IEEE *Access*

Multidisciplinary : Rapid Review : Open Access Journal

MIMO Cross-Layer Secure Communication Algorithm for Cyber Physical Systems Based on Interference Strategies

YUKAI HAO[1,2] AND XIN QIU[1]

[1]School of Management, Wuhan University of Technology, Wuhan 400070, China
[2]School of Economics and Management, Tibet University, Lhasa 850000, China

Corresponding author: Xin Qiu (qiux@whut.edu.cn)

ABSTRACT In this paper, a detailed analysis of multi-input multi-output (MIMO) cross-layer secure communication algorithms in information-physical systems is investigated employing an interference strategy. A three-stage data-assisted channel estimation method is proposed in this paper for the acquisition of channel state information for complex jamming channels in large-scale MIMO two-layer systems. To implement the data-assisted scheme, assuming that there are no errors and no delay in the system, if the data detection and decoding data sequences are completed at a small cell base station, they are sent to the macro base station via a wired backhaul. Due to the sparsity of the channel at the macro base station after user grouping, a channel estimation algorithm based on optimal block orthogonal matching tracking(s) is proposed in the case where the downlink channel at the macro base station utilizes the decoded uplink data and known training sequences. The simulation results show that the data-assisted method proposed in this paper is effective in improving channel estimation accuracy. A machine learning algorithm is directly used to classify the channel difference or channel matrix to obtain the authentication results. In this paper, the scheme is first simulated using channel data from dynamic communication scenarios, its feasibility is analyzed, and the parameters in the scheme are compared, and the optimal scheme is the bagging tree authentication scheme using a 128-dimensional channel matrix as input. To address the interference problem caused by the dense arrangement of SAPs in heterogeneous networks and the unbalanced network load, large-scale MIMO techniques are introduced to reduce the downlink interference caused by the microcell boundary expansion in heterogeneous networks.

INDEX TERMS Jamming strategies, cyber physical systems, MIMO, cross-layer security, communication algorithms.

I. INTRODUCTION

Today, with the dramatic increase in the number of user terminals and the diversification of terminal devices, modern communications are becoming increasingly complex, and both individuals and enterprises are inseparable from the communications services provided by wireless communication networks [1]. As a result, the 5th Generation Mobile Network (5G), which features a low latency, high reliability, low power consumption, and large connectivity, is slowly integrating into our lives and providing strong support for

The associate editor coordinating the review of this manuscript and approving it for publication was Po Yang.

our social infrastructure with its strong drive and permeability [2]. In wireless communications, especially in industrial control scenarios, a single security incident can become serious or even catastrophic [3]. For example, an attacker spoofed a fan controller by sending a false message that caused the fan to stop running, resulting in overheating and damage to the engine. Damage to the engine in turn causes a series of devices to shut down, resulting in huge financial losses and potentially even a major accident that threatens human safety [4]. For communication security reasons, some communication networks are independent of external networks. With wired communication systems, an attacker cannot attack if the attacker does not have access to the physical

IEEE *Access*

Y. Hao, X. Qiu: MIMO Cross-Layer Secure Communication Algorithm for Cyber Physical Systems Based on Interference Strategies

enclosure in which the independent communication network is located, e.g., a factory floor. Large-scale MIMO technology is a communication method in which a large number of base station antennas are used and a single antenna is received at the user's end, i.e., by modifying the base station without having to extensively update the user's terminal equipment, thereby increasing the system's spectrum utilization [5]. The significantly enhanced spatial resolution of large-scale MIMO enables deep mining of spatial dimensional resources, enabling multiple users in the system to communicate with the base station simultaneously on the same time-frequency resource using the spatial freedom provided by large-scale MIMO, thereby increasing capacity by 10 times or more while increasing radiated energy efficiency by 100 times; and providing more possible arrival paths. Signal reliability is improved; average cell throughput is increased, and interference to neighboring base stations is reduced, resulting in higher average cell edge user throughput rates [6].

Cross-layer and intra-layer interference are the main bottlenecks that limit the performance of large-scale MIMO two-layer networks. However, the interference situation in a large-scale MIMO double-layer network will be more complicated: firstly, compared with the macro base stations deployed after strict planning, the location of small base stations in the network is somewhat random, and the irregular deployment of a large number of small base stations will cause the interference characteristics of large-scale MIMO double-layer network is very complicated; besides, with the increase in the density of small base stations, the inter-layer interference of small base stations to the macro base stations and the interference of small base stations to the cell edge users will be more complicated. Intra-layer interference between different femtocells is bound to become increasingly serious, which will severely limit the quality of service (QoS), especially for users at cell boundaries, whose performance cannot be guaranteed [7].

II. RELATED WORK

Researchers have already proposed many concepts on how to effectively coordinate and eliminate interference in large-scale MIMO two-layer networks in real-life scenarios, such as self-configuration, self-optimization, and self-healing in ultra-dense deployment scenarios to achieve intelligent wireless network operations and reduce costs, which are all key technical points that need to be urgently addressed by researchers [8]. Also, researchers have proposed much corresponding interference coordination and elimination schemes, such as virtual layer technology (single-layer solid network to build virtual multilayer network) and cell dynamic clustering (base stations in the network cluster, the same cluster of base stations using the same frequency band resources), but the actual use of the effect is still to be further tested. The unconditional secure communication can only be achieved in the case of a binary deletion channel [9], and cannot be applied in practice. Subsequently, many researchers turned to specific secure coding schemes, such as Low-Density

Parity-Check (LDPC) [10], which can achieve theoretical secrecy capacity under binary deletion channel [11], and Polar coding, which can achieve secrecy capacity under binary symmetric channel [12]. In addition to this, there are coding techniques such as BCH code, Space-Time Coding (STC) based on multi-antenna MIMO systems for approximating the secrecy capacity [13]. A pre-coding design based on signal-to-noise ratio is proposed in the literature to effectively mitigate the interference in small intervals when the coordinated base station has non-perfect channel state information [14]. In the literature, the author investigates the interference elimination strategy based on pre-coding, which can ensure the intra-layer interference elimination and at the same time effectively eliminate the inter-layer interference, and can be combined with linear pre-coding to find a balance point between performance and complexity, to reduce the inter-system interference and improve the system performance [4]. A pre-coding scheme is proposed in the literature to mitigate strong inter-layer interference for users with full CSI, where MBS uses pre-coding to suppress inter-layer interference and SBS uses Maximum Ratio Transmission (MRT) pre-coding to serve dense users [15].

To solve these problems, this paper investigates ultra-dense networks from the perspective of resource management and interference control, aiming to protect and enhance the spectral efficiency and energy efficiency of the system and reduce the complexity of the algorithm, and through analysis, computation, and derivation, combined with algorithm design, it complements the past theoretical research work and deepens the research direction of large-scale MIMO two-layer systems. The scope of application of multi-user large-scale MIMO and its transmission characteristics are first introduced, and channel estimation, user grouping, and pre-coding techniques in multi-user large-scale MIMO systems are analyzed [16]. A clustering scheme suitable for practical scenarios is investigated to improve the throughput of the system while ensuring a certain communication quality. In this chapter, a user grouping algorithm based on local discriminative projection is proposed for the scenario of a large-scale MIMO two-layer system with high-density users, which improves the user grouping effect, reduces the computational complexity of the high-dimensional channel matrix, and reduces the interference of small intervals by taking advantage of the characteristics of angle and distance as similarity metrics. Finally, the simulation results show that the proposed algorithm in this chapter compares the performance of the traditional algorithm. In this paper, a BPNN-based single-point detection scheme for malicious nodes is proposed. The scheme discards the traditional algorithm based on threshold discrimination and directly classifies the node's reputation to detect malicious nodes. It is experimentally demonstrated that the detection performance can be improved by increasing the feature dimension of the input data, i.e., the number of input layer neurons when the number of hidden layers and the number of neurons is constant. Moreover, the scheme can achieve the ideal detection performance when the number of hidden
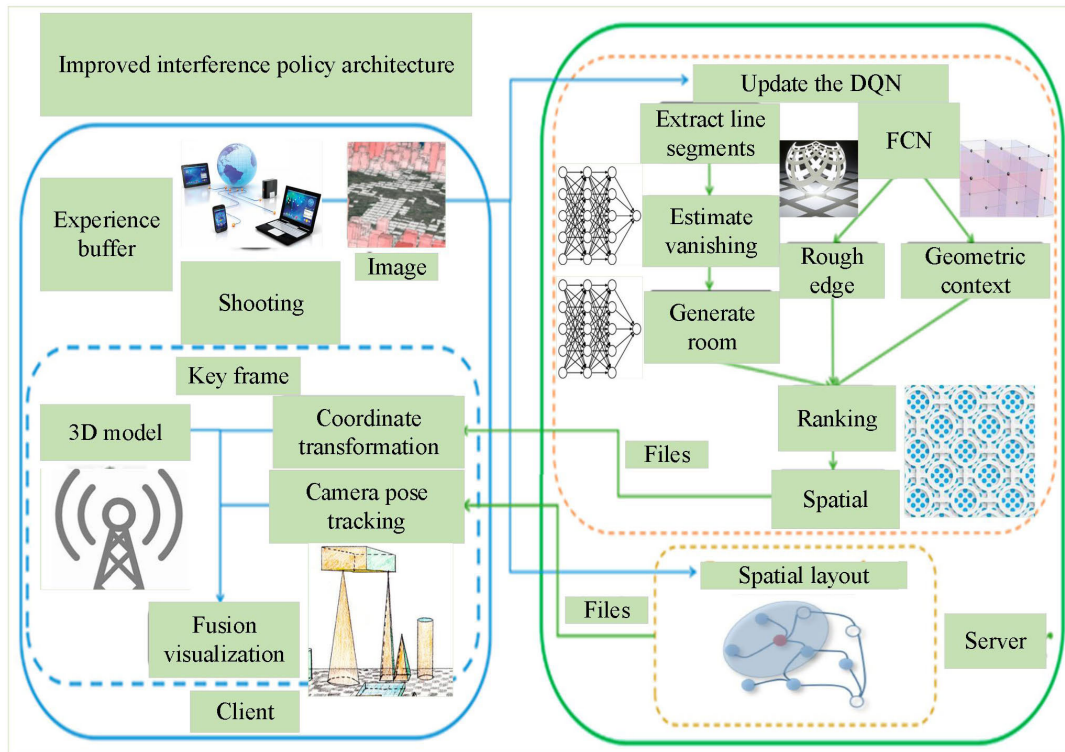
Y. Hao, X. Qiu: MIMO Cross-Layer Secure Communication Algorithm for Cyber Physical Systems Based on Interference Strategies

IEEE *Access*

FIGURE 1. Improved interference policy architecture.

layers and the number of neurons are large enough. However, the larger the number of hidden layers and the number of neurons is, the higher the computational complexity of the detection scheme.

This paper makes the following arrangements on the structure of the rest of article: In section III, we devote to Interference policy for cross-layer secure communication algorithm analysis and design; MIMO analysis design in cyber physical systems is the content of the Section IV; Section V contributes to simulation experiments and results analysis; Section VI summarizes the full text.

III. INTERFERENCE POLICY FOR CROSS-LAYER SECURE COMMUNICATION ALGORITHM ANALYSIS AND DESIGN

A. IMPROVED ANALYSIS OF INTERFERENCE STRATEGY COMMUNICATION ALGORITHMS

Due to its anti-interference, low interception, and other characteristics, frequency hopping communication have a wide range of applications in both military and civilian fields [17]. In the MIMO channel environment, the spatially propagated signals go through different caterers to reach the MS, and the signals reflected, refracted and bypassed by different caterers have indistinguishable relative time delays, which is understood as an indistinguishable multipath cluster, constituting a path in the usual sense. Corresponding to the same multipath cluster, all antennas at the receiving end have the same distribution of incoming wave direction.

In frequency hopping communication, the transmitting end generates a frequency hopping frequency rate through a frequency synthesizer, then modulates the information flow to the corresponding frequency and sends it out through the antenna [18]. At the receiving end, the received signal with noise and interference is sent to the mixer, and the local carrier frequency table generated by the frequency synthesizer at the receiving end completes the process. Unlike traditional frequency hopping, Uncoordinated Frequency Hopping does not require the transmitter and receiver to share the frequency hopping frequency band key in advance. With this technique, the transmitter can select a different channel to send data at each moment, so when the number of interfered channels is less than the total number of available channels, there is a possibility of successful data transmission, as shown in Figure 1. In general, non-cooperative frequency hopping techniques can be divided into passive and active frequency hopping [19], where, for passive frequency hopping, the transmitter chooses to change channels only when it perceives that the currently used channels are being interfered with, while for active FM, the transmitter reselects channels at each moment. It is assumed that the micro base station has a cognitive function, which senses the channel occupancy of the macro cell and opportunistically accesses the channel in the macro cell. When the distance from the micro base station to the macro user is less than the distance threshold this creates an interference-limited domain around the dispatching macro user [20]. In this paper, the set of microbuses located

IEEE *Access*

Y. Hao, X. Qiu: MIMO Cross-Layer Secure Communication Algorithm for Cyber Physical Systems Based on Interference Strategies

in the interference-limited domain of a macro user is defined as an Interfering Small cell base station cluster corresponding to the macro user.

The number of channels attacked by the jammer at each moment is not equal, based on this, we first analyze the probability density function expression for the estimated error under an arbitrary jamming strategy and the expression for the objective function T in the optimization problem, and then propose an algorithm for optimizing the jamming effect when the number of channels per jamming is not equal [21]. Also, this subsection analytically proves that the interference effect is better in the case where the number of interference channels per interference is unequal than in the case where the number of interference channels per interference is equal. Let ϕ_t denote the probability that the jammer successfully blocks data transmission at moment t [22]. Then, for a given number of channels m_t, there are:

$$\phi_t = \frac{\sum\limits_{t=1}^{T} m_t}{M}, \quad \forall t \in \{1, 2, \ldots, T_a\} \quad (1)$$

The T is the set of all moments. M is the count of all channels. Due to the limited energy of the jammer according to equation (1):

$$\sum_{t=1}^{T_a} \phi_t = \frac{E \sum\limits_{t=1}^{T} m_t}{M} \quad (2)$$

E is a constant that can change. For an arbitrary moment t, according to P_r iterative formula (3), the probability density function of P_r can be expressed as:

$$P_r(P_t = h^i(\overline{P})) = \begin{cases} (M + 1 - \phi_{i-1} \sum\limits_{t=1}^{T} m_t \sum\limits_{i=1}^{I-1} \phi_{i-k}, \\ \quad i = 1, 2, \ldots, t \\ 1 - \phi_{i-1}, i = 0 \end{cases} \quad (3)$$

Their corresponding mean values are [23]:

$$IE[P_t] = \overline{P} + \sum_{t=1}^{T} m_t \sum_{i=1}^{I-1} \phi_{i-k} \prod(h^j(\overline{P})) \quad (4)$$

Therefore, the objective function J for the optimization problem is:

$$\begin{aligned} J &= \frac{M}{T} \left(\sum_{t=1}^{T} m_t \sum_{i=1}^{I-1} \phi_{i-k} \prod(h^j(\overline{P}) - \sum_{i=1}^{I-1} \phi_{i-k} \prod(h^j(\overline{P}) \right) \\ &= Tr|\overline{P}| + \frac{M}{T} \\ &\quad \times \left(\sum_{t=1}^{T} m_t \sum_{i=1}^{J-1} \phi_{i-k} \prod(h^j(\overline{P}) + \sum_{i=1}^{I-1} \phi_{i-k} \prod(h^j(\overline{P}) \right) \\ &= Tr|\overline{P}| + \frac{M}{T} \left(\sum_{v=1}^{T} m_t \sum_{i=1}^{J-1} \phi_{i-k} \prod(h^j(\overline{P}) \prod(h^j(\overline{P}) \right) \quad (5) \end{aligned}$$

The setting of the interference threshold will affect the size of the interfering microsite cluster [23]. When the interference threshold value is small, there will be more tiny areas contained in the interfering microsite cluster, then the microcells suffer less residual interference from the tiny areas, but these microsites will also be deprived of transmission opportunities. Conversely, when the interference threshold is higher, the interfering microsite cluster contains fewer microscopic regions, then the microcells suffer less residual interference from microscopic regions, but more microsites will be deprived of transmission opportunities. Regardless of the value of the interference indicator variable, the microsites located outside the interference-limited domain can transmit data normally [24]. Thus, the sum of the network utility of micro users located outside the interference-limited domain is independent of the optimization variable and it is always non-negative.

$$P = \max F(\phi_1, \phi_2, \ldots, \phi_k) \quad (6)$$

$$\phi_k = \frac{M}{T} \sum_{t=1}^{T} m_t \quad (7)$$

Since in the single-coupling scenario, each optimization variable is only related to the macro-user weighted rate and the micro-area weighted and rate in the interference-limited domain, the optimization problem can be decomposed into subproblems for each of the interference-limited domains. According to the equivalence relation in formula (7), the optimization problem can be decomposed into subproblems corresponding to each of the interference-limiting domains to find the optimal solution [25]. For the interference-limited domain formed by the macro-user:

$$\frac{df(\nabla 0, k, t)}{d\nabla 0, k, t} = \beta\alpha t - \sum_i \sum_j \beta\alpha t \quad (8)$$

α, β are counts of channel and time, respectively. The intersecting interfering micro base-station clusters are split into new interfering micro base-station clusters that do not intersect each other, and then the multi-user scheduling set of macro base-stations under the generalized model condition is solved by the single-couple scenario approach.

$$\Delta^{(m)} = \alpha_{0,m}, T_{0,m,t} - \sum_i \sum_j \alpha_{0,m}, T_{0,m,t} \quad (9)$$

$$\Delta^{(k)} = \delta_{0,m}, T_{0,m,t} - \sum_i \sum_j \delta_{0,m}, T_{0,m,t} \quad (10)$$

The forced-zero coding matrix for each candidate user needs to be calculated in each iteration, i.e., the value of formula (10) must be calculated several times. This will increase the computational complexity of the algorithm. In large-scale antenna systems, the performance of the max-ratio merge precoding is like the forced-zero precoding, but the coding vector of the former is only a complex conjugate of the vector of each user channel. For any macro user, calculating its max-ratio merge precoding does not require knowing the

Y. Hao, X. Qiu: MIMO Cross-Layer Secure Communication Algorithm for Cyber Physical Systems Based on Interference Strategies

IEEE Access

channel vectors of the other scheduling users; the coding vector can be derived from its channel vector alone [26]. Thus, the coding vector of a macro user can also be derived from the maximum ratio merge coding.

$$w_{0,k,t} = \frac{h_{0,k,t}^{U}}{\left\| h_{0,k,t} \right\|^2 \cdot \beta\alpha t} \tag{11}$$

U is a constant and has a normal value of 10^{-5}. WISPS usually require relatively high feasibility studies for new technologies, and a new scheme must undergo at least field experimental validation. However, the economic and time costs of field experimental validation are relatively high, so we first perform simulation of the new scheme, and the proposed scheme is theoretically analyzed and validated by simulation, and the optimal parameter configuration is obtained [27]. Then, the scheme with the optimal configuration obtained by simulation is used for field experimental validation. This section first examines the feasibility and superiority of the TAMLA-based authentication scheme proposed in this chapter using channel information from the industrial wireless communication environment provided by NIST to select the best scheme. Note that NIST does not use MIMO for its data collection, so we can only further investigate the impact of MIMO on this scheme in subsequent experimental validation.

The physical layer secure access authentication technique is the process of physical layer authentication, which not only determines the authenticity of a message during transmission and reception but also checks the integrity of the message to ensure that there is no attacker intrusion in the communication process [28]. Authentication is the process of determining whether the communicating parties match their claimed identities and whether they agree to the user's access to the network, to prevent attacks on the network by illegal users after access. Authentication is usually a very important process in the communication system, is the primary security line of the wireless network system, if an illegal user breaks through this line of defense to access the network, will be a fatal blow to the entire communication system after all the security measures will be useless. The physical layer secure access authentication technology has developed in recent years towards the direction of low complexity, low latency, and lightweight, providing an effective complement to traditional physical layer security.

B. CROSS-LAYER SECURE COMMUNICATION DESIGN

When a terminal makes a communication request, both parties need to confirm the identity of the other party to ensure the legitimacy of the identity; before exchanging sensitive information, they also need to confirm the privileges of the other party and control the terminal's access to stored data. Between wireless communication entities, such as between mobile devices and access networks, it is necessary to ensure the confidentiality and integrity of signaling data and user data transmitted over the air, while ensuring the privacy of user identities and preventing attackers from tracking users.

As user needs are changing rapidly, the security mechanisms of the network need to be adapted to the needs of users, so the network needs flexible security mechanisms that allow users to negotiate security levels with the access network. Also, the network's security mechanisms should have the ability to cope with the rapid growth of communication devices and be robust and scalable. The core network needs to authenticate access to users to confirm their identity and privileges, and the authentication conclusions should be time-sensitive. The communication parties encrypt the information and signaling data using a negotiated key through an encryption algorithm, thus preventing attackers from eavesdropping on secret information. Through packet authentication, the integrity of user information and signaling data can be verified to prevent legitimate information from being illegally tampered with by an attacker. The communicating parties can authenticate the device by its physical characteristics, e.g., RF fingerprint, as shown in Figure 2.

In addition to the new security requirements, many heterogeneous networks exist in the new generation of communication systems, and the number of industrial machine communication type devices has increased dramatically, including sensors, intelligent coordination vehicles, and robotic arms. To ensure transmission rates and adaptability to heterogeneous networks, flat all-IP networking structures can pose challenges for authentication systems in next-generation communication systems.

Wireless channels have broadcast characteristics, openness, and freedom, which bring many advantages to wireless communication networks, but also bring a lot of potential security threat problems and malicious attack risks. We summarize some of the attack types in Figure 2. Active attacks are defined as attacks that would prevent legitimate users from receiving messages, and common active attacks include message forgery, message tampering, and Dos attacks [29]. Impersonation and message replay are information forgery attacks. Illegal users can pretend to be legitimate users and imitate their communication behaviors if they successfully connect to the network. Dos attack is a blocking attack, which prevents the communication system from providing normal communication service by crashing or overwhelming the communication network. A type of attack that is easy to carry out.

A common passive attack is eavesdropping, which does not interfere with the receipt of information by the legitimate user, but allows the attacker to gain access to the legitimate user's communications data, resulting in the disclosure of information, especially some sensitive and confidential information. There is also an active eavesdropping attack, which differs from a passive eavesdropping attack in that the active eavesdropper sends messages to the recipient to obtain CSI estimates, while the passive eavesdropper remains silent. For individuals, eavesdropping attacks may leak personal identification information, personal passwords, privacy, etc., posing a threat to personal security and property security; for enterprises, especially the financial industry will cause
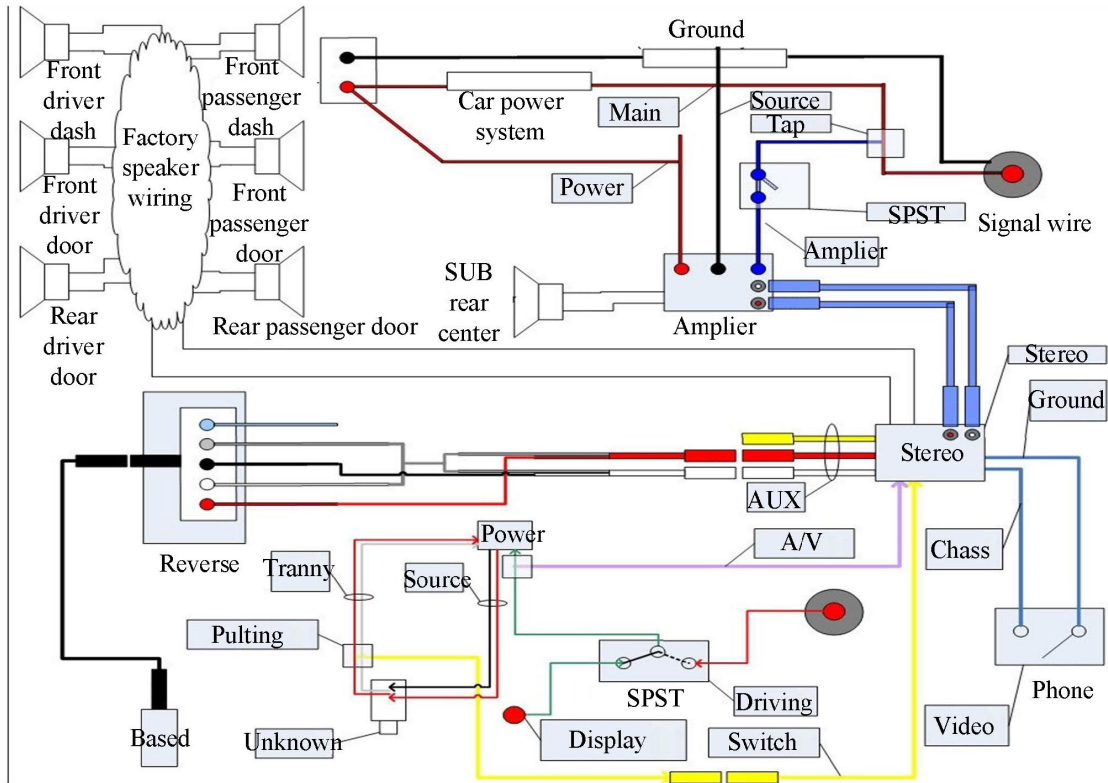
IEEE *Access*

Y. Hao, X. Qiu: MIMO Cross-Layer Secure Communication Algorithm for Cyber Physical Systems Based on Interference Strategies

FIGURE 2. Auxiliary enhanced security architecture based on channel information.

serious losses and threats; for national security is to ensure the security of information, national information security is one of the important aspects of national defense security, once the disclosure of confidential information, the harm is immeasurable. For active attacks, we need to make a comprehensive response plan due to the variety of attack types, strengthening security authentication and access at the same time, but also combined with malicious detection and other programs, early detection, and early resolution; for passive attacks, we need to strengthen the information encryption measures and do early prevention.

The authentication sequence received by terminal A is R_1, which is represented in the frequency domain [30].

$$R_1 = H \cdot S_1 + N \sum_i \sum_j \delta_{0,m}, T_{0,m,t} \qquad (12)$$

Terminal B receives an authentication response sequence of R_1'.

$$R_1' = H \cdot S_1' + N' \sum_i \sum_j \delta_{0,m}', T_{0,m,t}' \qquad (13)$$

Terminal S and Terminal N start data communication after completing the initial two-way authentication. CSI-based physical layer authentication is used in the data communication process. For each data information packet received by terminal H or terminal N, the channel information is extracted from it and the channel difference is obtained compared with the reference channel. Terminal H or terminal T uses the authentication model (14) to determine the channel difference value, and if it is legal, it continues to demodulate the information packet, and if it is illegal, it discards the packet [31].

The bi-directional authentication based on the physical channel is realized in D2D communication to avoid man-in-the-middle attacks; in the initial authentication, only a communication key needs to be stored to perform the initial authentication based on physical channel information, which no longer requires complex upper layer authentication and reduces the computational complexity of the initial authentication. The initial authentication step in this scheme is carried out directly in the terminal without going through the core network, which reduces the time delay of authentication; after the initial authentication, both parties to the D2D communication carry out packet authentication based on physical channel information for each received packet, which makes up for the lack of packet authentication in the D2D communication, protects user privacy and prevents malicious tampering of packets and other attacks by attackers.

IV. MIMO ANALYSIS DESIGN IN CYBER PHYSICAL SYSTEMS

A. MIMO DESIGN IN CYBER PHYSICAL SYSTEMS

The performance in wireless communication systems is largely dependent on the wireless channel environment, which is dynamic and unpredictable. Large-scale
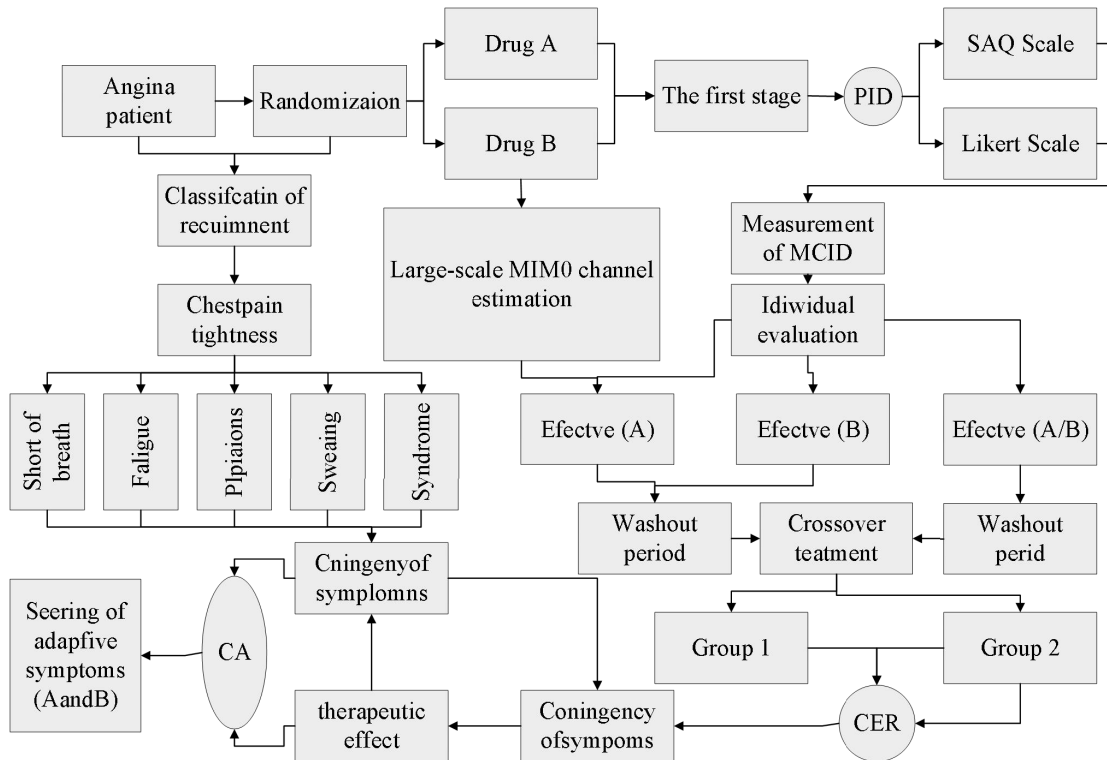
Y. Hao, X. Qiu: MIMO Cross-Layer Secure Communication Algorithm for Cyber Physical Systems Based on Interference Strategies

IEEE *Access*

FIGURE 3. Problems of Large-Scale MIMO Channel Estimation for Multiple Users.

MIMO relies on measuring the frequency response of the actual propagation channel. To do this, the user or base station sends a known training signal, and then the opposite receiver estimates the frequency response. Once the channel is estimated, the CSI must be utilized in time for the user's actions to significantly change the channel. Therefore, only a limited amount of time is available for training. In large-scale MIMO systems, where large antenna arrays are deployed on the base station side and the number of antennas set up on the user side is small or single, there are several band processing problems, especially with CSI acquisition [32]. The receiving end can take effective demodulation and detection of the received information based on CSIR to reduce the system error rate. Figure 3 vividly illustrates how the TDD system and FDD system, uplink and downlink channel status information collection and the problems to be handled. An improved MMSE channel estimation, i.e., a modified method for data-assisted MMSE estimation, is proposed in reference for turbo equalization in large-scale MIMO systems with frequency-guided contamination of the uplink, like conventional MIMO systems, based on the channel estimation method of the training sequence. The large-scale channel coefficients within the cell; from other perspectives, if the number of users is small, then channel estimation can be done using orthogonal training sequences [33].

Signal to Interference plus Noise Ratio (SINR) can affect the ability of large-scale MIMO systems to achieve their achievable Signal to Interference plus Noise Ratio due to channel estimation errors. Also, frequency-guided contamination can lead to uncertainty in channel state information due to interference. The accuracy of the estimated channel can effectively mitigate interference, especially between adjacent subsectors. Also, channel estimation in large-scale MIMO systems will pose technical challenges because many antennas will increase the number of frequency guides in the channel estimation process, thus increasing the impact of frequency guide contamination. Previous work in reference has addressed the effects of frequency-guide training during channel estimation due to frequency-guide contamination in downlink and uplink transmissions of large-scale MIMO systems.

In reference [31] it is proposed to modify the Discrete Fourier Transform (DFT) based channel estimation technique for large-scale MIMO systems by iterative and most importantly tapering methods to mitigate the frequency-guide contamination.

For temporally, spatially, or frequency selective channels, the known channel state information will effectively enhance the system channel capacity. In large-scale MIMO systems, channels are more likely to experience selective decay in time, space, or frequency, and when complete or partial channel state information is available, the system multiplexing gain can be significantly improved when pre-coding the signals sent from the base station. Therefore, in Chapter 2 of this paper, a data-assisted channel estimation algorithm is proposed to

IEEE Access

Y. Hao, X. Qiu: MIMO Cross-Layer Secure Communication Algorithm for Cyber Physical Systems Based on Interference Strategies

accurately obtain channel state information and improve system capacity.

For user grouping algorithm in multi-user large-scale MIMO systems, it is mainly divided into two categories: one is the study of user grouping algorithm based on FDD mode; the other is the study of user grouping algorithm based on TDD mode. For TDD systems, channel reciprocity can be used to estimate the channel characteristics of the downlink by transmitting training sequences on the uplink. However, for FDD systems, the channel characteristics need to be estimated from the feedback information of the frequency-conducting sequences, which results in the system consuming a large amount of spectrum and power resources. Therefore, the current academic research on the user grouping algorithm for FDD systems mainly focuses on reducing the waste of resources caused by the frequency guide information and CSI channel feedback during user grouping, but the research on the user grouping algorithm for TDD systems is more extensive.

In FDD systems, the literature proposes a two-layer pre-coding scheme to reduce the overhead of channel estimation and decomposes the pre-coding into inter-group and intra-group pre-coding to derive user grouping. Meanwhile, the authors summarize and propose a series of similar grouping algorithms, such as k-means clustered user grouping algorithm, weighted likelihood similarity measure grouping algorithm, subspace projection-based similarity measure grouping algorithm, and Fusin-Study similarity measure grouping algorithm. The newly generated group center values are further calculated by calculating the chord length distance of the eigenvectors of the channel correlation matrix between the users. Grouping is determined by comparing the minimum chord length distance of the remaining users with the group center. However, the algorithm needs to determine the number of groups before grouping and does not allow for flexible dynamic grouping and the system does not achieve optimal performance. To address this problem, the hierarchical multi-user grouping algorithm is given in the literature. The algorithm starts by dividing each user into a user group, then performs a series of successive mergers based on certain conditions, and finally, the number of desired groups or all users are divided into one group as the termination condition of the algorithm.

B. DESIGN ANALYSIS OF PERFORMANCE METRICS

We have mentioned the short-time interoperability, temporal variability, randomness, and non-clonability of the wireless channel, and these natural characteristics provide a foothold for us to design a physical layer security access authentication scheme. CSI as one of the typical physical layer channel features in addition to the above characteristics, there are also incomplete estimates of the characteristics of the wireless channel because the decay is random, the detection and estimation of the signal there will be errors, which will lead to unpredictable changes in the authentication process; on the other hand, the wireless communication system in the

environment once the change in the physical layer at different times observed properties of the physical layer on the There may be potential de-correlation that affects the performance of authentication. Based on the above two points, it is important to note that the physical layer secure access authentication algorithm should be designed to be highly robust against the incomplete estimation of CSI and the negative impact of interference and noise in the communication environment on the performance of the authentication algorithm.

Although the environment can cause channel variation, there must also be feature invariance in the CSI, which is known to be frequency-dependent. We call this the "blind extraction" of features, and we use it to extract CSI's depth features or to analyze the contextual links between different samples as sequence data. Therefore, it is feasible to design a physical layer secure access authentication scheme based on CSI and using a deep neural network algorithm, as shown in Figure 4.
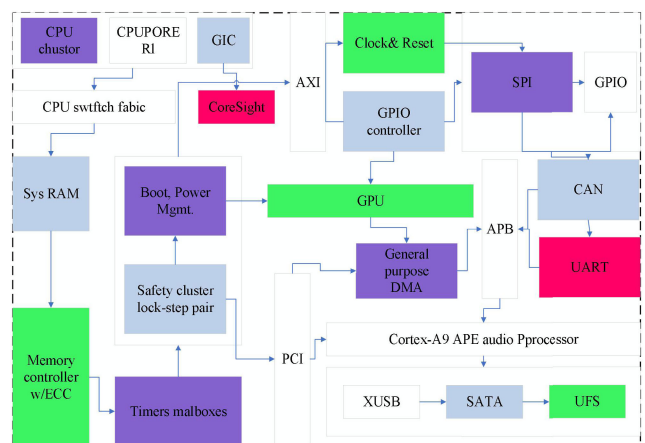

FIGURE 4. Performance index design.

In addition to this, there is a very important concept in machine learning called generalization capability. The prediction error of a model on training data is called empirical error, and the prediction error on test data is called generalization error, and we want machine learning algorithms to be able to perform well not only on the dataset they are currently processing but also on datasets of the same nature, which is the generalization ability of machine learning.

A greater generalization ability also means a greater ability to adapt to fresh datasets, which can also be popularly understood as the ability to lift and hold. The basic reason for poor generalization ability is that the optimization of the loss function does not reach the global optimum without considering the influence of insufficient data. The ability to generalize CSI data ensures the reliability of physical layer security access authentication.

Commonly used authentication or detection performance metrics include accuracy, detection rate, miss rate, and false alarm rate, where the sample space for accuracy is the set of legitimate and illegitimate samples, the sample space for

Y. Hao, X. Qiu: MIMO Cross-Layer Secure Communication Algorithm for Cyber Physical Systems Based on Interference Strategies

IEEE *Access*

detection rate and miss rate is the set of illegitimate samples, and the sample space for false alarm rate is the set of legitimate samples. The probability is the accuracy rate when the legitimate receiver correctly determines the legitimacy and illegitimacy of the information source [34].

$$Acc = P_r(H_0 | H_0) \cdot P_r(H_1 | H_1) \qquad (14)$$

H is the set of corresponding symbols. According to the binary hypothesis model in equation (12), the probability of detection where the transmitter is illegal and the authentication result is also judged to be illegal is the probability that.

$$dr = P_r(H_r | H_r + H_0) \qquad (15)$$

The miss rate is the rate at which the receiver judge's illegal information is legitimate.

$$Mdr = P_r(H_r | H_r + H_1) = M(1 - dr) \qquad (16)$$

The probability that a transmitter is legal but is falsely judged by the receiver to be illegal is a false alarm rate.

$$far = P_r(H_r | H_r + H_{r-1}) \qquad (17)$$

Accuracy, detection rate, miss rate, and false alarm rate are usually affected by the choice of the threshold value and may not represent the optimal state of the system. For example, Scheme A uses the optimal threshold value, while Scheme B does not use the optimal threshold value. The accuracy of scheme A is greater than that of scheme B, but this does not mean that scheme B, which adopts the optimal threshold value, is also necessarily worse than scheme A. To improve the performance of the communication system, this paper also adopts MIMO technology, which uses the spatial diversity of multiple antennas to enhance communication reliability. The transmitter transmits the same information from each antenna, and the receiver performs channel estimation on the information received by the multiple antennas and then averages the estimation results of each transceiver antenna pair to obtain the final channel estimation results. For physical layer authentication or detection, we only need to estimate the channel information of the received signal using the frequency guide and do not need to solve the complete information packet. Therefore, interpolation is not required in the experiments of this paper. When the communication experiments involving four antennas are performed, the two USRP devices are connected in series as a group and synchronized with an external clock to achieve the effect of four transmit and four receive. The experimental devices were debugged and the parameter settings that caused the lowest packet loss rate were selected, including center frequency, bandwidth, transmit power, transmit gain, and modulation mode. Also, the number of subcarriers was selected as the number with relatively low overhead after considering the communication performance and computational complexity.

V. RESULTS ANALYSIS
A. ANALYSIS OF SIMULATION RESULTS
The learning rate is initialized to 10^{-4} and the learning rate is halved after 20 epochs. The simulation results are shown in Figure 5.
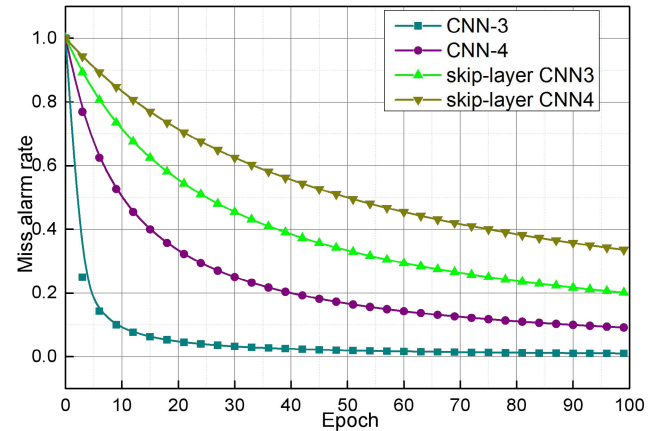
FIGURE 5. The learning rate is initialized to 10-4 and the learning rate decreases by half after 20 epochs.

A data storage module is added to the LabVIEW program at Bob's end to store the following data in txt format: CSI data for the legal channel from Alice to Bob and CSI data for the illegal channel from Eve to Bob. The collected CSI samples are two complex sets of data of size 4000*128, i.e. Alice and Eve send 4000 frames to Bob, and the number of CSI samples is 128. The real and imaginary parts of the CSI are stored separately to form four txt files, namely " Alice-real", "Alice-image", "eve-real", "eve-image". The data size of each file is 4000*128, and the partial data is shown in Figure 6.
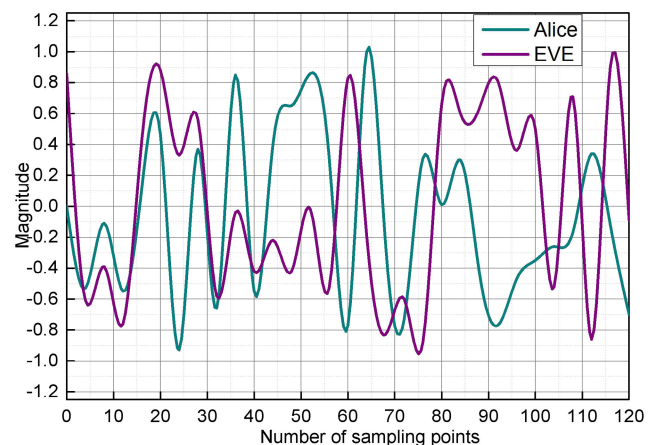
FIGURE 6. Partial measured data.

The CNN, skip-layer CNN and RNN algorithms proposed in this paper have good authentication performance by building a USRP authentication system to collect real channel state information, verifying the deep neural network algorithms

proposed in this paper, and then comparing and analyzing them with KNN and SVM algorithms. With the continuous integration and development of machine learning and deep learning with wireless communication systems, and the continuous advancement of chip technology, wireless communication networks are constantly moving towards automation and intelligence, and intelligent physical layer security access authentication technology will be one of the information security technologies that are constantly being researched and promoted.

With the increase of epoch, the false alarm probability and leakage probability of the four networks decreased significantly and stabilized after a while. CNN-3 has a slightly better authentication effect than CNN-4, but the convergence time of CNN-3 is shorter because the deeper the network, the higher the computational complexity. In terms of the convergence speed, the skip-layer CNN is faster, indicating that although the network becomes more complex, the feature map is multiplexed, the computation volume is greatly reduced, and the data flow becomes faster. The simulation results of several deep neural networks presented in this paper are compared comprehensively, and the change of false alarm probability with iteration period epoch is shown in Figure 7, the trend of missing alarm probability is similar so it is not shown again. CNN, SVM, and deep neural network algorithm simulation results are summarized in Figure 7.
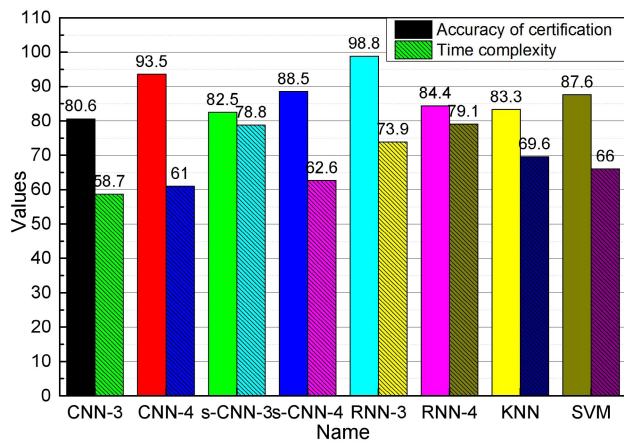

FIGURE 7. Comparison of the results of different algorithms.

As we can see in Figure 6, the difference in authentication accuracy between CNN, skip-layer CNN, and RNN for legitimate and illegitimate users is not very large because of the powerful "mining" ability of neural networks for depth features, which is similar in this experiment. In terms of authentication accuracy, the skip-layer CNN has the highest authentication accuracy, followed by the CNN, the RNN comes in third, the SVM has 92.1%, and the KNN has 87.3%, which is the worst exhibits better feature characterization capabilities. In terms of time complexity, CNN has the fastest convergence speed because CNN does not require many parameters and processes such as iterations of gradient

descent like neural networks, but is purely based on spatial distance computation.

CNN has the highest time complexity for SVM, and several deep neural networks have greater time complexity than CNN, but much less than SVM and several neural networks compare to RNNs. The time complexity of the strategy is the lowest.

B. ANALYSIS OF STRATEGY RESULTS

The performance of the proposed downlink pre-coding algorithm is verified based on numerical simulation results, and the impact of user scheduling on the system and rate under cell boundary expansion is discussed. In this chapter, the 3GPP path loss model is used, and the parameters are shown in Figure 8.
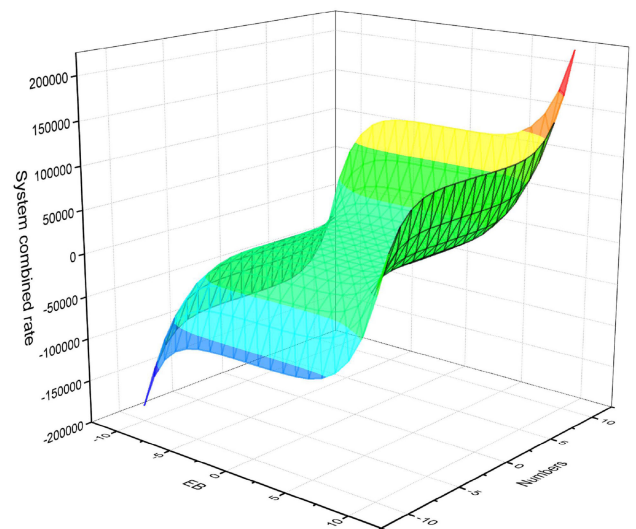

FIGURE 8. Schematic representation of the relationship between system and rate with REB (AEB,) and several SAP antennas N.

When the number of SAP antennas is fixed, the system user and rate will reach a maximum, i.e., optimum, in the case of cell boundary expansion. Once the optimal REB is exceeded, the system users and rates start to degrade due to the long distance from the SAP and fewer degrees of freedom to perform multi-user interference suppression. The best user scheduling strategy is for users outside the optimal boundary to communicate with the MBS rather than with the SAP. However, the rate of system and rate increase is not constant, and as the total number of users increases to a certain point, the system and rate increase slows down or even flattens out.

This is because the transmit power of SAP is limited, and as increased users communicate with SAP, the power received by each user becomes smaller and the interference between users increases, resulting in the system and rate no longer increasing. A malefactor's scheme for downlink data transmission in large-scale MIMO two-layer heterogeneous networks based on channel estimation under cell boundary expansion is investigated.

Y. Hao, X. Qiu: MIMO Cross-Layer Secure Communication Algorithm for Cyber Physical Systems Based on Interference Strategies

IEEE *Access*

This chapter gives the range definitions and the range extension base values for different cell boundary extensions, and demonstrates the relationship between the different boundaries. In the TDD mode, based on the uplink channel estimation results, a downlink pre-coding scheme is designed to eliminate the intercell interference problem caused by the cell expansion. This chapter mainly includes the following innovations and conclusions, as shown in Figure 9.
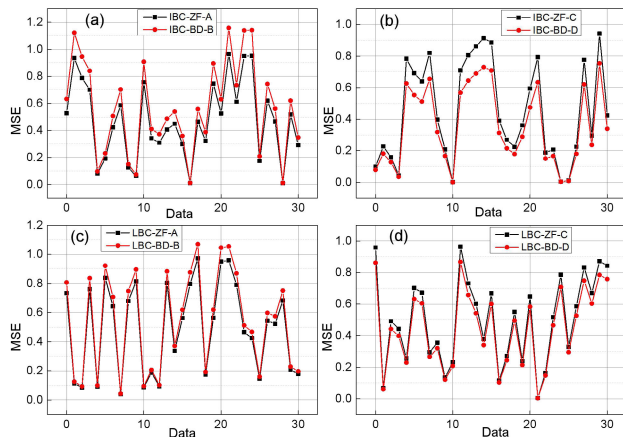

FIGURE 9. REB versus system and rate based on the estimated channel under backhaul capacity constraint.

Large-scale MIMO-based downlink data transmission in heterogeneous networks is investigated. Considering the rich spatial freedom of large-scale MIMO and the influence of the transmit power difference between MBS and SAP in heterogeneous networks, micro-area edge expansion is introduced to achieve MBS traffic offloading in heterogeneous networks to improve the fairness of heterogeneous networks. The micro-area boundary cannot be extended indefinitely, and different extension boundaries of the micro-area are given according to the user uplink firing power and the firing power between MBS and SAP, and the extension boundary base value is given. The CSI between MBS, SAP, and users in the heterogeneous network is obtained by uplink training, and the heterogeneous network downlink pre-coding design based on the CSI obtained is carried out. Different pre-coding schemes are used to improve the system performance for the differences in the number of antennas and transmit power of MBS and SAP. The ZIFF pre-coding algorithm is introduced to reduce the inter-area interference caused by the excessive MBS transmitting power to other users in the micro area. To reduce the interference between users in the micro area, the introduction of the BD pre-coding scheme to achieve the micro area users and rate maximization, as shown in Figure 10.

The average training time of the DT scheme is 6×10^{-2} and the average prediction time is 1×10^{-3} s. Although the accuracy of the DT scheme improves by 0.1042 or 23.25% over the TD scheme, its prediction time is also 5 orders of magnitude higher. To some extent, the prediction time reflects
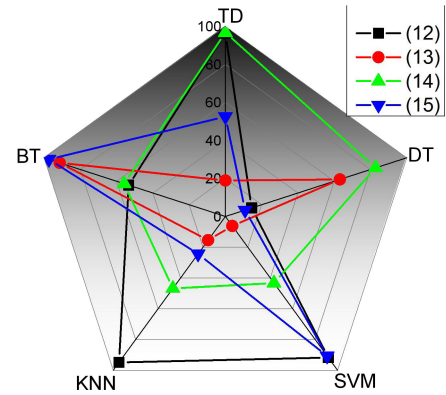

FIGURE 10. Comparison of average accuracy.

the computational complexity and authentication processing delay; the longer the prediction time, the higher the computational complexity and the longer the authentication delay. Therefore, the accuracy improvement of the DT scheme is based on the sacrifice of authentication latency and computational complexity.

It can be seen from Figure 10 that the scheme using channel difference formula (14) and SVM is the optimal scheme with the highest average accuracy and average improvement, 0.5638 and 0.1175, respectively. The suboptimal scheme is the scheme using channel difference formula (16) and DT. When the channel difference formula (17) is used, the accuracy rate of all ML-based schemes decreases, i.e., the optimal scheme when the channel difference formula (15) is used is the TD scheme, not the ML scheme.

C. ANALYSIS OF PERFORMANCE INDICATOR RESULTS

The use of the original channel matrix as input maximizes the retention of channel information obtained from channel estimation, but it also retains noise and redundancy, and substantially increases the computational complexity, and reduces the sample density. Therefore, it is necessary to reduce the dimensionality of the channel matrix while preserving as much valid channel information as possible. when k = 8188, the sampled matrix dimension is k × 1, k = 32, 64, 128, 256, 8188. Matrices are equal to the original matrices. The authentication accuracy of the ML scheme using different channel matrix dimensions is shown in Figure 11. When the input matrix dimension decreases, the authentication accuracy not only does not decrease but also increases. Among them, the BT authentication scheme using a 128-dimensional channel matrix is the optimal scheme with an average accuracy rate of 0.7710.

The accuracy of the BT scheme with a 128-dimensional channel matrix is significantly higher than the accuracy of the D scheme. At acquisition point 3, the BT scheme with a 128-dimensional channel matrix has a maximum accuracy of 1, which is ideal for authentication; at acquisition point 118, it has an accuracy of 0.9767, which is also very close to ideal; only at acquisition point 33 is the accuracy lower than the TD scheme, with a minimum value of 0.49.
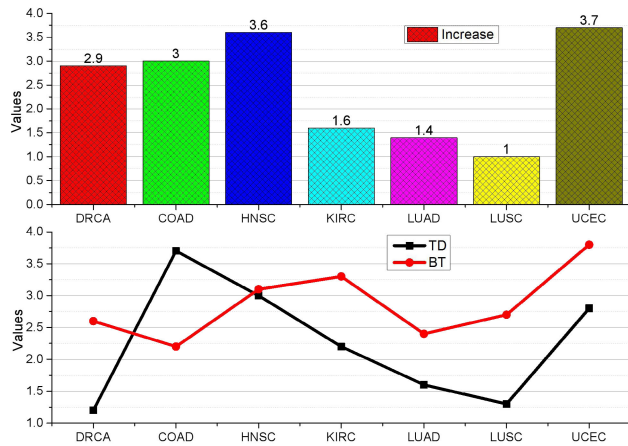
IEEE *Access*

Y. Hao, X. Qiu: MIMO Cross-Layer Secure Communication Algorithm for Cyber Physical Systems Based on Interference Strategies

FIGURE 11. Certification accuracy of BT with a 128-dimensional channel matrix and TD scheme.

The BT scheme with a 128-dimensional channel matrix has a maximum accuracy of 1, which is ideal for authentication. The average improvement rate of the certification scheme is 0.2467 relative to the TD scheme using formula (15). The average training time of the BT certification scheme using the 128-dimensional channel matrix is 1.26 s, and the average prediction time is 2×10^{-2}, which significantly reduces the computation compared to the BT certification scheme using the 8188-dimensional channel matrix.

From Figure 12, the interference effect is affected by the number of interference times, and different interference times will produce different effects, to maximize the interference effect, the jammer needs to select the optimal number of interference times. Also, it can be seen from Figure 12 that the optimal energy distribution scheme is different for different systems with arbitrary fixed jamming times and channels. Therefore, to obtain the optimal jamming strategy, it is necessary for the jammer to fully understand the operating parameters of the system to be jammed, to obtain the optimal jamming strategy.
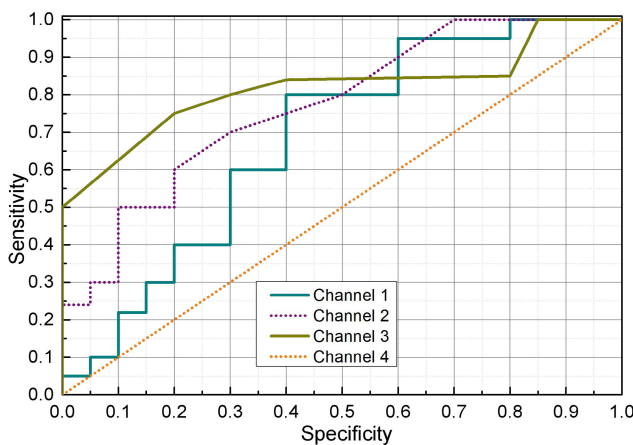
The problem of maximizing jamming strategy on two-hop remote estimation based on the relay in CPS is investigated, mainly considering the optimal jamming strategy in both cases of constant scheduling and dynamic scheduling, and the mixed-integer planning problem of maximizing jamming effect in the energy-limited case is established based on the terminal estimation error; for the constant scheduling case, the CD algorithm is proposed by proving the monotonically increasing nature of estimation error for packet loss rate; for the dynamic energy scheduling, the DED algorithm is proposed to obtain the optimal channel selection and the corresponding energy scheduling based on the analysis of MDP.

CNN, skip-layer CNN, RNN, CNN, and SVM are simulated and verified using the measured data, and the simulation results are summarized in Figure 12. The smaller the variance of the credibility is, the more stable the value of the credit is taken. Therefore, we choose R6 with the smallest variance as the channel difference algorithm for subsequent experiments. The channel variance obtained according to formula (15) is shown in Figure 12. Where the legal channel difference is the channel different from the normal node and the illegal channel difference is the channel different from the cloned node.

As can be seen from Figure 13, it is difficult to distinguish between legal and illegal channel differences, and even, some of the legal channel differences are larger than the illegal channel differences. However, when we accumulate the channel difference values and obtain the credibility R6 of the legal and cloned nodes, we find that the boundaries between them become clear. The input to the single-point detection scheme is 1 or more reputation degrees of a single node, and the output is the detection result of that node. Whereas, the multipoint integrated detection scheme has an input of 1 reputation degree for a group of nodes and the output is the detection result for that group of nodes.
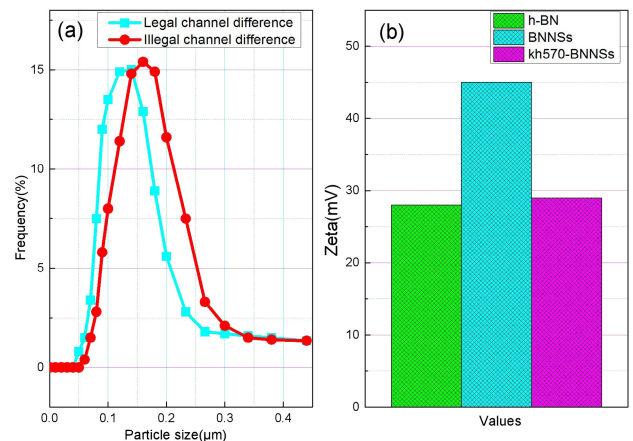

FIGURE 12. Influence of jamming times on jamming effect under different channels.

FIGURE 13. Channel difference.

The advantage of the single-point detection scheme is that it can locate the ID of a malicious node, but the disadvantage

Y. Hao, X. Qiu: MIMO Cross-Layer Secure Communication Algorithm for Cyber Physical Systems Based on Interference Strategies

IEEE Access

is that it is susceptible to chance errors. The advantage of the multi-point integrated detection scheme is that it is not susceptible to chance error and can accurately determine whether there is a malicious node in a group of nodes, but the disadvantage is that it cannot locate the ID of a malicious node.

However, as the number of hidden layers and neurons increases, the computational complexity of the scheme increases significantly. Therefore, users need to set the number of hidden layers and neurons according to their computing power. Also, users can combine the multi-point integrated detection scheme with the single-point detection scheme to first locate the group where the malicious node exists and then locate the ID of the malicious node.

VI. CONCLUSION

To address the problem that large-scale MIMO systems need to obtain accurate CSI, a large-scale MIMO uplink training study in TDD mode is conducted, and the influence of frequency-guide pollution on the system performance during the uplink training is analyzed. Based on the multiplexing guide-frequency allocation strategy, the efficiency of large-scale MIMO downlink spectrum under different guide-frequency multiplexing factors is studied, and a cell silence-based large-scale MIMO guide-frequency pollution cancellation scheme is presented. The scheme achieves the asynchronous transmission of frequency-guided sequences among different users in different cells by cell silence, thus effectively avoiding the influence of frequency-guided pollution. To further improve the transmission efficiency of large-scale MIMO systems and reduce the guide-frequency overhead of the system, the intelligent frequency allocation scheme is proposed. The scheme is based on the user with the most interference to allocate the best quality BN signal and the user with the least interference to allocate the worst quality BN signal. For multi-channel based remote state estimation in CPS, when the jammer uses sensors to send observations to the estimator via dynamically changing channels, this paper develops a model for dynamic channel sensing by sensors with cognitive capabilities and proposes an effective online learning-based algorithm for selecting the dynamic channel sequence by transforming the problem of maximizing the jamming effect into an online learning-based model for selecting the channel at each moment. For the case of remote estimation-based joint control in CPS, this paper establishes the integer planning problem for energy-limited dryers to enhance the interference effect by maximizing the LQG control cost function and proposes an algorithm for approximating the optimal policy in the case of sensors with a single interface by transforming the optimization problem into a problem for solving linear groups of equations. In this paper, the algorithm for an effective interference policy when sensors with multiple interfaces use multiple channels at a time is also presented.

REFERENCES

[1] C.-T. Cheng, T.-Y. Ho, T.-Y. Lee, C.-C. Chang, C.-C. Chou, C.-C. Chen, I.-F. Chung, and C.-H. Liao, "Application of a deep learning algorithm for detection and visualization of hip fractures on plain pelvic radiographs," *Eur. Radiol.*, vol. 29, no. 10, pp. 5469–5477, Oct. 2019.

[2] H.-Z. Hu, X.-B. Feng, Z.-W. Shao, M. Xie, S. Xu, X.-H. Wu, and Z.-W. Ye, "Application and prospect of mixed reality technology in medical field," *Current Med. Sci.*, vol. 39, no. 1, pp. 1–6, Feb. 2019.

[3] S. Sylaiou, K. Mania, I. Paliokas, L. Pujol-Tost, V. Killintzis, and F. Liarokapis, "Exploring the educational impact of diverse technologies in online virtual museums," *Int. J. Arts Technol.*, vol. 10, no. 1, pp. 58–84, Apr. 2017.

[4] G. Priestnall, E. FitzGerald, S. Meek, M. Sharples, and G. Polmear, "Augmenting the landscape scene: Students as participatory evaluators of mobile geospatial technologies," *J. Geography Higher Educ.*, vol. 43, no. 2, pp. 131–154, Apr. 2019.

[5] I. Pachoulakis, D. Tsilidi, and A. Analyti, "Computer-aided rehabilitation for the carpal tunnel syndrome using exergames," *Adv. Image Video Process.*, vol. 6, no. 2, p. 44, Apr. 2018.

[6] M. A. Martens, A. Antley, D. Freeman, M. Slater, P. J. Harrison, and E. M. Tunbridge, "It feels real: Physiological responses to a stressful virtual reality environment and its impact on working memory," *J. Psychopharmacology*, vol. 33, no. 10, pp. 1264–1273, Oct. 2019.

[7] H.-Z. Hu, X.-B. Feng, Z.-W. Shao, M. Xie, S. Xu, X.-H. Wu, and Z.-W. Ye, "Application and prospect of mixed reality technology in medical field," *Current Med. Sci.*, vol. 39, no. 1, pp. 1–6, Feb. 2019.

[8] Z. Al-Kassim and Q. A. Memon, "Designing a low-cost eyeball tracking keyboard for paralyzed people," *Comput. Elect. Eng.*, vol. 58, pp. 20–29, Feb. 2017.

[9] M. A. Martens, A. Antley, D. Freeman, M. Slater, P. J. Harrison, and E. M. Tunbridge, "It feels real: Physiological responses to a stressful virtual reality environment and its impact on working memory," *J. Psychopharmacology*, vol. 33, no. 10, pp. 1264–1273, Oct. 2019.

[10] R. Hu, T. Fan, J. Yang, H. Xiao, Y. Liu, and M. Lu, "Ultrasound and microwave technology for flake-TiO_2 growth and immobilization on cotton fabrics in micro-dissolution process," *Mater. Chem. Phys.*, vol. 249, Jul. 2020, Art. no. 123036.

[11] P. Rahi, S. P. Sood, and R. Bajaj, "Smart platforms of air quality monitoring: A logical literature exploration," in *Proc. Int. Conf. Futuristic Trends Netw. Comput. Technol.*, Nov. 2019, pp. 52–63.

[12] A. Keshavarzi and W. van den Hoek, "Edge intelligence-on the challenging road to a trillion smart connected IoT devices," *IEEE Des. Test.*, vol. 36, no. 2, pp. 41–64, Apr. 2019.

[13] S. Cespedes, J. Salamanca, A. Yanez, and D. Vinasco, "Group cycling meets technology: A cooperative cycling cyber-physical system," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 8, pp. 3178–3188, Aug. 2019.

[14] M. Manikandan, A. Deenadayalan, A. Vimala, J. Gopal, and S. Chun, "Clinical MALDI mass spectrometry for tuberculosis diagnostics: Speculating the methodological blueprint and contemplating the obligation to improvise," *TrAC Trends Anal. Chem.*, vol. 94, pp. 190–199, Sep. 2017.

[15] S. Colantonio, G. Coppini, D. Giorgi, M. A. Morales, and M. A. Pascali, "Computer vision for ambient assisted living: Monitoring systems for personalized healthcare and wellness that are robust in the real world and accepted by users, carers, and society," *Comput. Vis. Assistive Healthcare*, vol. 2018, pp. 147–182, Jan. 2018, doi: 10.1016/B978-0-12-813445-0.00006-X.

[16] A. Seba, N. Nouali-Taboudjemat, N. Badache, and H. Seba, "A review on security challenges of wireless communications in disaster emergency response and crisis management situations," *J. Netw. Comput. Appl.*, vol. 126, pp. 61–150, Jan. 2019.

[17] C. Fang, P. Zhang, and X. Qi, "Digital and intelligent liver surgery in the new era: Prospects and dilemmas," *EBioMedicine*, vol. 41, pp. 693–701, Mar. 2019.

[18] R. Alarcon, F. Wild, C. Perey, M. M. Genescà, J. G. Martínez, J. X. Ruiz Martí, M. J. Simon Olmos, and D. Dubert, "Augmented reality for the enhancement of space product assurance and safety," *Acta Astronautica*, vol. 168, pp. 191–199, Mar. 2020.

[19] P.-U. Malmström, S. Agrawal, M. Bläckberg, B. PJ, B. Malavaud, D. Zaak, and H. GG, "Non-muscle-invasive bladder cancer: A vision for the future," *Scandin. J. Urol.*, vol. 51, no. 2, pp. 87–94, Mar. 2017.

[20] E. I. Liem and T. M. de Reijke, "Can we improve transurethral resection of the bladder tumour for nonmuscle invasive bladder cancer?" *Current Opinion Urol.*, vol. 27, no. 2, pp. 149–155, Mar. 2017.

[21] F. Chen, Q. Wu, D. Song, X. Wang, P. Ma, and Y. Sun, "Fe₃O₄ PDA immune probe-based signal amplification in surface plasmon resonance (SPR) biosensing of human cardiac Troponin I," *Colloids Surf. B, Biointerfaces*, vol. 177, pp. 105–111, May 2019.

[22] A. M. Doshi, W. H. Moore, D. C. Kim, A. B. Rosenkrantz, N. R. Fefferman, D. L. Ostrow, and M. P. Recht, "Informatics solutions for driving an effective and efficient radiology practice," *RadioGraphics*, vol. 38, no. 6, pp. 1810–1822, Oct. 2018.

[23] E. I. Konstantinidis, G. Bamparopoulos, and P. D. Bamidis, "Moving real exergaming engines on the Web: The webFitForAll case study in an active and healthy ageing living lab environment," *IEEE J. Biomed. Health Informat.*, vol. 21, no. 3, pp. 859–866, Apr. 2016.

[24] I. Ishafit, T. K. Indratno, and Y. D. Prabowo, "Arduino and LabVIEW-based remote data acquisition system for magnetic field of coils experiments," *Phys. Educ.*, vol. 55, no. 2, Dec. 2019, Art. no. 025003.

[25] H. Wang, E. Sun, F. Feifei, and S. Liu, "A framework of a 3D DCPCS based on UWB positioning in underground mining," *Int. J. Georesources Environ.*, vol. 4, no. 3, pp. 153–162, 2018.

[26] P. Pouladzadeh, P. Kuhad, S. V. B. Peddi, A. Yassine, and S. Shirmohammadi, "Food calorie measurement using deep learning neural network," in *Proc. IEEE Int. Instrum. Meas. Technol. Conf.*, May 2016, pp. 1–6.

[27] S. Ding, L. Feng, J. Wu, F. Zhu, Z. Tan, and R. Yao, "Bioprinting of stem cells: Interplay of bioprinting process, bioinks, and stem cell properties," *ACS Biomaterials Sci. Eng.*, vol. 4, no. 9, pp. 3108–3124, Jul. 2018.

[28] S. Balasubramanian, J. Chenniah, G. Balasubramanian, and V. Vellaipandi, "The era of robotics: Dexterity for surgery and medical care: Narrative review," *Int. Surg. J.*, vol. 7, no. 4, pp. 1317–1323, Mar. 2020.

[29] P. Ji, S. U. Baek, C. H. Park, S. S. Lee, Y. E. Im, and Y. Choi, "Inline fiber optic power sensor featuring a variable tap ratio based on a tightly focused femtosecond laser inscription," *Opt. Exp.*, vol. 26, no. 12, pp. 14972–14981, Jun. 2018.

[30] A. Lapico, M. Sankupellay, L. Cianciullo, T. Myers, D. A. Konovalov, D. R. Jerry, P. Toole, D. B. Jones, and K. R. Zenger, "Using image processing to automatically measure pearl oyster size for selective breeding," in *Proc. Digit. Image Comput., Techn. Appl. (DICTA)*, Dec. 2019, pp. 1–8.

[31] S. Pearce and S. Daneshmand, "Enhanced endoscopy in bladder cancer," *Current Urol. Rep.*, vol. 19, no. 10, p. 84, Oct. 2018.

[32] T.-Y. Tai, H. H.-J. Chen, and G. Todd, "The impact of a virtual reality app on adolescent EFL learners' vocabulary learning," *Comput. Assist. Lang. Learn.*, vol. 2020, pp. 1–26, Apr. 2020, doi: 10.1080/09588221.2020.1752735.

[33] A. Tou, H.-H. Kim, H. Einaga, Y. Teramoto, and A. Ogata, "Ozone-assisted catalysis of CO: *In situ* Fourier transform IR evidence of the cooperative effect of a bimetallic ag-pd catalyst," *Chem. Eng. J.*, vol. 355, pp. 380–389, Jan. 2019.

[34] T. Rikakis, A. Kelliher, J. Choi, J.-B. Huang, K. Kitani, S. Zilevu, and S. L. Wolf, "Semi-automated home-based therapy for the upper extremity of stroke survivors," in *Proc. 11th Pervas. Technol. Rel. Assistive Environ. Conf.*, Jun. 2018, pp. 249–256.

YUKAI HAO was born in Shandong, China, in 1979. He received the Ph.D. degree from the Wuhan University of Technology, in 2012. He currently works with Tibet University and with the Wuhan University of Technology. He has published a total of ten articles. His research interest includes information management.

XIN QIU was born in Hubei, China, in 1978. She currently works with the Wuhan University of Technology. Her research interests include marketing management and information management.

● ● ●