Hindawi
Journal of Sensors
Volume 2021, Article ID 7022297, 11 pages
https://doi.org/10.1155/2021/7022297

Research Article

Secure Physical Layer Transmission and Authentication Mechanism Based on Compressed Sensing of Multiple Antenna Arrays

Xiaolong Zhang,[1,2] **Wei Wu**,[1] **and Bin Zhou**[2]

[1]*The 54th Research Institute of China Electronics Technology Group Corporation, Shijiazhuang 050002, China*
[2]*China Academic of Electronics and Information Technology, Beijing 100041, China*

Correspondence should be addressed to Xiaolong Zhang; xlzhang@bupt.edu.cn

Received 13 September 2021; Accepted 15 October 2021; Published 10 November 2021

Academic Editor: Guolong Shi

Large-scale antenna technology has become one of the most promising technologies in 5G because of its ability to effectively improve the spectral efficiency and energy efficiency of the system, as well as its better robustness. In this paper, a large amount of CSI (channel state information) data is characterized by feature mining and law analysis, and a large number of channel characteristics of the physical layer have the advantages of randomness and uniqueness, etc. From the perspective of improving the security of the authentication mechanism and reducing the computational complexity of the authentication mechanism, the physical layer security authentication model is analyzed, and the signal security transmission path, signal authenticity, and channel estimation are used to propose an effective physical layer secure transmission and authentication mechanism, which can be used as a security enhancement and lightweight authentication mechanism for existing authentication mechanisms. In this paper, we analyze the security advantage mechanism of physical layer authentication and prove the security performance boundary; propose an authentication security enhancement method based on the channel feature generation key, a message authentication method based on superimposed tag signals; and propose a method based on private guide frequency for high-speed service data authentication.

1. Introduction

While mobile communication technology is advancing by leaps and bounds, the importance of security is becoming increasingly prominent. The content of the communication may be eavesdropped; sensitive information such as identity and location can be leaked; communication services can be interfered with or abused, making the quality of service not guaranteed or even denied; and the widespread use of smart terminals, viruses, Trojan horses, and malware is emerging. Security threats in mobile communication systems come from three aspects: mobile side, network side, and wireless interface, especially in the wireless interface, where the vulnerability of the wireless link due to the open propagation of electromagnetic waves provides more opportunities for attackers to take advantage of and more easily constitute attacks such as wireless eavesdropping, tracking and positioning, and identity impersonation [1]. In the traditional wireless communication network, its information security is based on cryptography and is based on the premise that the encryption technology distributing keys so that the attacker cannot complete decryption in an effective time, but with the development of quantum computing technology and electronic devices, the computer's computing power has made a breakthrough—rich computing resources and time resources give the attacker the opportunity to take advantage of the key by making it easy to steal and breach [2]; on the other hand, in addition to eavesdropping attacks in wireless communication networks, there are also authentication-based attacks, such as attackers disguising as legitimate users for illegal access and then launching denial of service, node cloning, tampering with data, and sending Trojan viruses to

the network; relying on traditional cryptography alone will not guarantee the security of the communication system [3]. Due to the broadcast characteristics of wireless communication systems, the target user in any location in space can receive the signal transmitted by the base station. But the broadcast characteristics of wireless signals also give eavesdropping users a convenient way to implement eavesdropping; eavesdroppers in any corner of space can eavesdrop on the signal, threatening the wireless security transmission of private information. This security threat is fatal in some special areas, such as wireless transactions of credit card data or wireless transmission of account password information in the financial field, and wireless transmission of confidential data in the military field. The intruder can damage and invade through highly sensitive transceiver devices, which is likely to lead to the leakage of internal information and resources, and if the intruder successfully accesses the network, he can also obtain the MAC address of this site disguised as a legitimate user for further deception and attack, which will bring great harm and loss to individuals, enterprises, and even countries, so the problem of information security of wireless communication networks is becoming increasingly prominent.

With the advancement of science and technology and the development of new industries, wireless communication networks will allow access and interconnection of massive devices, the distribution management and update of keys will incur huge overhead, and there is also the problem of high latency, then it is easy for attackers to exploit the latency to take advantage of the situation. If the information security is increased by increasing the key length will bring higher complexity of computing, which is biased for low-power and hardware resource-limited devices. Physical layer-based secure access authentication techniques have received a lot of attention and research in recent years. Physical channels are difficult to be forged because of their uniqueness, randomness, and reciprocity. Under time-varying channels, physical channels have space-time uniqueness, which can overcome some shortcomings of traditional information security schemes. A secure access authentication scheme built on the physical layer can be combined with a high-level access authentication scheme to further strengthen the authentication and identification standards for user identity in wireless communication networks, which plays a key role in improving the information security of communication networks. Some physical layer features such as channel state information (CSI), received signal strength (RSS), channel impulse response (CIR), and hardware fingerprinting have been subject to many studies and advancements, plus the current and future MIMO-OFDM technology used in large scale also provides quite rich physical layer features, especially in OFDM modulation technology, the channel response of multiple subcarriers provides detailed CSI, so the physical layer based secure access authentication technology has deeper research significance and broader research prospect [4].

2. Related Work

The current physical layer security research can be divided into four branches, which are wireless channel security coding and confidential capacity analysis research, physical layer feature-based key generation research, physical layer feature-based authentication research, and physical layer antimalicious interference research. The research on physical layer security coding and capacity analysis is mainly focused on the wire-tap model and information theory.

The literature [5] proposes the wire-tap model, which is a classical three-user model consisting of Alice, the sending user; Bob, the receiving user; and Eve, the eavesdropping user. The model assumes that Bob's primary channel quality is better than Eve's eavesdropping channel quality so that legitimate users can achieve perfect confidential communication without relying on shared keys. Subsequently, the research on wireless channel secrecy capacity analysis based on the wire-tap model has been gradually developed. The literature [6] considered the secrecy capacity of cognitive radio networks in the presence of eavesdropping users. The literature [7] has the confidentiality capacity of a multi-input multioutput system model based on Gaussian signal input. The literature [8] proposed a method for approximating the confidential channel capacity using space-time coding in an ultrawideband-MIMO system. Since the relay-based collaborative communication can increase not only the reliability of communication but also the confidentiality capacity of the channel. The first analysis of the confidentiality capacity under a single collaborative relay was presented in the literature [9]. Subsequently, the literature [10] analyzed the secrecy capacity of a single collaborative relay in a MIMO system. Unlike collaborative communication with a single relay, the literature [11] analyzed the secrecy capacity of collaborative communication with three relays. Alternatively, it is shown that artificial noise and collaborative can effectively increase the confidentiality capacity of the channel. For example, the literature [12] treats secondary user signals or nonauthenticated user signals as noise that can interfere with the eavesdropping user and primary user channels and achieves covert communication of primary user signals. The literature [13] proposes a beamforming approach using relaying; proposes a physical layer security solution for untrustworthy relaying based on amplification and forwarding protocols; proposes two secure beamforming schemes, namely, collaborative beamforming and noncollaborative beamforming; and demonstrates that their schemes are due to the conventional schemes in terms of secrecy capacity. The literature [14] makes an experimental comparison for four relay node selection schemes which are optimal relay with no interference, optimal relay with random interference, optimal relay with optimal interference, and random relay with random interference to represent the impact of different selection methods and interference power on the overall network security capacity metrics. The use of carefully designed artificial noise while relaying can be achieved by interfering only with eavesdroppers without affecting normal users. The literature [15] focused on the impact of the eavesdropper's attack pattern on the security of the system and investigated the communication reliability of normal network users in the case of interference collaboration with eavesdroppers switching between passive eavesdropping and active jamming modes.

The literature [16] exploits the decorrelation property of the channel, which is used to achieve user identification and authentication at different locations. The literature [17] exploits the uncorrelated nature of channel characteristics for authentication, assuming that the channel frequency response at adjacent moments is compared to determine whether the sender has changed in an environment with slow-changing channel characteristics and rich multipath, and performs authentication analysis in a time-varying channel, terminal mobility, and MIMO environment. In addition, the literature [18] proposes a detection method for attacks during authentication and verifies it experimentally in a wireless LAN environment. The literature [19] improves the performance of channel fingerprint authentication using authentication threshold adaptive adjustment, power spectral density detection, and artificial noise. The literature [20] introduced the support vector machine (SVM) theory in machine learning to improve the intelligence of wireless channel fingerprinting.

2.1. Research on Physical Layer Secure Transmission and Authentication Mechanism Based on Compressed Sensing of Multiantenna Arrays

2.1.1. Compression-Aware Physical Layer Model Based on Multiple Antenna Arrays. An array antenna is formed by some antennas arranged together in a certain way, and the individual antennas of the array are called array elements, although the array elements in the array antenna can be different in principle, in most practical applications, each array element is not only the same form but also the same orientation. Generally speaking, the array antenna array element is mostly used dipole, ring antenna, symmetric oscillator, horn antenna, microstrip patch antenna, parabolic reflector antenna, and waveguide slit, and another simple antenna, and the research focus on the group array.

The array antenna has better radiation characteristics than a single antenna; the fundamental reason is that the radiation electromagnetic waves from multiple antenna units in free space are superimposed on each other to form the interference phenomenon of electromagnetic waves, so that in some regions of space in the same phase superposition, there is field strengthening, and in some other regions in reverse superposition, there is field weakening, thus forming a strong and weak distribution of electromagnetic fields in space, so that the total constant radiation energy in space undergoes redistribution. With the development of wireless system communication services to broadband, convergence, and mobility, the technology will be more and more widely used in the wireless access side. According to the electromagnetic field theory, it is known that the radiated electromagnetic field generated in free space by a current source with current density J can be expressed as

$$\vec{J} = J \cdot (u_1, u_2, u_3, u_4, \cdots, u_n). \tag{1}$$

For an array antenna, the current value for each cell corresponds to a discrete sampling of a continuous source. The above line current source is discretized into the sum of N small current sources, the total current on each small current source is represented by I_n, the surface current source is discretized into the sum of M small current sources, and the total current on each small current source is represented by I_m; each small current source is equivalent to an array cell; thus, the continuous line source and surface source are discretized into an N element linear array and an M element planar array, respectively [21], and the corresponding far-field radiation characteristics are

$$M = \begin{vmatrix} N \cdot \sin u \cos x, & I_n \cdot \cos \gamma, \\ I_m \cdot \sin \gamma, & -\sin y. \end{vmatrix} \tag{2}$$

In the mathematical model of compressed perception,

$$A(t+n) = (1-y)\kappa(x) + \Delta\kappa_{ij}(t). \tag{3}$$

x denotes the original signal, A denotes the sparse mapping matrix, y denotes the compressive measurement, and n denotes the additive noise. In the mathematical model of compressive sensing, if the original signal$x$is sparse, it can be sparsely represented. The process of sparse representation is that the original signal can be reflected into a very small vector space by the effect of the sparse mapping matrix A. The number of rows in the vector space after the auction will be much less. This process is the core idea of sparse theory, which is to describe a high-dimensional signal in terms of a low-dimensional signal. The block diagram of the mathematical model of compressed perception is shown in Figure 1.

There are a huge amount of definitions of sparse signals, but the idea is the same; in layman's terms, it means a signal with few nonzero elements or most elements with coefficients of 0. Although the signals that exist in nature can be sparse, they are generally not sparse and need to be approximated as sparse and compressible under the conditions of a certain transformation domain. Theoretically, as long as the corresponding sparse representation space can be found, i.e., under some transform domain, any signal can potentially be compressible, which can make the compressive sampling effective, and the sparse signal can be expressed through the sparse representation, so it is said that an important prerequisite for compressive perception is the sparse representation, so the sparsity of the signal is the theoretical basis of compressive perception, and it is known from many literatures that the sparse representation can be performed. The signal has its important role because only when the original signal is sparse, assuming that the signal length is N and is K sparse, it is possible to reconstruct the original signal data of length N by using the M observations obtained, where K is less than M and much less than N, and we can successfully reconstruct the signal data of length N from the K larger signal element coefficients we obtained, and the signal data we obtained of length N is still highly accurate. In other words, when the signal we get at the beginning is sparse, we can use signal element coefficients that are much smaller than the signal length to recover the original signal accurately [22].

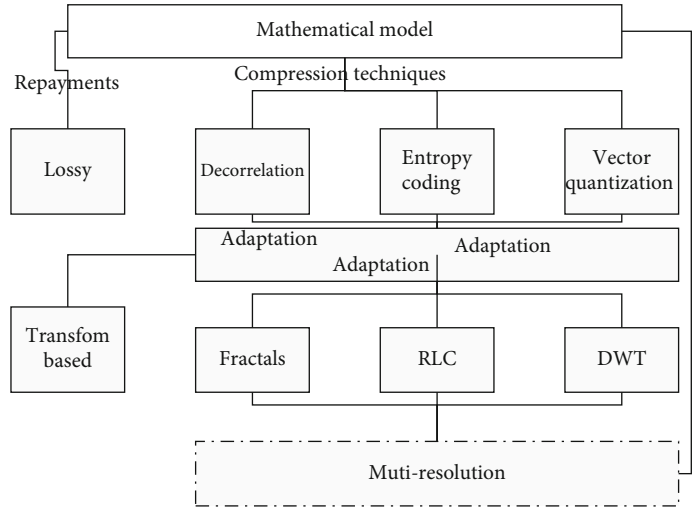

Figure 1: Mathematical model of compression perception.

The development of MIMO technology can be divided into three phases: (1) point-to-point MIMO, (2) multiuser MIMO, and (3) large-scale MIMO. Point-to-point MIMO systems are the simplest early implementation of MIMO systems, which refers to communication between an access point (AP) and a single user configured with multiple antennas. Point-to-point MIMO systems enhance the reliability of the communication system through spatial diversity. When the channel environment is good, multiple antennas at the transmitter or receiver can provide spatial freedom for signal transmission, which can be used to transmit more data streams simultaneously in the MIMO channel to obtain higher channel capacity. The presence of additive Gaussian white noise in a stable channel with perfect channel state information and the spectral efficiency of the system at the receiver side can be expressed as

$$E(k) = R_k \cdot {L_k}^2 + \int Q_k x dx. \tag{4}$$

In multiuser MIMO technology, a single transmitter serves multiple receivers, and multiple receivers share the same time-frequency resources in the communication system. The equipment overhead is relatively low. Therefore, multiuser MIMO technology is widely used in communication systems such as long-term evolution (LTE), 802.11 (WiFi), and 802.16 (WiMAX). Converting the original serial branched data bitstreams of several high-speed rates into several low-speed parallel branched data streams, which is the main purpose of the serial-parallel transformation of data. However, in the downlink of a multiuser MIMO system, both the access point and the user side need to know the information about the transmitted channel. Therefore, a considerable number of known guide frequency sequences are used to train the channel parameters. From most of the previous literature, researchers have presented an analysis of the advantages and challenges of multiuser MIMO systems and the system performance. The spectral efficiency of the uplink (uplink, ul) and downlink (downlink, dl) of a multiuser MIMO system with K single-antenna users is denoted as

$$\begin{aligned} C_{ij} &= \sum_{i=1}^{n} x_i^2 \sigma_i + {x_j}^2 \sigma_j + {x_k}^2 \sigma_k, \\ L_k &= \sum_{i=1}^{k} h_k(v_k). \end{aligned} \tag{5}$$

Improving communication security using physical layer security techniques requires specific security evaluation metrics to quantify the security performance of the system. Security metrics focus on parameters such as the transmission rate of communication and the probability of interruption. By the different focus of wireless networks on security, security evaluation criteria are often divided into two categories: the first evaluation criteria are based on rate measures, such as confidential capacity, and traversal confidential capacity; the other evaluation metrics focus on whether the communication is interrupted, mainly the probability of security interruption. The security interruption probability is used to evaluate the reliability of message delivery in communication. When we have certain requirements for the quality of communication, the minimum secrecy capacity, that is, a secrecy capacity of 0, cannot satisfy our requirements for quality. We need the secrecy capacity to be higher than a predetermined value, and when the secrecy capacity is lower than this value, it is considered that security cannot be guaranteed and the communication is interrupted. The security outage probability can be quantified numerically by the probability of an outage during communication and is more suitable as an evaluation metric in scenarios where low latency is required. Assuming a minimum secrecy capacity of R is given in advance, the security interruption probability can be obtained from the following equation:

$$R_k = \sum_{i=1}^{k} f_k(w_k). \quad (6)$$

Also, multiantenna relaying can be used with different relaying schemes to secure the transmission from the source node to the destination node by exploiting spatial freedom. For example, through the spatial freedom brought by multiple antennas, artificial noise and relayed forwarded messages can be sent simultaneously to reduce the eavesdropper channel quality. When there are multiple source nodes in the system, multiple antennas can be cooperated to forward signals together to achieve higher spectrum utilization. Social networking techniques can be integrated into the multiantenna array compressed-aware physical layer security technology, where the multiantenna array compressed-aware physical layer secure communication system model consists of a BS and a user community that can use dense user terminals to store popular content on storage capable devices. The mapping of the symbols of a subcarrier is obtained by synthetically modulating the symbols of multiple subcarriers, and each subsite carrier can choose a different digital modulation according to the subcarrier channel state. Each subcarrier can be digitally modulated according to the subcarrier channel state. The system can switch back and forth between normal cellular cell communication and multiantenna array compressed-aware physical layer secure communication behavior. The former is where the user sends a request to the base station and obtains data through the base station transit. The latter is where the user sends a request to the base station, which performs a device discovery process, and when a terminal is detected to have the desired file cached, secure communication is established to fetch the desired file directly from the storage device. When social and secure communication networks are combined, the whole can be seen as consisting of two layers: the physical layer and the social layer, where each participant in the social layer can correspond one-to-one with a device in the physical layer. In the social layer, the connection between participants can express the offline relationship between users and can be seen as the closeness of the relationship between the two. In the physical layer, the device-to-device relationship indicates whether a device can establish a secure communication connection with another device.

As shown in Figure 2, the differences between the social and physical layers are physically significant. For example, User A and User B have an online social connection, but at the physical layer, a secure communication connection cannot be established due to the long physical distance from the device to the device. Another example is that in the physical layer node C and node D are close but not socially connected, indicating that these two nodes can establish a secure communication connection at the physical layer, but are not social friendships online and will not be connected by the system given the security of file transfers. The primary challenge in secure communication integrated into social networks is how to select and utilize the appropriate social awareness from the complex social networks to enhance secure communication performance. Among them, social trust can effectively motivate the establishment of secure communication among users and share spectrum resources, while interest similarity can effectively predict the probability of having the same needs among users, which in turn motivates the establishment of connections between secure communication devices to increase resource utilization.

2.1.2. Secure Physical Layer Transmission and Authentication Mechanism Based on Compressed Sensing of Multiple Antenna Arrays. The physical layer authentication method based on compressed sensing channel information through multiple antenna arrays can meet the demand for lightweight authentication in time-varying wireless environments for future resource-constrained networks such as 5G networks, IoT, and sensor networks. The inherent drawback of physical layer authentication techniques is that initial authentication is not possible, so physical layer authentication needs to be combined with traditional authentication mechanisms and rely on traditional upper layer authentication techniques for the initialization of authentication [23]. In this paper, the combination of physical layer authentication methods based on compressed channel information of multiantenna array and upper-layer authentication can constitute a cross-layer authentication scheme, whose flowchart is shown in Figure 3.

Physical layer authentication, as an enhanced secondary authentication method, consists of two aspects: the authentication of the first data frame in each data transmission needs to be completed by upper-layer authentication, and the authentication of all subsequent data frames can be performed using physical layer authentication to confirm the sender's identity. When the upper layer authentication uses digital signatures under the public key system, the process of authenticating all data frames for each data transmission is shown in Figure 4. Thus, we can effectively eliminate symbol-to-symbol interference and confirm that the OFDM subsymbols are orthogonal to each other's carriers. As an enhanced secondary authentication method, the authentication of the first data frame needs to be completed by the upper layer authentication, and the authentication of all subsequent data frames can apply the physical layer authentication to confirm the sender identity. Each data transmission contains fN data frames, and if the first data frame fails the upper layer authentication or the subsequent data frames fail the physical layer authentication, the data frame is considered to be subject to spoofing, tampering, and other attacks, and is directly discarded for the next data frame authentication. When a data frame is pending authentication, the key reaches the life cycle, at which point the upper layer authentication needs to be restarted to authenticate the data frame. This scheme of cross-layer authentication uses upper-layer authentication only when there is a special need. Compared with traditional upper-layer authentication, the cross-layer authentication scheme reduces the complex computation caused by upper-layer computation, while using the channel fingerprint as the basis for authentication is difficult to forge, and has significant features such as low complexity and high accuracy, which is suitable for 5G systems with a large number of wirelessly interconnected devices.

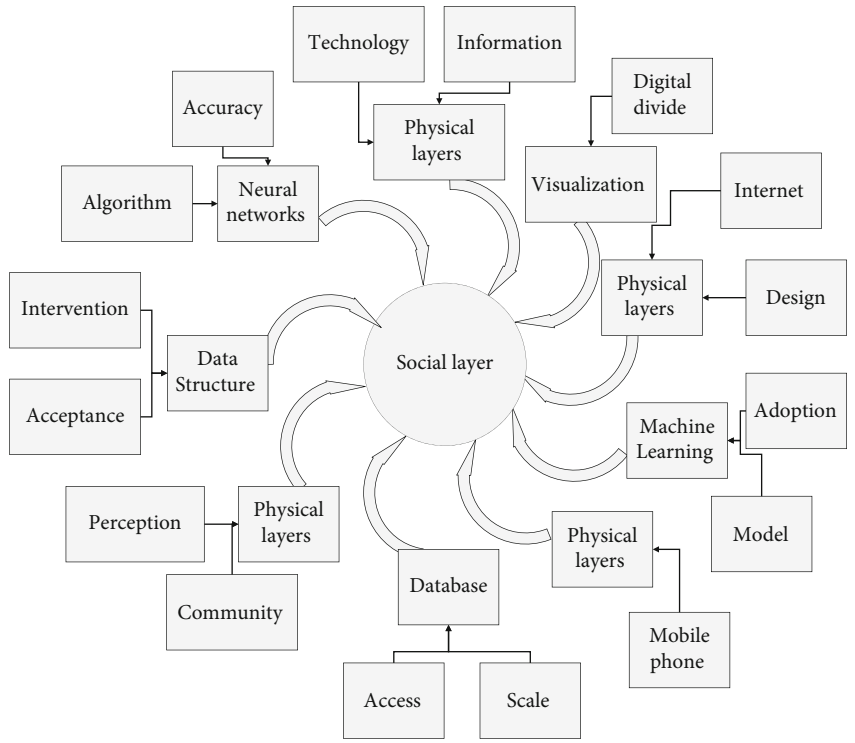

Figure 2: Interaction between the social and physical layers.

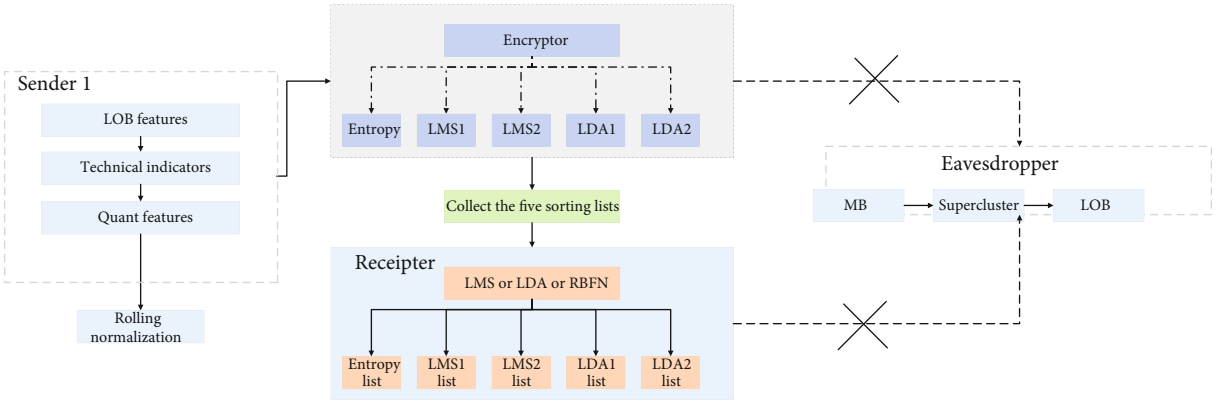

Figure 3: Flowchart of cross-layer authentication method based on compressed sensing channel information from multiple antenna arrays.

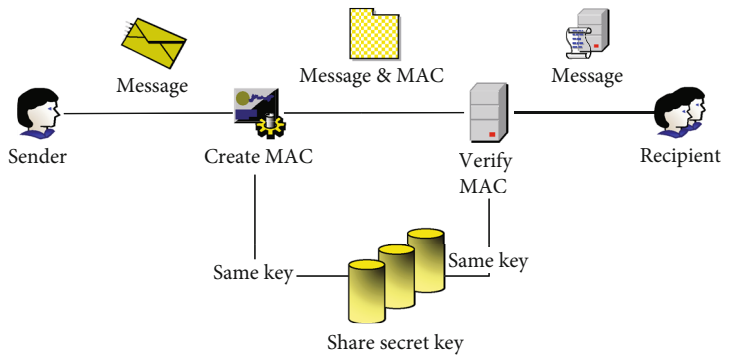

Figure 4: Data frame authentication process.

In simple terms, physical layer security authentication is the use of the physical characteristics of the channel or electronic device to encrypt and authenticate information. The main research in this paper is to perform authentication operations based on the channel estimation information in the physical layer.

For authentication, because the wireless channel has many excellent features and rich available resources as described in the previous section, the physical layer security authentication based on the wireless channel has the advantages of confidentiality and reliability, low implementation complexity, and many algorithmic solutions compared with the traditional key-based security authentication. Specifically, the confidentiality and reliability are reflected in the very different differences between unrelated channels and the strong correlation between the wireless channel and the geographical location of the user, which makes it difficult for an attacker to listen to or imitate the channel of a potential attackee and establishes a near-perfect defense against eavesdropping attacks and forgery attacks; due to the reciprocity of the wireless channel, the channel characteristics are observed by both legitimate senders and receivers in a certain time gap. Due to the reciprocity of the wireless channel, the channel characteristics observed by both legitimate senders and receivers in a certain time interval are approximately the same, so the channel information can be directly used instead of the key based on complicated calculations, which directly eliminates the distribution, update, and management of a series of operations and does not require the assistance of the upper layer, which can significantly reduce the load on the system, and the complexity of the implementation of the scheme is low; as of today and in the future for a long time, MIMO technology will be more and more widely used. This will provide more available resource features for the wireless channel, and with the combination of today's and machine learning-related algorithms, there are numerous new intelligent algorithm solutions and a wide development space. For physical layer security authentication, authentication schemes in different scenarios are studied to different degrees and have different characteristics. Referring to the "three handshakes" when TCP connection is established in computer networks, if the authenticated parties perform similar operations such as mutual interrogation and confirmation before communication, then it can be called active security authentication; On the contrary, if there is no such "three handshake" before the communication, the safety certification will not be guaranteed. In contrast, if the communication is not preceded by these "three handshake" operations, but by the direct inlay of authentication information in the message sent or by the use of a prenegotiated key for data transmission, this approach is called passive security authentication. There is also a difference between static and dynamic security authentication, depending on the mobile state of the authenticating parties.

After the introduction of the guide frequency update mechanism, the security threat comes from two aspects, one is the theft of the guide frequency signal itself during its use, which has been analyzed before by the performance characteristics of blind estimation. The second is the security of the generated key. In the general wireless environment, a certain key generation rate can be guaranteed, while for the blind estimation the algorithm converges slowly, so the generation rate is much higher than the update rate requirement. Moreover, for the one-way hash function SHA-1, a small difference between its input seeds can lead to a large difference in the output result, which also eliminates the possibility of Eve directly obtaining the format of the guide frequency signal. The security of key distribution during the guide frequency update can be ensured by the transmission security of the equivalent channel. According to the wire-tap model of wireless channels, a dominant channel needs to be constituted to ensure perfect security.

2.2. Experimental Validation and Conclusions. The simulation is verified based on a typical Rayleigh fading channel, assuming that the system uses symbols carried on 64 subcarriers, 64 OFDM symbols per frame, CP length of 16, and QPSK modulation. The number of multipaths is chosen to be 5, the number of guided symbol groupings $n = 10$, the minimum mean square error (MMSE) algorithm is used as the channel estimation algorithm, the confidence level of the hypothesis test is chosen to be 0.95, and the average of the false alarm rate and missed alarm rate is obtained using the 10,000 times Monte Carlo method.

The probability of successful recovery of channel state information for each feedback scheme with different feedback compression ratios is given in Figure 5. We choose NMSE to evaluate the accuracy of feedback reconstruction. By performing 100 reconstructions of the signal at the base station side using each algorithm and calculating the normalized mean square error of the channel matrix for each user reconstructed by each algorithm, this reconstruction is judged to be successful if the algorithm reconstruction error is less than 10-2; otherwise, the reconstruction is judged to have failed. As a whole, the probability of successful reconstruction of all algorithms increases with increasing compression ratio, which is an inevitable trend, because as the compression ratio increases, the more information of the original signal is carried in the observations, and the probability of successful reconstruction is increased. Before 0.2, the successful reconstruction probability of the joint-OMP algorithm is slightly higher than that of the improved DCS-OMP algorithm, and after 0.2, the successful reconstruction probability curve of the improved DCS-GOMP grows rapidly and exceeds that of the joint-OMP algorithm, and the successful reconstruction probability is slightly higher than that of the joint-OMP algorithm. The user's information can be transmitted over several subcarriers, and a single fading or some fading will only interfere with a small portion of the carrier channel, which can be interfered with using channel coding The channel coding can be used to perform carrier error correction on these interfered channels. The performance of the scheme based on compression-aware reconstruction using the OMP algorithm is poor compared to the other three schemes, and the high probability of successful reconstruction is reached only after the compression ratio of 0.4. On the whole, when a certain compression ratio is reached, each scheme achieves

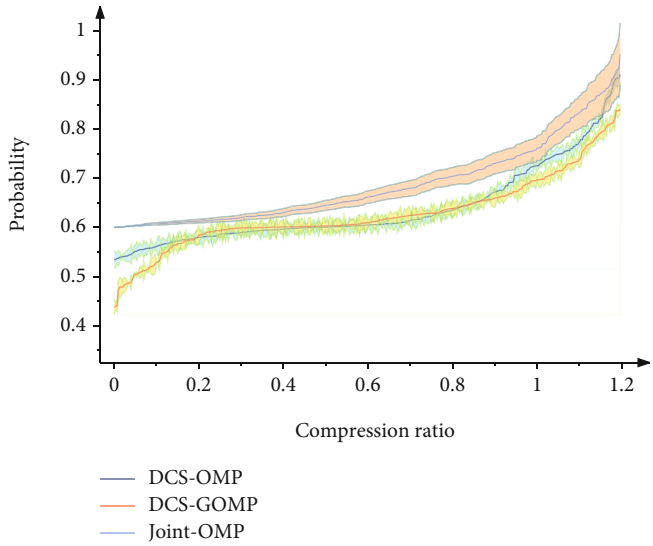

Figure 5: Probability of successful recovery of channel state information for each feedback scheme with different compression ratios.

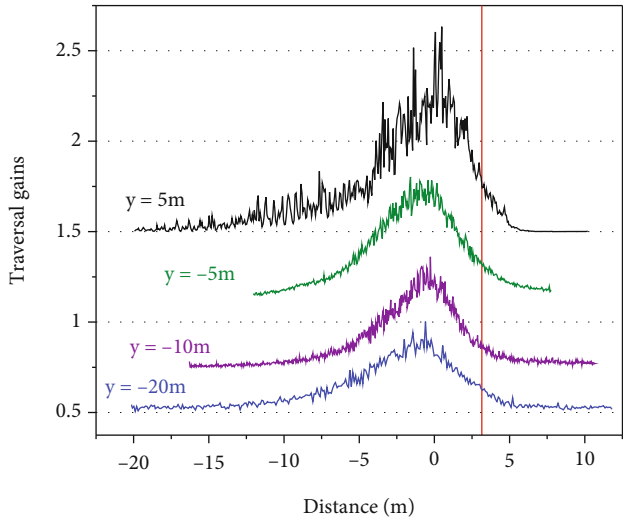

Figure 6: Traversal gains for virtual users at different locations.

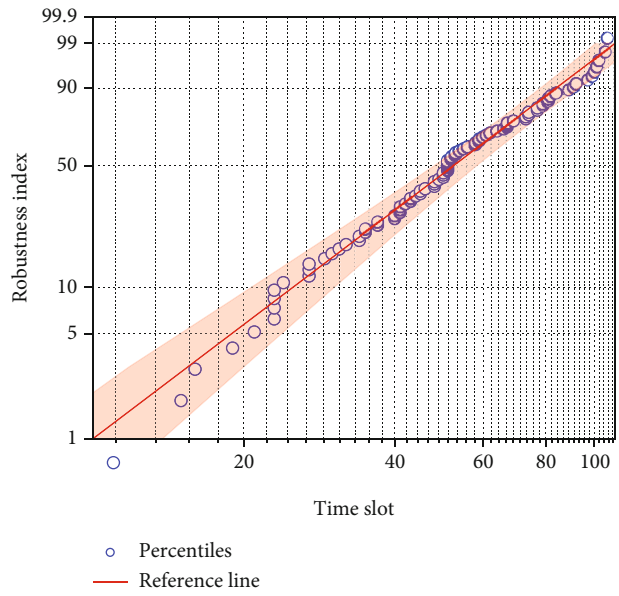

Figure 7: Robustness of security performance of physical layer security system based on compressive sensing of multiple antenna arrays.

a high probability of successful reconstruction, which means that each scheme is more effective. In summary, the performance of the feedback scheme using the DCS-GOMP algorithm is higher than that of the scheme using the other algorithms, and the DCS-GOMP algorithm can achieve better reconstruction performance.

As can be seen from Figure 6, the gain of the virtual user gradually increases as the distance between the virtual user and the base station decreases. In particular, the change of the distance between the virtual user and the base station has a nonlinear relationship with the increase or decrease of the gain of the virtual user, for example, when $x = 0$, the coordinate of y increases 0.25 dB from -20 m to -15 m; when the coordinate of$y$is from -15 m to -10 m, the gain increases by 0.65 dB. In addition, it can be seen from the figure that the gain available to the virtual user is maximum when its distance is at (0 m, 0 m). Whenever a digital signal is transmitted over a digital channel with a limited bandwidth of the digital signal band, there must be some degree of intercode crosstalk caused. When the location of the fixed virtual user is (5 m, -5 m), after 1000 Monte Carlo simulations, the traversal gain of the UAV is shown in Figure 6. The results show that the closer the distance between the virtual user and the UAV, the larger the gain obtained by the UAV. In addition, the gain of the UAV gradually decreases as the flight distance gradually increases. The decreasing trend of gain gradually becomes obvious when the coordinate of y is greater than 2 m. The results show that if the UAV only interferes with the virtual user in a one-time slot, then the UAV will get as close as possible to the virtual user to maximize the current instantaneous gain. In addition, the results show that the traversal gains of the UAV are symmetrically distributed with $x = 5$ as the coordinate axis.

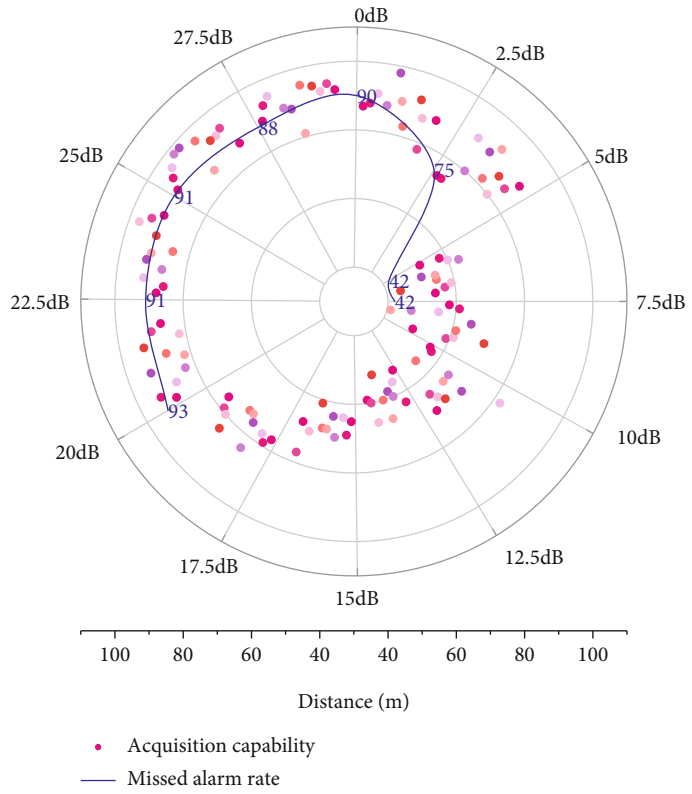

Figure 8: Simulation of missed alarm rate with Eve acquisition capability.

Figure 7 shows the robustness of the security performance of the physical layer security system based on compressed sensing of multiple antenna arrays. The physical layer security system based on compressed sensing of the multiantenna array uses the subarray phase random inversion technique to randomize the side flaps, and the signal-to-noise ratio in the target receiver region is maintained at a value of 20 dB. As can be seen from the figure, at different observation locations, such as the target angular direction or away from the target receiver's directional angular primary flap location, either the eavesdropping noise power drops to zero or the eavesdropper infinitely increases the received signal-to-noise ratio; the physical layer security technique based on multiantenna array compressed sensing provides physical layer performance close to the upper limit of the security rate due to the parameterization technique. Consequently, the multiantenna array compression-aware physical layer security techniques based on low-parallax synthesis with mutually canceling sunbeams and parallax randomization techniques can solve the zero security rate problem outside the target reception region and provide robust physical layer security performance. In the physical layer security system technique based on compressed sensing of multiple antenna arrays, the security rate of the system does not drop to zero unless the eavesdropper is in the same position as the eavesdropper.

Figure 8 shows the simulation schematic of the optical interference location in one round based on the compressed sensing of the multi-antenna array in the physical layer and the virtual user's Eve acquisition capability under the missed alarm rate. From the figure, it can be seen that the communication location of the virtual user starts at (-2 m, 1 m) and ends at (15 m, 8 m) in one round. The interference location of the physical layer based on the compressed sensing of the multiantenna array starts at (0 m, 0 m, 0 m) and terminates at (15 m, 15 m, 0 m). To obtain the maximum long-term cumulative gain, the UAV is not necessarily close to the virtual user to obtain the real-time maximum gain but may choose a location far from the virtual user. The reason for this result is that the state of the physical layer changes dynamically between time slots with a certain transfer probability, therefore, the compression-aware algorithm considers the state transfer probability of the physical layer when selecting behavior to ensure that the long-term cumulative gain is maximized. The effect of Eve's ability to acquire the private guide frequency on the leakage rate can also be seen, and the leakage rate of Eve acquiring the correct number of guide frequency symbol groups is simulated under different signal-to-noise ratios. When the number of Eve's correct guide symbol groups is gradually increased, the leakage rate also gradually increases, and the higher the signal-to-noise ratio, the lower the leakage rate when Eve's ability to be informed is poor, and the authentication completely fails when Eve once all the guide symbols are known. Then, we simulate the false alarm rate under different SNR environments, and from the simulation results, we can see that when the SNR gradually increases, the false alarm rate decreases, and when the SNR exceeds 7 dB, the false alarm rate is already below 0.01, which indicates that it is practical in a typical environment.

In the typical channel environment of mobile communication, for legitimate communicating parties Alice and Bob, the channel is nontime-varying over a while. For the attacker Eve, who is not aware of the private guide frequency, posing as a legitimate communicator is equivalent to signaling a time-varying channel with artificial noise added. Eve does not have a priori knowledge of the channel and does not know the private guide signal specification, so the best way to get rid of the artificial noise is to perform blind estimation of the signal, which requires a large number of samples and a large amount of computation. At the same time, the technique of extracting keys using channel reciprocity is maturing and is used to update the key and private guide frequency can ensure that the attack capability of Eve is limited to a certain level so that the security of authentication is not degraded during the continuous communication. The method of using a private guide frequency signal for authentication is performed on the normal communication process without introducing too much processing and can achieve good authentication performance. The lead generation and update algorithm using a one-way hash function has low computational complexity, adds very little extra processing, and can achieve good real-time performance.

3. Conclusions

In this paper, we propose a time-varying physical layer security transmission and authentication scheme based on compressed sensing of multiple antenna arrays for wireless authentication. The scheme is a lightweight and enhanced secondary authentication technique, which can be combined with upper layer authentication to form a "cross-layer" authentication scheme that can address the security flaws in the current 3G/4G. In this paper, we analyze the traditional authentication model and model the physical layer authentication, taking the high correlation of channel information between communication parties and the decorrelation to third parties as to the privacy advantage. The existence of a secure authentication framework is demonstrated through the theory of typical set and eavesdropping channel models to provide a theoretical basis and rationale for physical layer authentication methods. The continuous development of quantum computing technology has led to a qualitative leap in the computing power of supercomputers, and the traditional encryption mechanism is not so secure and can be easily broken. An authentication security enhancement method based on physical layer-generated keys is additionally proposed. One of the major threats to the authentication mechanism is the malicious relay attack by a man-in-the-middle. To address this security threat, the key is extracted by using the channel characteristics of reciprocity, and the "location stamp," which is closely related to the location, can effectively prevent the man-in-the-middle attack. An improved scheme based on the physical layer key authentication process is designed and analyzed for security.

This paper also proposes a message authentication method based on superimposing tag signals. A tag signal generated by a preassigned key is superimposed on top of the normal transmission of the communication signal which does not affect the communication signal, making the superimposed signal authenticated. The tag signal is characterized by good autocorrelation and intercorrelation and also needs to be generated quickly under very low computational complexity. By comparing several sequence codes, the gold sequence is chosen as the generation sequence of the tag signal. Simulated in a typical signal-to-noise environment, it can achieve a low false bit rate, as well as a very low false alarm rate and missed alarm rate. In addition, the special characteristics of wireless channels are analyzed, the law that channels can be used but not changed is found, the characteristics of strong cooperation in channel estimation are studied, it is pointed out that being informed of the guide frequency is a manifestation of having the right to use the channel, and an authentication implementation method for hypothesis testing of the channel estimation characteristics of the privatized guide frequency is proposed. A theoretical analysis of information-theoretic security is performed on the attack behavior, and the authentication performance is verified by simulation.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported by the NSFC (source) Research on Physical Layer Secure Transmission Method of Multi Domain Cooperative Wireless Communication based on Intelligent Perception (name) 6142104190203 (No.)

References

[1] N. Wang, W. Li, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical layer authentication for 5G communications: opportunities and road ahead," *IEEE Network*, vol. 34, no. 6, pp. 198–204, 2020.

[2] J. D. V. Sánchez, L. Urquiza-Aguiar, M. C. P. Paredes, and D. P. M. Osorio, "Survey on physical layer security for 5G wireless networks," *Annals of Telecommunications*, vol. 76, no. 3-4, pp. 155–174, 2021.

[3] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 282–310, 2021.

[4] S. Balakrishnan, S. Gupta, A. Bhuyan, P. Wang, D. Koutsonikolas, and Z. Sun, "Physical layer identification based on spatial–temporal beam features for millimeter-wave wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1831–1845, 2020.

[5] L. Jiao, N. Wang, P. Wang, A. Alipour-Fanid, J. Tang, and K. Zeng, "Physical layer key generation in 5G wireless

networks," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 48–54, 2019.

[6] N. Wang, W. Li, A. Alipour-Fanid, L. Jiao, M. Dabaghchian, and K. Zeng, "Pilot contamination attack detection for 5G mmwave grant-free IoT networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 658–670, 2021.

[7] S. Asheer and S. Kumar, "A comprehensive review of cooperative MIMO WSN: its challenges and the emerging technologies," *Wireless Networks*, vol. 27, no. 2, pp. 1129–1152, 2021.

[8] M. Wen, B. Zheng, K. J. Kim et al., "A survey on spatial modulation in emerging wireless systems: research progresses and applications," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 9, pp. 1949–1972, 2019.

[9] Z. Lv, A. K. Singh, and J. Li, "Deep learning for security problems in 5G heterogeneous networks," *IEEE Network*, vol. 35, no. 2, pp. 67–73, 2021.

[10] U. Challita, H. Ryden, and H. Tullberg, "When machine learning meets wireless cellular networks: deployment, challenges, and applications," *IEEE Communications Magazine*, vol. 58, no. 6, pp. 12–18, 2020.

[11] A. H. Nalband, M. Sarvagy, and M. R. Ahmed, "Power saving and optimal hybrid precoding in millimeter wave massive MIMO systems for 5G," *Telkomnika*, vol. 18, no. 6, pp. 2842–2851, 2020.

[12] C. Liaskos, A. Tsioliaridou, S. Nie, A. Pitsillides, S. Ioannidis, and I. F. Akyildiz, "On the network-layer modeling and configuration of programmable wireless environments," *IEEE/ACM Transactions on Networking*, vol. 27, no. 4, pp. 1696–1713, 2019.

[13] M. F. Hossain, A. U. Mahin, T. Debnath, F. B. Mosharrof, and K. Z. Islam, "Recent research in cloud radio access network (C-RAN) for 5G cellular systems - a survey," *Journal of Network and Computer Applications*, vol. 139, pp. 31–48, 2019.

[14] S. Kumar, A. Vasudeva, and M. Sood, "Battery and energy management in UAV-based networks," in *Unmanned Aerial Vehicles for Internet of Things (IoT) Concepts, Techniques, and Applications*, Wiley Online Library, 2021.

[15] H. I. Ahmed, A. A. Nasr, S. Abdel-Mageid, and H. K. Aslan, "A survey of IoT security threats and defenses," *International Journal of Advanced Computer Research*, vol. 9, no. 45, pp. 325–350, 2019.

[16] J. Zhang, B. Wei, F. Wu et al., "Gate-ID: WiFi-based human identification irrespective of walking directions in smart home," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7610–7624, 2021.

[17] G. J. Sutton, J. Zeng, R. P. Liu et al., "Enabling technologies for ultra-reliable and low latency communications: from PHY and MAC layer perspectives," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2488–2524, 2019.

[18] F. Zafari, A. Gkelias, and K. K. Leung, "A survey of indoor localization systems and technologies," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2568–2599, 2019.

[19] R. Martins, M. E. Correia, L. Antunes, and F. Silva, "Iris: secure reliable live-streaming with opportunistic mobile edge cloud offloading," *Future Generation Computer Systems*, vol. 101, pp. 272–292, 2019.

[20] J. Kołodziej, D. Grzonka, A. Widłak, and P. Kisielewicz, "Ultra wide band body area networks: design and integration with computational clouds," *High-Performance Modelling and Simulation for Big Data Applications*, Springer Nature Switzerland AG, 2019.

[21] M. Bada, D. E. Boubiche, N. Lagraa, C. A. Kerrache, M. Imran, and M. Shoaib, "A policy-based solution for the detection of colluding GPS-spoofing attacks in FANETs," *Transportation Research Part A: Policy and Practice*, vol. 149, pp. 300–318, 2021.

[22] D. Li, L. Deng, M. Lee, and H. Wang, "IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning," *International Journal of Information Management*, vol. 49, pp. 533–545, 2019.

[23] A. Agarwal and S. N. Mehta, "Analyzing impacts of spatial correlation for multi-user environment with robust concatenation of advanced FEC schemes," *Wireless Personal Communications*, vol. 109, no. 2, pp. 1237–1283, 2019.