Matchingof 3D Curve Based on the Hash Method," *Chinese Journal of Electronics*, vol. 31, no. 2, pp. 294-296, February, 2003. Article (CrossRef Link)

[31] M P C Fossorier and S Lin, "A unified method for evaluating the error-correction radius of reliability-based soft-decision algorithms for linear block codes," *IEEE Transactions on Information Theory*, vol. 44, no.2, pp. 691-700, March 1998. Article (CrossRef Link)

Jing Yang received her B.E. degree in Communication Engineering from Huazhong University of Science and Technology, Wuhan, Hubei, P.R.China in June 2013. She received her M.S. degree in National Digital Switching System Engineering & Technological R&D Center (NDSC). She is currently a Ph.D. candidate at NDSC. Her research interests include physical layer security, wireless communication.



Xinsheng Ji received the B.E. degree in Fudan University, Shanghai, China, in 1984, and received the M.S. degrees in PLA Information Engineering University, Zhengzhou, China, in 1991. He has been a faculty member of NDSC since 1988, where he is currently a professor and the chief engineer of NDSC. He has been a member of the Network and Communication (NaC) specialist group for China 863 High Technology Program and a senior member of China Institute of Communication. He was awarded as an outstanding expert of state in 2015. His major research interests include wireless communication network, security and signal processing. Email: jxs@mail.ndsc.com.cn

Kaizhi Huang received her B.E. degree in digital communication and M.S. degree in communication and information system from Information Engineering University, Zhengzhou, China, and Ph.D. degrees in communication and information system from Tsinghua University, Beijing, China, in 1995, 1998 and 2003 respectively. She has been a faculty member of NDSC since 1998, where she is currently a professor and director of the Laboratory of Mobile Communication Networks.

Ming Yi received the B.E. degree in PLA Information Engineering University, Zhengzhou, China. He then received the M.S. and Ph.D degrees in NDSC. He has been a faculty member of NDSC since 2012. His research interests include physical layer security, channel coding.

Yajun Chen received the B.E. and M.S. degrees in UESTC University and National Digital Switching System Engineering & Technological R&D Center, respectively. He is currently a Ph.D. candidate at NDSC, Zhengzhou, China. His research interests include physical layer security, wireless location and resource management in 5G networks.