Intelligent and Converged Networks ISSN 2708-6240
2023, 4(4): 355−365 DOI: 10.23919/ICN.2023.0029

Physical layer authentication of MIMO-STBC systems based on constellation dithering

Yongli An, Haifei Bai, Shikang Zhang, and Zhanlin Ji*

Abstract: Most of the existing physical layer watermarking authentication schemes are based on a single-input single-output system and require pre-issue of shared keys. To address these problems, in this thesis, a physical layer authentication scheme without the distribution keys is proposed based on the constellation dithering physical layer authentication watermarking mechanism with a multiple-input multiple-output (MIMO) system, and space-time block coding (STBC) is used to improve the robustness of transmission. Specifically, the legitimate node obtains channel state information (CSI) through channel probing and couples CSI with the message signal using a hash function to generate an authentication tag, which is then embedded through constellation dithering. The receiver extracts the tag and authenticates it using hypothesis testing. Performance analysis shows that the scheme is resistant to various attacks such as replay, interference, tampering, and forgery. Simulation results show that the use of MIMO multi-antenna diversity with STBC coding technique reduces the bit error rate (BER) of message signals and tag signals and improves the detection rate of legitimate signals.

Key words: constellation dithering; channel state information (CSI); hash function; MIMO-STBC; physical layer authentication

1 Introduction

With the rapid development and advancement of wireless devices, it has found applications in related fields such as medical, military, tracking, and surveillance. However, compared with wired communication, wireless communication is more challenging to secure the transmission due to its openness, where signals can be broadcast to every receiver. In terms of security, authentication is crucial in data confidentiality, and it is considered the first line of defense for communication security[1]. On the one hand, traditional authentication methods rely on cryptography and higher-level encryption, introducing high complexity and key management issues. On the other hand, physical layer authentication (PLA) using non-cryptographic methods overcomes the cryptographic aspects by exploiting the characteristics of the communication channel. Physical layer authentication offers many advantages over conventional authentication at the upper layers using cryptographic tools, including enhanced security by introducing uncertainty to the adversary and increased efficiency and compatibility by avoiding upper-layer operations[2]. In addition, the physical layer is considered an effective alternative to traditional key-based approaches due to its rich physical layer channel characteristics[3].

Currently, many studies are addressing physical layer authentication. Conventional physical layer authentication schemes require channel estimation and additional complex preprocessing such as demodulation and decoding to recover message symbols. Although there are many pre-processing schemes such as channel estimation[4], pre-processing should be avoided in the authentication process. In Ref. [5], new physical layer authentication was

• Yongli An, Haifei Bai, Shikang Zhang, and Zhanlin Ji are with College of Artificial Intelligence, North China University of Science and Technology, Tangshan 063210, China. E-mail: anyl@ncst.edu.cn;baihaifei2022@163.com;15127280221@163.com; zhanlin.ji@gmail.com.
* To whom correspondence should be addressed.
Manuscript received: 2023-05-30; accepted: 2023-09-04

proposed that overcomes the drawback of requiring preprocessing. Similarly, in Ref. [6], a method was proposed to realize the security authentication of physical layer without prior knowledge of signal and only it needs a short sequence of noise samples. As deep learning is increasingly studied in image processing, speech recognition, natural language processing, etc., the ability to introduce deep learning into wireless communication has grown significantly[7, 8]. Physical layer authentication in wireless communication sometimes requires receiving channel state information (CSI), which can be used to perform channel estimation using deep learning[9], and studies have shown that the performance of working with deep learning models is better. In addition, physical layer authentication based on CSI is susceptible to channel noise, which can be well solved using deep learning[10]. In addition, deep learning is also widely used in end-to-end communication[11, 12], which lays a foundation for the application of physical layer authentication to end-to-end communication. Physical layer security authentication based on deep learning can eliminate the need for key distribution and management by using channel characteristics as an endogenous security mechanism, which will not lead to additional computing overhead and communication delay. However, using deep learning requires a large amount of data for model training, which consumes a lot of resources[13]. Many current studies on physical layer authentication aim at improving authentication performance[14, 15], but most of these studies focus on the operation of new statistical models or algorithms for binary hypothesis testing, whose accuracy is highly dependent on the test threshold[16, 17]. Physical layer watermarking technology is to artificially add label signals to transmitted signals. This type of identity authentication mechanism regards noise as a favorable resource for identity authentication. By hiding authentication labels in noise, information theory security can be realized, and threshold free physical layer authentication can be realized[18, 19].

1.1 Related work

Most of the existing physical layer watermarking techniques add a watermark signal to the user signal, which is unencrypted and insufficiently secure. In Ref. [20], a well-designed watermark signal independent of the transmitter message signal is encrypted and embedded in the user signal. Also to improve the security of the watermark signal, a new watermarking scheme based on orthogonal frequency division multiplexing (OFDM) was proposed in Ref. [21], using Pseudo-User-Bit as the watermark generation parameter to ensure that different data frames are embedded with different watermark signals. However, since it is not changed during communication, the watermark signal can be easily detected by eavesdroppers. In Ref. [1], to make the watermark signal not easy to be detected, it is proposed to generate the watermark signal using random wireless channel gain between the communicating entities. Also, in Ref. [22], a scheme is proposed that can improve the authentication rate and tag confidentiality without incurring any additional requirements. In these schemes, the watermark signal interferes with the user signal, which reduces the signal-to-noise ratio (SNR) of the user signal, so the watermark can be embedded in the pilot frequency to eliminate the interference of the watermark[23]. In addition, Ref. [24] designs a physical layer watermark authentication scheme for large-scale Internet of Things (IoT) scenarios, which generates authentication tags using asymmetric keys, and weighted fractional Fourier transform, respectively. Especially for today's large-scale IoT scenarios, the dense population and increasing connectivity requirements may increase the load on the certified entity and increase the corresponding processing latency. To solve this problem, more and more reliable physical layer authentication algorithms are being developed for large-scale IoT systems[25, 26]. However, these schemes are based on single-input single-output (SISO) systems and require the distribution of shared keys. In multipath or mobile environments, the channel state fluctuates randomly due to fading. Recently, many studies have used the wireless channels of legitimate users as random sources to generate shared keys[27, 28], and these works provide lightweight solutions for large-scale, heterogeneous

wireless devices with limited computing power. Reference [29] utilizes channel impulse responses with message signals to generate authentication tags without the need to pre-issue shared keys. Similarly, Ref. [30] proposes a PLA scheme based on channel impulse response (CIR) that aims to achieve high authentication performance without knowing the attacker's previous channel information, and can be trained with a small amount of data even in complex environments. However, many physical layer authentication schemes are limited by quantization errors, local optimal values, and performance losses due to changes in the communication environment. References [31, 32] use the phase information of the channel to solve the limitations of the existing scheme. While these schemes perform well in SISO scenarios, their performance can be further improved by multiple-input multiple-output (MIMO). In Ref. [10], a physical layer authentication scheme based on distance features is proposed, which uses the characteristics of multi-input and multi-output channels in the beam space of millimeter wave network to resist spoofing attacks. In addition, the proposed multi-antenna device can not only improve the data transmission rate, and provide higher degrees of freedom, but also improve the accuracy and security of physical layer authentication[33].

1.2 Contributions

Most of these physical layer watermarking authentications mentioned above are being studied for tags, with little consideration of how the tags are embedded. Among the physical layer watermarking mechanisms, the most widely used watermarking addition scheme is the constellation dithering technique designed for constellation modulated signals. In this thesis, an authentication scheme is proposed for MIMO systems without distributing keys based on the watermark embedding method of constellation map dithering.

Specifically, the main contributions of this paper are as follows:

- In this thesis, the use of channel state information instead of pre-issue of shared keys to generate authentication tags can effectively reduce the burden of key distribution and management, and embed authentication tags using constellation dithering without additional transmission bandwidth.
- The use of MIMO to transmit diversity techniques with space-time block coding (STBC) can improve the robustness of the transmission data and authentication tags.
- The authentication performance of the system is analyzed using hypothesis testing theory, and the security analysis shows that the proposed authentication scheme can resist a variety of attack models.

Explanation of operation symbols: $(\cdot)^{\mathrm{T}}$, $(\cdot)^{*}$, and $(\cdot)^{\mathrm{H}}$ denote the transpose, conjugate, and transpose conjugate of the matrix, respectively. $X \sim CN(0, Y)$ denotes that the random variable X obeys the complex Gaussian random distribution with mean 0 and variance Y. $d^2(\cdot,\cdot)$ denotes the Euclidean distance between vectors, sign(·) is the sign function, and Re(·) and Im(·) functions can extract the real and imaginary parts of the complex numbers, respectively. $Q(\cdot)$ denotes the right-tail function of the standard normal distribution, χ_n^2 denotes that it obeys the chi-square distribution with degree of freedom n, and $\Gamma_{\chi_n^2}(\cdot)$ denotes the right-tail probability function of the chi-square distribution χ_n^2.

2 Constellation dithering and STBC coding

2.1 Constellation dithering

Constellation dithering is a common scheme of PLA watermarking mechanism, which is commonly used for quadrature phase shift keying (QPSK) signals. Figure 1 shows two methods of constellation dithering, one by rotating the constellation map angle to embed the authentication tag[34], and the other by shifting the constellation map position to embed the authentication tag[35]. Assuming that the QPSK signal is $s_n = a_n + jb_n$, constellation rotation (CR) scheme can be expressed as

$$x_n = (a_n + jb_n)\,\mathrm{e}^{-\mathrm{j}a_n b_n t_n \theta} = a_n(\cos\theta + t_n \sin\theta) + \mathrm{j}b_n(\cos\theta - t_n \sin\theta) \quad (1)$$

where $a_n = \pm 1$ and $b_n = \pm 1$ are the I and Q branches of

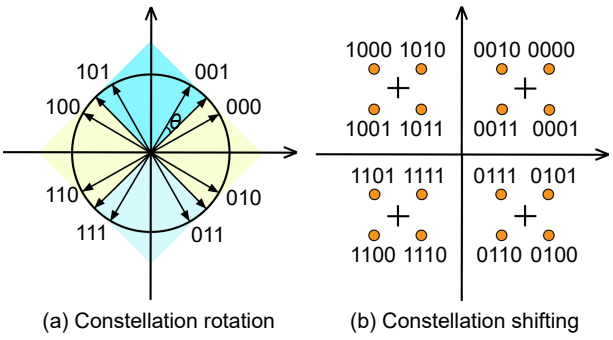


Fig. 1 Constellation dithering.

the QPSK signal, respectively, $t_n = \pm 1$ is the watermark tag bits, and θ is the rotation angle.

The constellation shifting (CS) scheme can be expressed as

$$x_n = a_n\left(\sqrt{1-\alpha} + \sqrt{\alpha}t_n^{\mathrm{I}}\right) + \mathrm{j}b_n\left(\sqrt{1-\alpha} + \sqrt{\alpha}t_n^{\mathrm{Q}}\right) \tag{2}$$

where $1-\alpha$ and α are the power distribution of the original signal and the tag signal. t_n^{I} and t_n^{Q} are the I and Q branches of the complex tag signal t_n, respectively.

2.2 STBC coding

STBC coding is a technique of physical layer diversity that resists channel fading by transmitting multiple copies of the transmission signal to improve the robustness of data transmission. STBC uses coding theory, matrix algebra, and signal processing to process the input information block to produce the symbols and output of the matrix, whose rows and columns represent the antenna and time slot, respectively. The STBC coding matrix $\boldsymbol{X}$ can be expressed as

$$\boldsymbol{X} = \begin{bmatrix} x_{11}, & x_{12}, & \cdots, & x_{1N_{\mathrm{T}}} \\ x_{21}, & x_{22}, & \cdots, & x_{2N_{\mathrm{T}}} \\ \vdots & \vdots & & \vdots \\ x_{i1}, & x_{i2}, & \cdots, & x_{iN_{\mathrm{T}}} \end{bmatrix} \tag{3}$$

where N_{T} is the number of transmitting antennas and i is the number of transmitting time slots. Then the receiving signal at time slot k can be expressed as

$$\boldsymbol{Y}_{(k)} = \boldsymbol{H}\boldsymbol{X}_{(k)}^{\mathrm{T}} + \boldsymbol{V} \tag{4}$$

where $\boldsymbol{Y}_{(k)} = \left[y_{k1}, y_{k2}, \ldots, y_{kN_{\mathrm{R}}}\right]^{\mathrm{T}}$ and $\boldsymbol{H}$ are the channel matrices of $N_{\mathrm{R}} \times N_{\mathrm{T}}$, and N_{R} is the number of the receiving antennas. The channel model in this thesis is Rayleigh block fading channel, $\boldsymbol{H}$ obeys complex Gaussian random process, $h_i \sim CN(0, \delta_h^2)$. $\boldsymbol{V} = \left[v_1, v_2, \ldots, v_{N_{\mathrm{T}}}\right]^{\mathrm{T}}$ is complex Gaussian channel noise, $v_i \sim CN(0, \sigma_v^2)$.

Alamouti coding is a special coding scheme in STBC. In this thesis, the modulated signal s_n is embedded in the authentication tag through constellation map dithering, then Alamouti coding is performed and finally sent through the transmitting antenna. As shown in Fig. 2, the Alamouti scheme has 2 transmitting antennas and 1 receiving antenna. At time slot 1, x_1 and x_2 are sent by antenna 1 and antenna 2, respectively, and at time slot 2, antennas 1 and 2 transmit $-x_2^*$ and x_1^*, respectively. h_1 and h_2 are channel gains, then the receiving signal at the receiver can be expressed as

$$\begin{cases} y_1 = h_1 x_1 + h_2 x_2 + v_1, \\ y_2 = -h_1 x_2^* + h_2 x_1^* + v_2 \end{cases} \tag{5}$$

STBC can reduce the decoding complexity by orthogonal or quasi-orthogonal coding. The receiver requires only simple and linear processing to achieve maximum likelihood decoding. For multiple phase shift keying (M-PSK) modulation, the receiver performs maximum likelihood decoding to obtain

$$\begin{cases} \hat{s}_1 = \arg\min\limits_{\hat{s}_1 \in S}\left\{d^2(\hat{x}_1, \hat{s}_1)\right\}, \\ \hat{s}_2 = \arg\min\limits_{\hat{s}_2 \in S}\left\{d^2(\hat{x}_2, \hat{s}_2)\right\} \end{cases} \tag{6}$$

where

$$\begin{cases} \hat{x}_1 = \left(h_1^* y_1 + h_2 y_2^*\right) / \left(h_1^2 + h_2^2\right), \\ \hat{x}_2 = \left(h_1^* y_2 - h_2 y_1^*\right) / \left(h_1^2 + h_2^2\right) \end{cases} \tag{7}$$

$\hat{x}_1$ and $\hat{x}_2$ contain not only the channel noise but also the authentication tag. The estimated value of the message signal can be expressed as

$$\hat{s}_n = \mathrm{sign}\left(\mathrm{Re}\left[\hat{x}_n\right]\right) + \mathrm{sign}\left(\mathrm{Im}\left[\hat{x}_n\right]\right)\mathrm{j} \tag{8}$$

Usually, the embedded tag signal and noise are considered interference. Assuming that the message bit

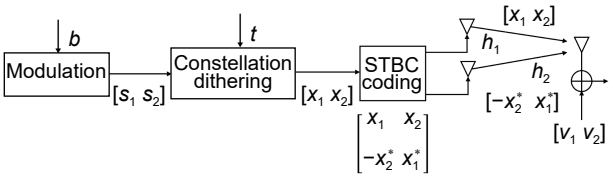


Fig. 2 Alamouti coding.

error rates (MBER) of the CR scheme and CS scheme are $P^{s}_{\mathrm{e,CR}}$ and $P^{s}_{\mathrm{e,CS}}$, respectively, then

$$P^{s}_{\mathrm{e,CR}}=\frac{1}{2}Q(\sqrt{\delta}(\cos\theta+\sin\theta))+\frac{1}{2}Q(\sqrt{\delta}(\cos\theta-\sin\theta)) \tag{9}$$

$$P^{s}_{\mathrm{e,CS}}=\frac{1}{2}Q(\sqrt{\delta}(\sqrt{1-\alpha}+\sqrt{\alpha}))+\frac{1}{2}Q(\sqrt{\delta}(\sqrt{1-\alpha}-\sqrt{\alpha})) \tag{10}$$

where δ is the SNR. The tag signal is also decoded by maximum likelihood, whereas in the CR scheme,

$$\hat{t}_n=\mathrm{sign}\left((\mathrm{Re}[x_n])^2-(\mathrm{Im}[x_n])^2\right) \tag{11}$$

In the CS scheme,

$$\begin{cases}\hat{t}^{\mathrm{I}}_n=\mathrm{sign}\left(|\mathrm{Re}[x_n]|-\sqrt{1-\alpha}\right),\\ \hat{t}^{\mathrm{Q}}_n=\mathrm{sign}\left(|\mathrm{Im}[x_n]|-\sqrt{1-\alpha}\right)\end{cases} \tag{12}$$

Assuming that the tag bit error rates (TBER) of the CR and CS schemes are $P^{t}_{\mathrm{e,CR}}$ and $P^{t}_{\mathrm{e,CS}}$, respectively, then

$$P^{t}_{\mathrm{e,CR}}=Q(\sqrt{2\delta}\sin\theta)+Q(\sqrt{2\delta}\cos\theta)-2Q(\sqrt{2\delta}\sin\theta)Q(\sqrt{2\delta}\cos\theta) \tag{13}$$

$$P^{t}_{\mathrm{e,CS}}=Q(\sqrt{\alpha\sigma})+\frac{1}{2}Q(\sqrt{\sigma}(2\sqrt{1-\alpha}-\sqrt{\alpha}))-\frac{1}{2}Q(\sqrt{\delta}(2\sqrt{1-\alpha}+\sqrt{\alpha})) \tag{14}$$

3 Authentication scheme

PLA mainly includes identity authentication and message authentication. Identity authentication mainly verifies the identity legitimacy of the sender, with the purpose of receiving the information of the legitimate sender and rejecting the information sent by the illegal sender. Message authentication is designed to protect data integrity from attacks such as deletion, tampering, and forgery. In this thesis, the proposed scheme mainly verifies message integrity. As shown in Fig. 3, Bob (the legitimate sender) sends the identity and detection signal to Alice, the legitimate receiver, using a highly directed beam. After verifying Bob's legal identity, Alice performs channel estimation, obtains the CSI between Alice and Bob, and uses the estimated CSI to generate the private sequence $\boldsymbol{H}$. Alice uses the hash

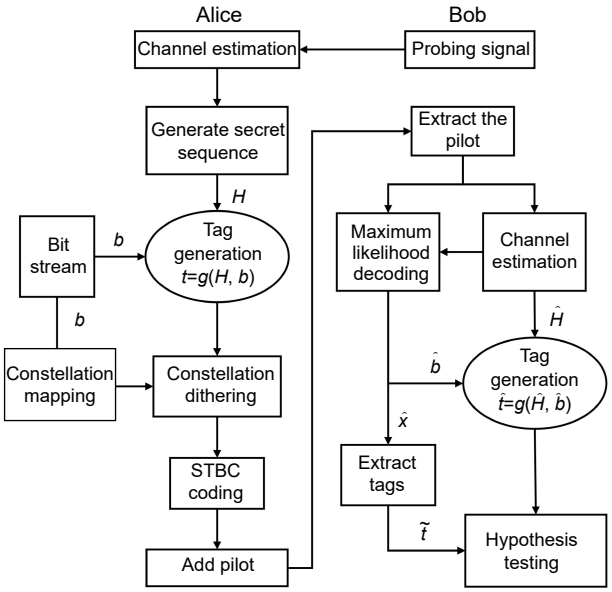


Fig. 3 Authentication framework.

function $g(\cdot)$ to couple the private sequence $\boldsymbol{H}$ with the input bit stream $\boldsymbol{b}$ to generate the authentication tag $\boldsymbol{t}$. By means of constellation dithering, the authentication label is embedded into the message signal to be sent to get the mark signal containing the label. Bob receives the signal and performs channel estimation and decoding, generates tag $\hat{\boldsymbol{t}}$ and extracted tag $\tilde{\boldsymbol{t}}$ using estimated signal $\hat{\boldsymbol{b}}$, modulated symbols, and private sequence $\hat{\boldsymbol{H}}$, then extracts residual $\boldsymbol{z}$ and finally authenticates using hypothesis testing.

3.1 Tag generation and embedding

Based on the short-time reciprocity of the wireless channel, by estimating the channel in channel coherence time, Alice and Bob can obtain consistent or highly similar CSI. Assuming that the probe signal is p, the received signal is y_p. Then, linear minimum mean square error (LMMSE) algorithm is utilized to estimate the channel,

$$\hat{\boldsymbol{h}}=R_{\boldsymbol{hh}}\left(R_{\boldsymbol{hh}}+\sigma_n^2 I\right)^{-1}\boldsymbol{h}_{\mathrm{ls}} \tag{15}$$

$$\boldsymbol{h}_{\mathrm{ls}}=y_p\frac{1}{|p|^2}p^{\mathrm{H}} \tag{16}$$

where $R_{\boldsymbol{hh}}$ is the channel autocorrelation matrix and $\boldsymbol{h}_{\mathrm{ls}}$ is the channel least squares channel estimate. Alice first preprocesses the detected signal with wavelet denoising, which can reduce the influence of channel noise, then performs channel estimation and performs

four-level uniform quantization for the mode value $|\hat{\boldsymbol{h}}|$ of channel estimation. Then the quantized values is gray encoded. To further reduce the differences in channel estimates between Alice and Bob and the effects of wireless channel fading and noise. Finally, the encoding sequence is mapped to the private sequence $\boldsymbol{H}$. Alice generates the authentication tag from the private sequence $\boldsymbol{H}$ to the input bitstream $\boldsymbol{b}$ using a hash function,

$$\boldsymbol{t} = g(\boldsymbol{H}, \boldsymbol{b}) \tag{17}$$

The authentication tag is then embedded into the message signal through constellation dithering and the pilot frequency is added, which is finally sent to the receiver.

3.2 Tag generation and extraction

After channel estimation, Bob uses the same algorithm as Alice to generate the private sequence $\hat{\boldsymbol{H}}$ and obtains $\hat{\boldsymbol{x}}$ and $\hat{\boldsymbol{b}}$ by maximum likelihood decoding. Bob uses the hash function to generate the tag $\hat{\boldsymbol{t}} = g(\hat{\boldsymbol{H}}, \hat{\boldsymbol{b}})$. It is assumed that the power allocation of the message signal and the tag signal are ρ_s^2 and ρ_t^2, $\rho_s^2 + \rho_t^2 = 1$, respectively. For the CR scheme, $\rho_s = \cos\theta$ and $\rho_t = \sin\theta$. For the CS scheme, $\rho_s = \sqrt{1-\alpha}$ and $\rho_t = \sqrt{\alpha}$. Bob uses the receiving signal $\hat{\boldsymbol{x}}$ and $\hat{\boldsymbol{b}}$ to extract the tag

$$\tilde{\boldsymbol{t}}_n = \hat{\boldsymbol{x}}_n - \rho_s f_e\left(\hat{\boldsymbol{b}}_n\right) \tag{18}$$

where $\tilde{\boldsymbol{t}}_n$ is the actual observed value of the tag extracted by Bob and $f_e(\cdot)$ is the QPSK encoding function.

3.3 Hypothesis testing authentication

Bob extracts the residual $\boldsymbol{z}$ of the tag estimate $\hat{\boldsymbol{t}}$ and the tag observation $\tilde{\boldsymbol{t}}$. For the CR scheme,

$$\boldsymbol{z} = \tilde{\boldsymbol{t}} - \rho_t \cdot \boldsymbol{s}^* \hat{\boldsymbol{t}} \tag{19}$$

In the CS scheme,

$$\boldsymbol{z} = \tilde{\boldsymbol{t}} - \rho_t \cdot (\mathrm{Re}(\boldsymbol{s})\mathrm{Re}(\hat{\boldsymbol{t}}) + \mathrm{jIm}(\boldsymbol{s})\mathrm{Im}(\hat{\boldsymbol{t}})) \tag{20}$$

then it is authenticated with test function $\ell(\boldsymbol{z})$,

$$\ell(\boldsymbol{z}) \triangleq \boldsymbol{z}\boldsymbol{z}^{\mathrm{H}} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} \tau \tag{21}$$

$$\begin{cases} \mathcal{H}_0 : \text{Authentic}, \\ \mathcal{H}_1 : \text{Unauthentic} \end{cases} \tag{22}$$

where $\ell(\boldsymbol{z})$ is the sufficient statistic, $\boldsymbol{z}$ is the residual, and τ is the judgment threshold. The residual $\boldsymbol{z}$ contains not only the channel noise but also the tag difference between Alice and Bob. Assuming that the tag difference between Alice and Bob is $\Delta\boldsymbol{t}\Delta\boldsymbol{t}^{\mathrm{H}}$. When $\boldsymbol{t} = \hat{\boldsymbol{t}}$, $\Delta\boldsymbol{t}\Delta\boldsymbol{t}^{\mathrm{H}} = \boldsymbol{o}$. At this time $\boldsymbol{z}_n \sim CN\left(0, \frac{1}{\sigma}\right)$. Let $\alpha = \frac{1}{2\sigma}$, then $\frac{\ell(\boldsymbol{z})}{\alpha} \sim \chi^2_{2L}$ where L is the tag length. When $\boldsymbol{t} \neq \hat{\boldsymbol{t}}$, $\frac{\ell(\boldsymbol{z}) - \Delta\boldsymbol{t}\Delta\boldsymbol{t}^{\mathrm{H}}}{\alpha} \sim \chi^2_{2L}$.

In Formulas (21) and (22), hypothesis testing is used for authentication, which also introduces two types of unavoidable errors. One is the false alarm rate (i.e., the probability that Bob rejects a normal signal), denoted as P_{FA}, and the other is the missed detection rate (i.e., the probability that Bob accepts an illegal signal), denoted as P_{MD}. P_{FA} and P_{MD} can be expressed as

$$P_{\mathrm{FA}} = p\{\ell(\boldsymbol{z}) > \tau \mid \mathcal{H}_0\} = 1 - \Gamma_{\chi^2_{2L}}\left(\frac{\tau}{\alpha}\right) \tag{23}$$

$$P_{\mathrm{MD}} = p\{\ell(\boldsymbol{z}) < \tau \mid \mathcal{H}_1\} = \Gamma_{\chi^2_{2L}}\left(\frac{\tau - \Delta\boldsymbol{t}\Delta\boldsymbol{t}^{\mathrm{H}}}{\alpha}\right) \tag{24}$$

4 Performance analysis

4.1 Authentication performance

The authentication performance of the scheme in this thesis is described by the detection rate P_{D} of Alice for legitimate signals in the absence of interference, $P_{\mathrm{D}} = p\{\ell(\boldsymbol{z}) < \tau\}$. From Formulas (21) and (23), it can be seen that the main factors affecting the detection rate are the setting of the judgment threshold τ and the length of the authentication tag L. Usually, the higher the τ, the higher the detection rate is for a fixed tag length. But increasing the judgment threshold τ will lead to an increase in the missed detection rate P_{MD}, which will reduce the system security.

The MIMO-STBC technique used in this thesis can improve the authentication detection rate without increasing threshold τ. As shown in Fig. 4, the detection rate increases with the increase of SNR when the tag length L is 64 bits, τ = 25. In the CR scheme, the detection rate increases with a larger constellation map rotation angle for the same SNR, and in the CS scheme, the detection rate increases with a larger constellation map shifting amplitude. The MIMO-

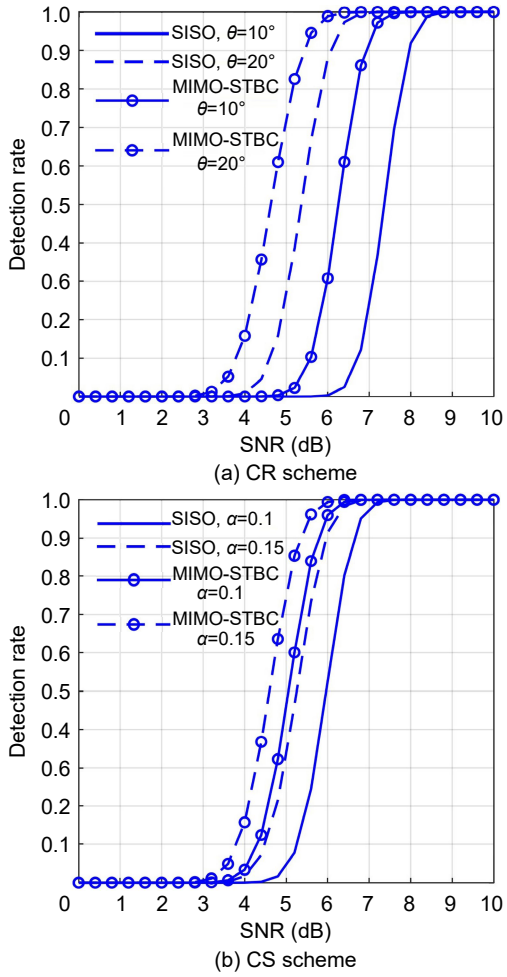


Fig. 4 Detection rate under different SNR.

STBC multiple antenna diversity techniques improve the detection rate for both schemes. In addition, Fig. 4 shows that the detection rate curve decreases rapidly with the decrease of SNR after a certain threshold value. Therefore, the MIMO-STBC multiple antenna diversity techniques are more advantageous in the low SNR environment.

4.2 Robustness

A robust authentication scheme should be able to withstand the effects of channel and noise and can continue the authentication process in the midst of interference. Because the receiver generates the tag using an estimate of the channel with the symbols, the accuracy of the estimated parameters is critical. In general, increasing the average power of the transmitting signal (i.e., increasing the SNR) can improve the robustness of the system.

As shown in Fig. 5, the MBER of CR and CS

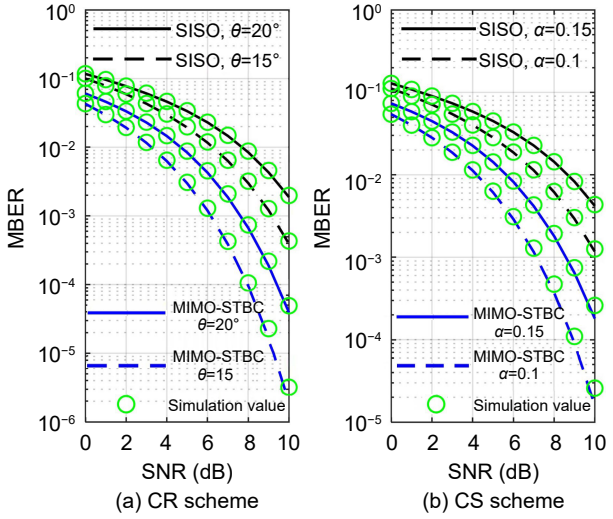


Fig. 5 MBER under different SNR.

schemes decreases with the increase of SNR, and the smaller the constellation rotation angle, the lower the MBER for the CR scheme, and the smaller the constellation shifting amplitude, the lower the MBER for the CS scheme. The BER performance of both schemes is significantly improved by using MIMO-STBC multiple antenna diversity. The MBER of MIMO-STBC coding is close to 1×10^{-6} when SNR = 10 dB, the rotation angle of is 15° in the CR scheme, and 1×10^{-5} when SNR = 10 dB, $\alpha=0.1$ in the CS scheme, which shows that the scheme of this thesis has a higher robust performance.

Figure 6 shows the TBER for different SNRs, and the TBER decreases with the increase of SNR. The use of MIMO-STBC coding significantly reduces the BER of both schemes. In the CR scheme, in contrast to MBER, TBER decreases with the increase of the constellation rotation angle. In the CS scheme, the larger the constellation shifting magnitude, the lower the TBER. It can be seen from Fig. 6 that after MIMO diversity and STBC coding are adopted, the TBER of CR scheme and CS scheme can be reduced simultaneously without increasing the label power. This result also proves that MIMO-STBC systems can transmit at lower tag power compared to SISO systems at the same TBER. Therefore, in MIMO-STBC system, the label power can be reduced by increasing antenna diversity to improve the concealability of the label signal without reducing the robustness of the label signal.

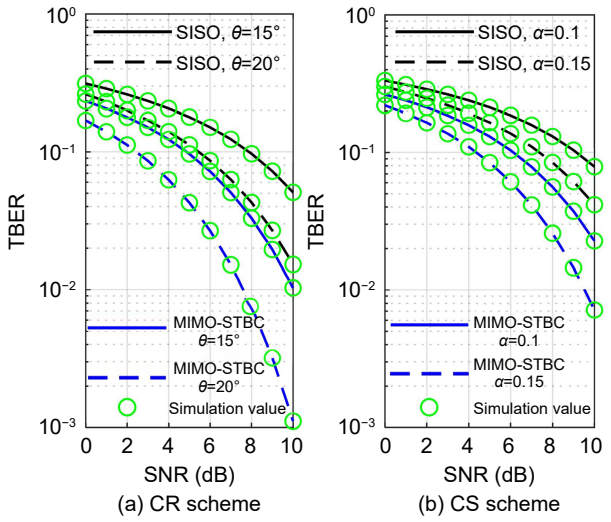


Fig. 6 TBER under different SNR.

It is worth noting that the robustness of the message signal versus the label signal is always carefully weighed during the physical layer authentication process. Figure 7 describes the changes of TBER of SISO and MIMO-STBC systems and CR and CS schemes with MBER when SNR = 15 dB. It can be found that as MBER increases, TBER decreases. Under the same SNR and MBER, CS scheme has lower TBER and better robustness than CR scheme. At the same time, compared with CR scheme, CS scheme can embed more label bits. This proves the excellent performance of CS scheme. Compared with SISO systems, MIMO-STBC systems have lower TBER under the same MBER. When TBER is the same, MIMO-STBC systems have lower MBER. The simulation results show that the MIMO-STBC system can improve the robustness of message and tag and the concealability of tag signal without affecting the authentication security.

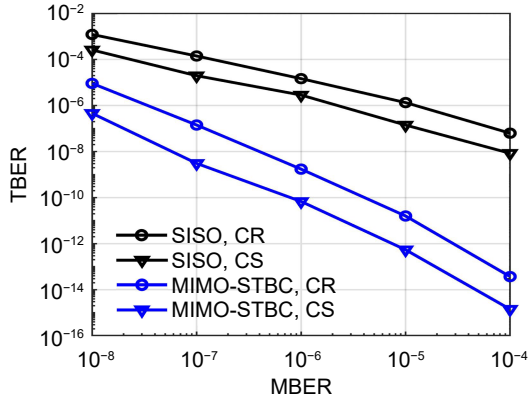


Fig. 7 Message and label error performance comparison.

4.3 Security

This section discusses several attacks by attacker Eve and the security performance of the proposed scheme under different attack models. The following four attack models are considered in the work of this thesis.

- **Replay attacks**. Eve intercepts the transmitting signal from Alice at a certain moment and launches a replay attack on Bob in expectation of passing the authentication, thus disrupting the communication by affecting the normal reception of the signal by Bob. Because the wireless channel has time-varying characteristics, the tag signal embedded into the modulated message signal will change over time, so Bob will reject the outdated tag signal.
- **Detection attacks**. It is assumed that Eve tries to detect the authentication tag and then removes or destroys the tag making Bob unable to authenticate the message accurately. In this thesis, low-power tag embedding is used to mask the tags using noise. Figure 6 shows that the lower the power of the embedded tags, the higher the TBER. The low-power tag signal has essentially no perceptible effect on the message signal, so it is difficult for an attacker to detect the authentication tag with a normal distribution of surrounding noise.
- **Tampering attacks**. It is assumed that Eve fully masters the tag embedding algorithm of Alice and then uses the same method as Alice to extract the tag. Eve tampers with the message signal and embeds the extracted authentication tag signal into the tampered message signal and sends it to Alice in expectation of passing authentication. Since Alice uses the message signal with CSI to generate the authentication tag, tampering with the message signal causes an error in the generation of the tag by Alice, i.e., $\boldsymbol{t} \neq \hat{\boldsymbol{t}}$. Since a hash function is used in this thesis to generate the authentication tag, even if there is a 1-bit error in the input, a completely different result will be obtained. It can be seen from Eq. (24) that the success rate of the attack by Eve is lower when $\Delta \boldsymbol{t} \Delta \boldsymbol{t}^{\mathrm{H}}$ is larger.
- **Forgery attacks**. Eve tries to create her own

message signal with tags to try to pass Bob's authentication. Although Eve can create her own message signal, she cannot obtain the CSI with the legitimate node and thus cannot obtain the private sequence $\boldsymbol{H}$. Eve can only forge channel characteristics by learning imitation. Due to the randomness and time-varying nature of the wireless channel, Eve cannot generate an authentication tag consistent with Bob's. The larger the error of Eve's forged authentication tag, i.e., the larger the $\Delta \boldsymbol{t}\Delta \boldsymbol{t}^{\mathrm{H}}$, the lower the success rate of Eve's attack.

5 Conclusion

Based on the physical layer security authentication watermark mechanism of constellation dithering with the MIMO system, a physical layer security authentication scheme is proposed in this thesis, which uses channel characteristics to generate authentication tags. Instead of distributing keys, the scheme generates shared private sequences based on the uniqueness, location distinction, time-varying, and hard-to-imitate characteristics of the legitimate node channels, and uses hash algorithms to generate authentication tags. In this thesis, the STBC diversity technique is used to improve the robustness of the transmission data and the authentication tag, and the authentication performance of the proposed scheme is analyzed using hypothesis testing theory. The simulation results show that the use of the MIMO-STBC multiple antenna diversity techniques significantly reduces the BER of the message and tag signals and improves the detection rate of the system. The security analysis shows that the proposed scheme resists a variety of attacks such as replay, interference, tampering, and forgery.

Acknowledgment

This work was supported by the National Key Research and Development Program of China (No. 2017YFE0135700), the High Level Talent Support Project of Hebei Province (No. A201903011), the Natural Science Foundation of Hebei Province (No. F2018209358), the Tsinghua Precision Medicine Foundation (No. 2022TS003), the Ministry of Education and Science (MES) for NCDSC, part of the Bulgarian National Roadmap on RIs (No. D01-387/18.12.2020), and the Telecommunications Research Centre (TRC) of University of Limerick, Ireland.

References

[1] Y. Ran, H. Al-Shwaily, C. Tang, G. Y. Tian, and M. Johnston, Physical layer authentication scheme with channel based tag padding sequence, *IET Commun.*, vol. 13, no. 12, pp. 1776–1780, 2019.

[2] N. Xie and S. Zhang, Blind authentication at the physical layer under time-varying fading channels, *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1465–1479, 2018.

[3] Y. Chen, P-H. Ho, H. Wen, S. Y. Chang, and S. Real, On physical-layer authentication via online transfer learning, *IEEE Internet Things J.*, vol. 9, no. 2, pp. 1374–1385, 2022.

[4] Y. An, J. Yue, L. Chen, and Z. Ji, Channel estimation for one-bit massive MIMO based on improved CGAN, *J. Commun. Inf. Netw.*, vol. 7, no. 2, pp. 214–220, 2022.

[5] N. Xie and C. Chen, Slope authentication at the physical layer, *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 6, pp. 1579–1594, 2018.

[6] X. Xie and Z. Xu, Blind watermark detection based on K-S test in radio-frequency signals, *Electron. Lett.*, vol. 56, no. 1, pp. 30–32, 2020.

[7] L. Alhoraibi, D. Alghazzawi, R. Alhebshi, and O. B. J. Rabie, Physical layer authentication in wireless networks-based machine learning approaches, *Sensors*, vol. 23, no. 4, p. 1814, 2023.

[8] H. Fang, X. Wang, and L. Xu, Fuzzy learning for multi-dimensional adaptive physical layer authentication: A compact and robust approach, *IEEE Trans. Wirel. Commun.*, vol. 19, no. 8, pp. 5420–5432, 2020.

[9] B. Lin, X. Wang, W. Yuan, and N. Wu, A novel OFDM autoencoder featuring CNN-based channel estimation for Internet of vessels, *IEEE Internet Things J.*, vol. 7, no. 8, pp. 7601–7611, 2020.

[10] S. Wang, K. Huang, X. Xu, Z. Zhong, and Y. Zhou, CSI-based physical layer authentication via deep learning, *IEEE Wirel. Commun. Lett.*, vol. 11, no. 8, pp. 1748–1752, 2022.

[11] Y. An, S. Wang, L. Zhao, Z. Ji, and I. Ganchev, A learning-based end-to-end wireless communication system utilizing a deep neural network channel module, *IEEE Access*, vol. 11, pp. 17441–17453, 2023.

[12] Y. An, M. Wang, L. Chen, and Z. Ji, DCGAN-based symmetric encryption end-to-end communication systems, *AEU Int. J. Electron. Commun.*, vol. 154, p. 154297, 2022.

[13] X. Qiu, Z. Du, and X. Sun, Artificial intelligence-based security authentication: Applications in wireless

multimedia networks, *IEEE Access*, vol. 7, pp. 172004–172011, 2019.

[14] L. Afeef, H. M. Furqan, and H. Arslan, Physical layer authentication scheme in beamspace MIMO systems, *IEEE Commun. Lett.*, vol. 26, no. 7, pp. 1484–1488, 2022.

[15] M. Abdrabou and T. A. Gulliver, Adaptive physical layer authentication using machine learning with antenna diversity, *IEEE Trans. Commun.*, vol. 70, no. 10, pp. 6604–6614, 2022.

[16] F. Pan, Z. Pang, H. Wen, M. Luvisotto, M. Xiao, R. F. Liao, and J. Chen, Threshold-free physical layer authentication based on machine learning for industrial wireless CPS, *IEEE Trans. Ind. Inform.*, vol. 15, no. 12, pp. 6481–6491, 2019.

[17] H. Fang, X. Wang, and L. Hanzo, Learning-aided physical layer authentication as an intelligent process, *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2260–2273, 2018.

[18] J. B. Perazzone, P. L. Yu, B. M. Sadler, and R. S. Blum, Artificial noise-aided MIMO physical layer authentication with imperfect CSI, *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 2173–2185, 2021.

[19] N. Xie, W. Xiong, M. Sha, T. Hu, P. Zhang, L. Huang, and D. Niyato, Physical layer authentication with high compatibility using an encoding approach, *IEEE Trans. Commun.*, vol. 70, no. 12, pp. 8270–8285, 2022.

[20] P. Zhang, J. Liu, Y. Shen, H. Li, and X. Jiang, Lightweight tag-based PHY-layer authentication for IoT devices in smart cities, *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3977–3990, 2020.

[21] X. Xie, W. Chen, and Z. Xu, A physical-layer watermarking scheme based on 5G NR, *Electronics*, vol. 11, no. 19, pp. 3184, 2022.

[22] M. Qaisi, S. Althunibat, and M. Qaraqe, Phase-assisted dynamic tag-embedding message authentication for IoT networks, *IEEE Internet Things J.*, vol. 9, no. 20, p. 20620–20629, 2022.

[23] N. Xie and Y. Chen, Pilot-based physical-layer authentication with high covertness, *IEEE Wirel. Commun.*, vol. 28, no. 1, pp. 97–103, 2021.

[24] N. Zhang, X. Fang, Y. Wang, S. Wu, H. Wu, D. Kar, and H. Zhang, Physical-layer authentication for Internet of Things via WFRFT-based Gaussian tag embedding, *IEEE Internet Things J.*, vol. 7, no. 9, pp. 9001–9010, 2020.

[25] Y. Wang, J. Jin, Y. Li, and C. Choi, A reliable physical layer authentication algorithm for massive IoT systems, *IEEE Access*, vol. 8, pp. 80684–80690, 2020.

[26] S. Han, Y. Lee, J. Choi, and E. Hwang, Lightweight physical layer aided key agreement and authentication for the Internet of Things, *Electronics*, vol. 10, no. 14, p. 1730, 2021.

[27] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, Physical layer security for the Internet of Things: Authentication and key generation, *IEEE Wirel. Commun.*, vol. 26, no. 5, pp. 92–98, 2019.

[28] L. Jiao, N. Wang, P. Wang, A. Alipour-Fanid, J. Tang, and K. Zeng, Physical layer key generation in 5G wireless networks, *IEEE Wirel. Commun.*, vol. 26, no. 5, pp. 48–54, 2019.

[29] Y. An, S. Zhang, and Z. Ji, A tag-based PHY-layer authentication scheme without key distribution, *IEEE Access*, vol. 9, pp. 85947–85955, 2021.

[30] R. Meng, X. Xu, B. Wang, H. Sun, S. Xia, S. Han, and P. Zhang, Physical-layer authentication based on hierarchical variational autoencoder for industrial Internet of Things, *IEEE Internet Things J.*, vol. 10, no. 3, pp. 2528–2544, 2023.

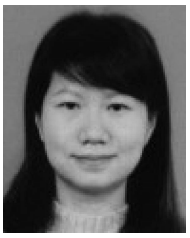
[31] X. Lu, J. Lei, Y. Shi, and W. Li, Improved physical layer authentication scheme based on wireless channel phase, *IEEE Wirel. Commun. Lett.*, vol. 11, no. 1, pp. 198–202, 2022.

[32] N. Xie, W. Xiong, J. Chen, P. Zhang, L. Huang, and J. Su, Multiple phase noises physical-layer authentication, *IEEE Trans. Commun.*, vol. 70, no. 9, pp. 6196–6211, 2022.

[33] H. Forssell and R. Thobaben, Worst-case detection performance for distributed SIMO physical layer authentication, *IEEE Trans. Commun.*, vol. 70, no. 1, pp. 485–499, 2022.

[34] T. Jiang, H. Zeng, Q. Yan, W. Lou, and Y. T. Hou, On the limitation of embedding cryptographic signature for primary transmitter authentication, *IEEE Wirel. Commun. Lett.*, vol. 1, no. 4, pp. 324–327, 2012.

[35] Z. Xu and W. Yuan, Watermark BER and channel capacity analysis for QPSK-based RF watermarking by constellation dithering in AWGN channel, *IEEE Signal Process. Lett.*, vol. 24, no. 7, pp. 1068–1072, 2017.



Yongli An received the PhD degree in information science from Beijing Jiaotong University, China in 2015. She is a professor at the North China University of Science and Technology, China. Her current research interests include wireless network security, interference cancellation technology, and large-scale MIMO technology.

Haifei Bai is currently a master student at the Department of Information and Communication Engineering, North China University of Science and Technology, China. His current research interests include wireless network security and physical layer security authentication.

Shikang Zhang is currently a master student at the Department of Information and Communication Engineering, North China University of Science and Technology, China. His current research interests include wireless network security and physical layer security authentication.

Zhanlin Ji received the MEng degree from Dublin City University, Ireland in 2006, and the PhD degree from the University of Limerick, Ireland in 2010. He is currently a professor with the North China University of Science and Technology, China, and a researcher with the Telecommunications Research Centre (TRC), University of Limerick, Ireland. He has authored/coauthored 100 research articles in refereed journals and conference papers. His research interests include Ubiquitous Consumer Wireless World (UCWW), the Internet of Things (IoT), cloud computing, big data management, and data mining.