Network selection model of terminal security based on ultra-dense heterogeneous network

Wei Ao, Kaiwen Hou, Zhenkun Zhong, Nan Tang, Xi Liu and Hao Dong*

Digital Research Branch of Inner Mongolia Power (Group) Co., Ltd, Hohhot, Inner Mongolia, China
Email: impcsyy_ao@163.com
Email: 15352845003@163.com
Email: zhongzhenkun1111@163.com
Email: 15661097116@163.com
Email: 15547161105@163.com
Email: impcsyy_dh@163.com
*Corresponding author

Abstract: How to design an ultra-dense heterogeneous wireless network selection algorithm to improve the network access security level and improve the quality of user experience in the network selection process has become a hot issue in current research. In order to improve terminal security and end user experience, this paper designs a network slice selection algorithm based on SDN and terminal security. At the same time, considering the possible negative unevenness between the two kinds of slices, an adaptive slice adjustment mechanism is proposed. Combined with data transmission rate and access blocking rate, the comprehensive benefit function is constructed, and the optimal slice resource allocation strategy is solved by ant colony optimisation algorithm, and then the optimal access slice of the terminal is designed. The experimental results show that the algorithm can reduce the access blocking rate and average load of the network, and effectively improve the service satisfaction of users. Therefore, the algorithm model proposed in this paper can provide a reliable reference for the subsequent terminal security network selection model, and also provide a more reliable network foundation for end users.

Keywords: ultra-dense heterogeneous network; terminal; secure networks; select model.

Reference to this paper should be made as follows: Ao, W., Hou, K., Zhong, Z., Tang, N., Liu, X. and Dong, H. (2024) 'Network selection model of terminal security based on ultra-dense heterogeneous network', *Int. J. Information and Communication Technology*, Vol. 25, No. 11, pp.69–89.

Biographical notes: Wei Ao holds a Master's degree in Engineering and is a Senior Engineer. He is a member of the Communist Party of China and graduated from Inner Mongolia University with a Bachelor's degree in Computer Science and Technology in July 2004. In the same year, he started working at Inner Mongolia Power Information and Communication Company. In June 2014, he graduated with a Master's degree in Engineering from North China Electric Power University with a major in Industrial Engineering. In September 2023, he became the Deputy General Manager of Inner Mongolia Power Digital Research Company, responsible for scientific and technological innovation and production operation management. He has won three technical

innovation achievements in the autonomous region's power industry, one second prize in group company level management innovation achievements, five third prizes in scientific and technological progress awards, and four utility patents.

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

Zhenkun Zhong graduated from Jianqiao College, Heilongjiang University in June 2013 with a Bachelor's degree. He worked at the Information and Communication Branch of Inner Mongolia Electric Power (Group) Co., Ltd. from July 2013 to November 2023, and at the Digital Research Branch of Inner Mongolia Electric Power (Group) Co., Ltd. from November 2023 to present. Currently, his main research directions are network security and artificial intelligence.

Nan Tang graduated from Changchun University of Science and Technology with a Master's degree in Electronic Science and Technology in 2015. She worked at the Information and Communication Branch of Inner Mongolia Electric Power (Group) Co., Ltd. from September 2015 to November 2023. From November 2023 until now, she has been working at the Digital Research Branch of Inner Mongolia Electric Power (Group) Co., Ltd. Her main research direction is information networks and network security.

Xi Liu graduated from Inner Mongolia University of Technology with a Bachelor's degree in Automation in 2018. She worked at the Information and Telecommunication Branch of Inner Mongolia Electric Power (Group) Co., Ltd. from August 2018 to November 2023. Since November 2023, she has been working at the Digital Research Branch of Inner Mongolia Electric Power (Group) Co., Ltd. Her main research areas are network security and information network construction.

Hao Dong received his Bachelor's degree from Beijing Institute of Technology, Beijing, China, in 2019. From 2019 to 2023, he worked in Inner Mongolia Power Information and Telecommunication Company. Up to now, he works in Inner Mongolia Power Digital Research Company. His current research interests focus on network security and artificial intelligence.

1 Introduction

With the increase of the number of intelligent devices, a single wireless communication technology can no longer meet the increasingly diversified needs, so a heterogeneous wireless network environment formed by overlapping and covering different wireless access technologies has been born. Existing wireless communication technologies can be roughly divided into wireless local area networks, wireless metropolitan area networks and wireless wide area networks according to coverage. With the development of access technology, the differences between different types of networks are getting bigger and

bigger, so the diverse needs of users can be met. To sum up, the development of wireless networks will continue to flourish towards various access technologies and no blind spots in coverage. There are various access technologies of wireless networks, which not only provide users with diversified choices, but also face the problem of how to meet the individual needs of users to the maximum extent. At present, people are no longer limited to using wireless networks for simple functions such as telephone chat or short message communication, but use emerging services such as video chat and entertainment software, and the requirements for network performance are becoming more and more stringent. Therefore, how to choose the appropriate network for users to access and make full use of heterogeneous wireless network resources is an urgent problem to be solved.

The basic idea of network selection algorithm based on single threshold decision is to select a single threshold as the parameter of network selection decision. This algorithm mainly exists in the early research field of network selection, and most of them choose received signal strength (RSS) as the threshold for network selection. This kind of algorithm is simple in principle, short in decision-making time and easy to implement. However, this kind of algorithm also has some shortcomings, such as serious ping-pong effect and one-sided switching decision result.

As a key technology in the next generation mobile communication, dense network expands the coverage by deploying dense APs, narrows the distance between users and APs, and greatly increases the system capacity. However, while the deployment of dense networks becomes more flexible, it also brings more dense and complicated network topologies, so it also faces a series of new problems. The main changes are concentrated in the following three aspects:

1 new networking architecture

2 higher base station density and more antennas

3 inter-cell interference.

In order to cope with these changes, dense networks need to redesign new network architectures, use advanced wireless transmission technology to greatly improve the utilisation efficiency of multi-bit resources such as frequency, time slot, space, antenna, base station, power, etc., and reasonably allocate these limited resources to eliminate inter-cell interference and obtain better network performance.

In order to improve terminal security and end user experience, this paper designs a network slice selection algorithm based on SDN and terminal security. At the same time, considering the possible negative unevenness between the two kinds of slices, an adaptive slice adjustment mechanism is proposed. Combined with data transmission rate and access blocking rate, the comprehensive benefit function is constructed, and the optimal slice resource allocation strategy is solved by ant colony optimisation algorithm, and then the optimal access slice of the terminal is designed.

2 Related work

Sun et al. (2021) proposed a vertical switching algorithm based on residence time and predicted RSS. This algorithm uses a back propagation (BP) neural network to predict the RSS of the network. Firstly, during the residence time, if the predicted target network

RSS is consistently greater than the set threshold, the network will be added to the candidate network set. Secondly, using a fuzzy logic system, input network parameters and adaptively match them with rules to obtain decision values, thereby selecting the optimal network for access. Mansouri and Leghris (2020) proposed a cross layer predictive RSS adaptive network selection algorithm, which predicts RSS through polynomial regression to reduce switching times and improve ping-pong effect. At the same time, relying on cross layer solutions, the transmission control protocol (TCP) sender can predict the available bandwidth and adaptively adjust the size of the transmitted data to increase network throughput. Tadić et al. (2020) summarise the past, present, and future of RSS based vertical switching algorithms. The initial vertical switching algorithm based on RSS treated RSS as a single decision attribute. The advantage of this type of algorithm is that it is simple and easy to implement, but at the same time, it has serious ping-pong effect, overly one-sided judgement conditions, and may not meet the service needs of users. To improve the ping-pong effect, subsequent algorithms introduce the concept of dwell time, which is based on the idea that the RSS of the target network remains above the threshold for a certain period of time before triggering a switch (Ho-Van and Do-Dac, 2020). However, introducing dwell time will result in a certain switching delay. With the emergence of high mobility terminals, the introduction of dwell time may result in switching delays that may cause the terminal to leave the coverage area of the target network when triggering a switch. In high mobility environments, combining residence time with RSS prediction can solve the problem of switching delay caused by the introduction of residence time and meet the network access needs of high mobility terminals. To improve the one sidedness of single threshold judgement, RSS can be used as the threshold for generating candidate network sets in future research, and other network parameters can be selected for network selection decisions (Park et al., 2021).

The basic idea of the algorithm based on multi-attribute decision making is to select multiple network parameters, determine the weights of each network parameter through subjective and objective weight determination algorithms such as analytic hierarchy process, fuzzy analytic hierarchy process, or entropy method, and then use simple weighting method, good and bad solution distance method, or grey correlation method to score each candidate network. The network with the highest score is selected for access (Shim et al., 2021). Khoshafa et al. (2020) use fuzzy analytic hierarchy process (FAHP) to calculate the weights of various network parameters, and then adopts grey relation analysis (GRA) algorithm to sort each network and select the optimal network for access. However, this algorithm only uses subjective weight analysis when calculating network parameter weights, resulting in poor algorithm stability. Liu et al. (2020) propose a network selection algorithm based on FAHP combined with SAW (simple additive weight). The algorithm selects five network parameters: RSS, available bandwidth, latency, jitter, and packet loss rate. FAHP is used to calculate the network parameter weights for different service types, and SAW is used to calculate the scores of each candidate network and select the optimal network for access. This algorithm fully considers the different network parameter requirements of different business types, but FAHP has the characteristic of strong subjectivity, and the calculated weights are greatly affected by subjective factors, which may cause algorithm instability. The current mainstream multi-attribute decision-making algorithms mostly combine subjective weight analysis and objective weight analysis for joint weight calculation, with the most representative being Verma et al. (2020). Gelenbe et al. (2020) combine analytic

hierarchy process and standard deviation method to calculate a joint weight for each network parameter. Then use the improved technique for order preference by similarity to an ideal solution (TOPSIS) to rank the candidate networks and select the optimal network for access. This algorithm introduces an improved TOPSIS algorithm, which has better performance in the decision-making process compared to the traditional TOPSIS algorithm. Simultaneously combining subjective and objective weights avoids the adverse effects of weight fluctuations on the ranking of candidate networks. Yan et al. (2020) introduce the method of eliminating and expressing reality to sort candidate networks and select the optimal network for access. Wang et al. (2024) introduce historical information to prioritise users' access to networks they have previously accessed. When there are no networks in the historical information database, multi-attribute decision-making methods are used to select networks for users.

The general process of network selection algorithm based on fuzzy logic is fuzzification, fuzzy inference, and deblurring. Fuzziness refers to the process of fuzzifying the selection parameters through membership functions, which avoids calculating the weights of each parameter and enhances the stability of the algorithm; fuzzy reasoning is the process of inferring the fuzzy parameters based on the generated fuzzy rule library to obtain the inference results; defuzzification is the process of refining the fuzzy results obtained from fuzzy inference to determine the optimal network (Srinivasu et al., 2021). Zhang and Peng (2021) proposed a weighted fuzzy self optimisation network access algorithm. The input parameters for the fuzzy logic of this algorithm are: signal-to-noise ratio, load of serving and target base stations, and user speed. The so-called self optimisation refers to automatically adjusting the switching margin and triggering time. The design of the two mechanisms of switching margin and triggering time is mainly aimed at reducing unnecessary switching and improving the ping-pong effect. Iwendi et al. (2021) proposed a network selection algorithm based on speed prediction and fuzzy logic in private heterogeneous wireless networks. The algorithm first predicts the speed of the vehicle terminal and selects a suitable candidate network set based on the predicted speed. Next, fuzzify the RSS and bandwidth parameters. The difference between this algorithm and other traditional fuzzy logic based algorithms is that after fuzzifying the parameters, it does not perform deblurring, but adopts a standardised membership degree to obtain the scores of each network, which can effectively reduce the switching delay. Due to the fact that network selection algorithms based on fuzzy logic experience a significant increase in decision time with an increase in input parameters, some research has divided fuzzy logic into two levels, reducing the input size of each level and lowering decision time. Luo et al. (2020) proposed a network selection algorithm based on second-order fuzzy logic. This algorithm takes delay, jitter, and packet loss rate as inputs to the first level fuzzy logic and outputs the fuzzy value of quality of service (QoS); then, the fuzzy values of QoS, RSS, bandwidth, and network coverage are used as inputs for the second level fuzzy logic, and the fuzzy logic outputs decision values for network selection. The use of two-level fuzzy logic can effectively reduce the size of the fuzzy rule base, thus effectively reducing time complexity, and the decision time is also lower than algorithms using first-order fuzzy logic. Shandilya et al. (2022) first use fuzzy logic algorithm to evaluate the necessity of decision making. When the user determines that a switch is needed, the TOPSIS algorithm is triggered to select the network based on the score of each candidate network.

The network selection algorithm based on fuzzy logic improves the problem of difficult weight determination in multi-attribute decision-making algorithms. If combined with a dynamic fuzzy rule library, it can also adapt to the dynamic changes of the network. But as the input parameter size increases, the time complexity of the algorithm will significantly increase, and the difficulty of designing the fuzzy rule library will also significantly increase (Davila-Frias and Yadav, 2022).

In summary, although the single parameter based network selection algorithm has low time complexity and is easy to implement, it is not suitable for solving the network selection problem in Ud HetNet networks because the considered selection parameters are too single to meet the service needs of users in multiple business scenarios. The introduction of artificial intelligence algorithms has effectively improved users' QoE and optimised network performance, but it also brings prominent problems such as high switching latency, which has limited impact on further enhancing user experience. In addition, the above algorithms also ignore a very critical issue, that is, in the process of network selection, none of the above algorithms consider the security of the terminal itself, which may have an impact on the performance of the entire network system and switching algorithms. Especially in the Ud HetNet network environment with a large number of networks and terminals, the impact of malicious terminals will be even more severe. In order to improve terminal security and end user experience, this paper designs a network slice selection algorithm based on SDN and terminal security. At the same time, considering the possible negative unevenness between the two kinds of slices, an adaptive slice adjustment mechanism is proposed. Combined with data transmission rate and access blocking rate, the comprehensive benefit function is constructed, and the optimal slice resource allocation strategy is solved by ant colony optimisation algorithm, and then the optimal access slice of the terminal is designed.

3 Network model

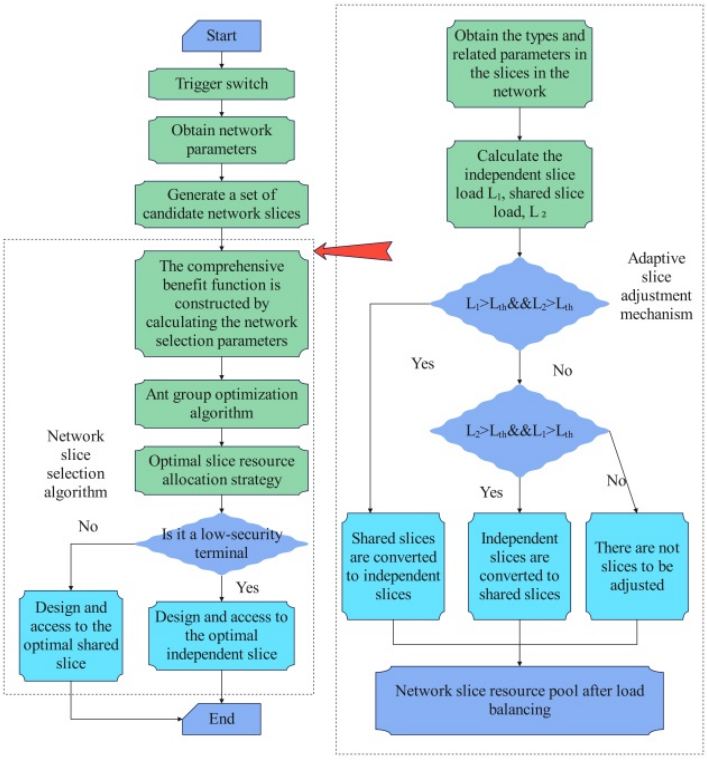
In the handover algorithm, the impact of terminal security on network service quality and user experience quality is rarely considered. Some network selection algorithms evaluate the security of terminals before accessing, and take it as a key network selection index, but there may still be some low-security terminals attacking the network after successfully accessing the network. Moreover, whether before or after accessing the network, the attack behaviour of low-security terminals will consume a lot of system resources, resulting in the decline of user experience quality. At this time, the above switching algorithm has been difficult to effectively solve the problems in this environment.

From the perspective of improving network service quality and user experience, this paper proposes a network-slice selection algorithm based on SDN and terminal security (SDNTS-NSA), which is based on SDN and terminal security, so as to alleviate the impact of low-security terminals on the performance of handover algorithm and improve the experience quality of users in the process of network selection.

3.1 Algorithm flow

The execution process of the algorithm is shown in Figure 1.

Figure 1 Algorithm flow (see online version for colours)



1 Switching trigger module: when the bandwidth available to the terminal from the service network is lower than its minimum bandwidth requirement, a switch is triggered.

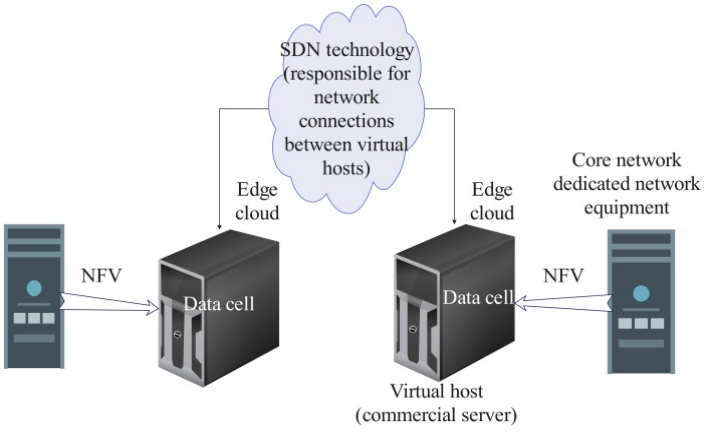
2 Adaptive slice adjustment mechanism: after triggering the switch, the load levels of independent slices and shared slices are calculated separately based on the types and related parameters of each slice obtained in the network; then compare it with the load threshold L^{th} set by the system. If the independent slice load exceeds L^{th} and the shared slice load is lower than L^{th}, the shared slice will be converted to an independent slice; if the shared slice load exceeds L^{th} and the independent slice load is lower than L^{th}, the independent slice will be converted to a shared slice, otherwise there is no need to adjust the slice type; after completing real-time adjustment of slice load, a network slice resource pool that has achieved load balancing can be obtained as a candidate network slice set in the network selection process (Li et al., 2020).

3 Switching decision module: firstly, calculate the network selection parameters, including access blocking rate and data transmission rate; then, a comprehensive benefit function is constructed and the optimal slice resource allocation strategy is obtained through ant colony optimisation algorithm; finally, based on the optimal slice resource allocation strategy and the security type of the terminal, generate the optimal network slice that meets the service requirements of the terminal and

conforms to its security type. To reduce interference from low security terminals to other secure terminals, the system will control low security terminals to only access the optimal independent slice, so that secure terminals will access the optimal shared slice.

Network slicing mainly depends on two key technologies: software defined network (SDN) and network function virtualisation (NFV). Firstly, NFV technology is used to transfer the software and hardware functions of dedicated network devices in the network to virtual hosts, such as mobility management entities in the core network, serving gateways and digital units in radio access network (RAN). As shown in Figure 2, the virtual host is mainly a commercial server based on industry standards, so it can replace the dedicated network equipment in the traditional network.

Figure 2 Implementation process of network slicing technology (see online version for colours)



Network slicing adopts end-to-end technology, and each slice mainly includes three types of sub-slices: radio access network sub-slice, bearer network sub-slice and core network sub-slice. The life cycle of network slices is managed through the network slice management system, and its core architecture is shown in Figure 3.

1 Wireless access network slicing

Base stations on the wireless access network side usually need to have the characteristics of flexible deployment of distributed and centralised units to meet the various needs of users for network slicing services in different business scenarios. Among them, the main task of distributed units is to process real-time business, while centralised units are responsible for centralising and carrying some non-real time business. The main responsibilities of wireless access network slicing are: slicing resource allocation and isolation, slicing perception and selection, and service quality assurance.

2 Carrying mesh slicing

The carrier network slicing utilises a virtual network function (VNF) manager with virtualisation technology to virtualise the topology resources (such as links, nodes, and ports) of the wireless network, resulting in several virtual subnets. Among them,

each virtual subnet has four core functions: connection, computing, storage, and management, all of which are separated from control and forwarding through SDN technology. Therefore, various types of services can be independently supported in the virtual subnet, ensuring that different services do not interfere with each other.

3 Core network slicing

The core network is responsible for the core business of the operator, and in order to ensure its adaptability to different business scenarios, it is required that the core network has the ability to flexibly deploy network functions. For example, in certain specific business scenarios, it is necessary to add or reduce some functions in order to improve user experience and enhance network service efficiency. In addition, the core network slicing also introduces service-based architecture (SBA) to reduce the coupling of network functions and provide technical support for slicing.

4 Network slicing management system

The management function of network slicing requires collaboration with wireless access networks, bearer networks, and core networks to achieve the management and orchestration of network slicing. Therefore, when designing a slice management system, an SDN/NFV based management platform can be used as technical support for slice instantiation.

According to the SDN/NFV technology, this section combines the Ud-HetNet network on the basis of the existing software-defined network, and further abstracts the software-defined ultra-dense heterogeneous wireless network (SD-Ud-HetNet), as shown in Figure 4.

Figure 3 Network slicing architecture (see online version for colours)

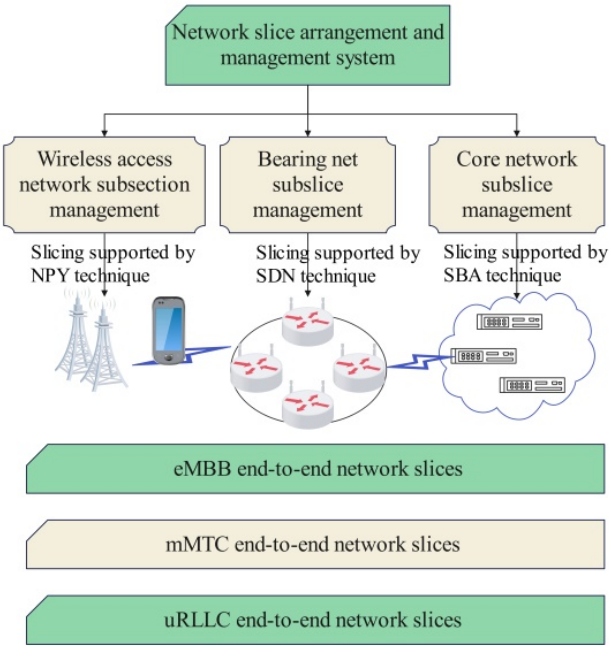
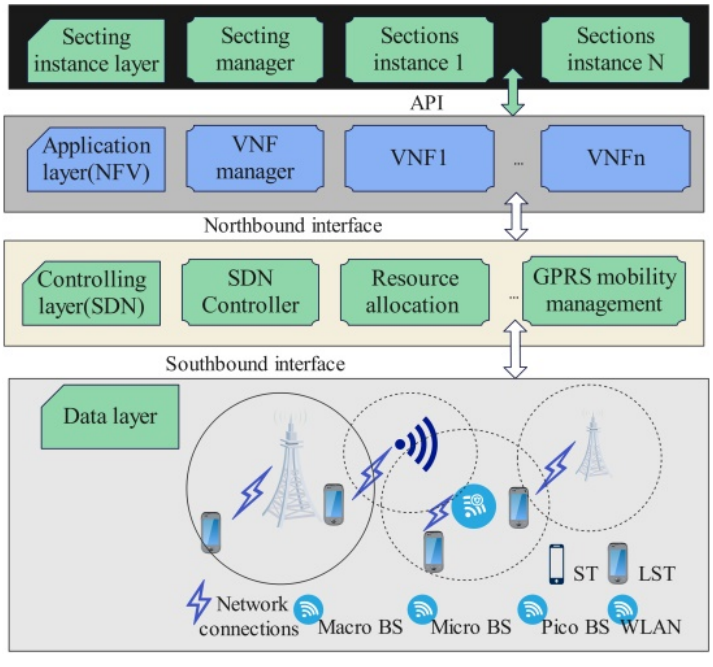


Figure 4 Ultra-dense heterogeneous wireless network (see online version for colours)



The proposed network scenario is mainly divided into four layers: data layer, control layer, application layer and slice instance layer.

Data layer: it mainly includes ultra-dense heterogeneous wireless networks composed of 5G macro-cells, microcells, picocells and WLANs, as well as secure terminals (ST) and low-security terminals (LST). Control layer: it interacts with the data layer through the southbound interface, and is mainly responsible for link discovery, topology management and command downloading. Application layer: in order to enable all kinds of services to call the network resources of the data layer, the application layer adopts a northbound interface to realise data transmission with the control layer. Slice instance layer: it interacts with the application layer through the application programming interface (API), and is mainly responsible for the design and partition of network slices, including slice resource allocation and slice type determination.

3.2 Parameter calculation

We assume that the number of terminals in the network scenario is m and the number of networks is n, denoted by the sets M and N, respectively. Because there are different service requirements in SD-Ud-HetNet network, all network resources are divided into W different types of slices, including U independent slices and V shared slices. According to the proportion of the sum of resource usage of each type of slice in the total resources of this type of slice at time t, the average slice load rate is defined, which is used as an index to measure the load of each type of slice (Marabissi et al., 2021).

$$L_{\ell}(t)=\frac{\sum_{j=1}^{\ell}\sum_{i=1}^{m}b_{i,j}^{k}(t)}{\sum_{j=1}^{\ell}B_{j}^{k}},\qquad 0\le L_{\ell}\le 1 \tag{1}$$

Among them, $L_{\ell}(t)$ represents the average load rate of slices with slice type l at time t, L_u is the average load rate of independent slices, and L_v is the average load rate of shared slices. $b_{i,j}^{k}(t)$ represents the bandwidth resource obtained when the terminal i accesses the slice j of the network k at time t, and B_j^k is the maximum bandwidth resource that the slice j can allocate in the network k.

In order to avoid the situation that multiple terminals choose the same slice at the same time, this section stipulates that each end user can only enjoy the network services provided by a certain slice of a certain network at the same time. If we assume that the number of candidate networks is K, where the slice type configured by each network is J, there are the following three constraints (Miao and Wang, 2019):

$$K\le n \tag{2}$$

$$J\le W \tag{3}$$

$$U+V\le W \tag{4}$$

Equation (2) indicates that the number of candidate networks shall not exceed the total number of networks in the network scene, and equation (3) indicates that the slice types configured by each network shall not exceed the total network slice types, and equation (4) indicates that the sum of the number of independent slices and shared slices in the network is at most the total number of slice types. In addition, since all bandwidth resources in the network are allocated to each slice, in order to ensure the effectiveness of resource allocation, when a network slice provides services to different terminals, its bandwidth resources and transmission power should meet the following constraints:

$$\sum_{j=1}^{J}B_{j}^{k}\le B_{k},\qquad \forall j\in J,\forall k\in K \tag{5}$$

$$\sum_{j=1}^{J}P_{j}^{k}\le P_{k},\qquad \forall j\in J,\forall k\in K \tag{6}$$

Equation (5) indicates that the sum of the bandwidths of all slices in each network k does not exceed its maximum available bandwidth B_k, and equation (6) indicates that the sum of slice transmission powers in any network does not exceed the maximum transmission power P_k of the network.

When the terminal measures the channel quality of the target network, it usually uses a network indicator: received signal strength. Therefore, the RSS of terminal i in slice j of network k is defined as (Zhu et al., 2021):

$$RSS_{i,j}^{k}=P_{j}^{k}-\hbar_{j}^{k}\lg\left(d_{i,j}^{k}\right)+\varsigma_{a} \tag{7}$$

Among them, P_j^k is the signal transmission power of slice j in network k, $\hbar_j^k \lg(d_{i,j}^k)$ is the path loss, $\hbar_j^k$ is the path loss factor, $d_{i,j}^k$ represents the distance from terminal i to slice j in network k, and a represents a Gaussian random variable with a mean value of 0 and a variance of a.

According to Shannon's formula and combined with equation (7), the data transmission rate of terminal i in the j^{th} slice of network k can be defined as $C_{i,j}^k$:

$$C_{i,j}^k = A_{i,j}^k \cdot B_{i,j}^k \cdot \log_2\left(1 + \frac{RSS_{i,j}^k}{\xi_j^k \cdot B_{i,j}^k}\right) \tag{8}$$

Among them, $A_{i,j}^k$ represents the access relationship between the terminal and the slice, if $A_{i,j}^k = 1$, it indicates that the terminal i has accessed the j^{th} slice of the network k, and if it is 0, it indicates that the slice has not been accessed. ξ_j^k represents the power spectral density of slice j in network k, and $B_{i,j}^k$ is the bandwidth resource obtained by terminal i in the j^{th} slice of network k.

The access blocking rate of the terminal is defined as the probability that when the terminal accesses the network slice at time t, the handover request issued by the terminal at this time enters the blocking state because the number of accessed terminals in the network where the current slice is located exceeds the maximum capacity limit of the network. We assume that the behaviour of each terminal selecting slice is independent of each other, the number of newly arrived terminals at time t is M ($M \le m$), among which c terminals issue handover requests, and the access probability $X(c, t)$ of the terminals obeys binomial distribution

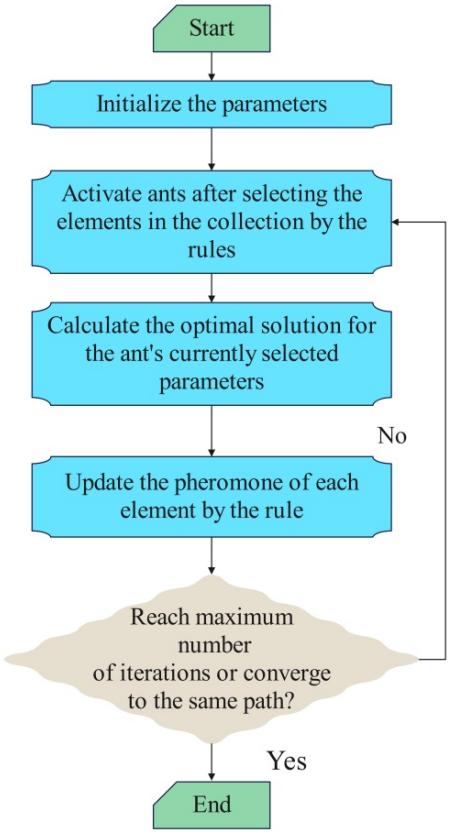
$$X(c,t) = C_{M'(t)}^c p_{i,j(t)}^k \cdot \left(1 - p_{i,j(t)}^k\right)^{M'(t)-c} \tag{9}$$

In the formula, $p_{i,j(t)}^k$ represents the probability that the terminal i accesses the slice j at time t, and $1 - p_{i,j(t)}^k$ is the probability that the terminal does not access the slice j. If we assume that the maximum number of terminals that the network k can accommodate is $M_{\max}^k$, and the number of terminals that network k has accessed at this time t is $M''(t)$, then the remaining number of terminals that network k can accommodate is $M_r(t) = M_{\max}^k - M''(t)$, so the access blocking rate is:

$$Q_{i,j}^k(t) = \begin{cases} 0, & M'(t) \le M_r(t) \\ \sum_{c=M_r(t)}^{M'(t)} X(c,t), & M'(t) > M_r(t) \end{cases} \tag{10}$$

When the number of newly arrived terminals $M''(t)$ at time t exceeds the number of remaining terminal capacity $M_r(t)$ of the network k, terminal access blocking will be caused, and the blocking rate is expressed as $Q_{i,j}^k(t)$. If the remaining capacity is not exceeded, the access blocking rate is 0.

Figure 5 Schematic diagram of ant colony optimisation algorithm flow (see online version for colours)



3.3 Improvement plan

The situation that a large number of users choose network slices at the same time is comprehensively considered, that is, the blocking probability when the terminal accesses the slice. Then, combined with the data transmission rate of the terminal in the slice, the network performance is maximised by optimising the slice resource allocation. Based on this, this section constructs the comprehensive benefit function of equation (12) (Singh et al., 2021)[

$$T_{i,j}^{k} = Maximise \sum_{i=1}^{M'} \sum_{j=1}^{J} \sum_{k=1}^{K} \left(A_{i,j}^{k} \cdot C_{i,j}^{k} - A_{i,j}^{k} \cdot Q_{i,j}^{k} \right) \tag{11}$$

$$\sum_{j=1}^{J} \sum_{k=1}^{K} A_{i,j}^{k} = 1 \tag{12}$$

$$\sum_{j=1}^{J} \sum_{k=1}^{K} A_{i,j}^{k} \le M_{\max}^{k} \tag{13}$$

$$D_{\min}^{i} \le D_{i,j}^{k}, \qquad \forall i \in M', \forall j \in J, \forall k \in K \tag{14}$$

Equation (12) indicates that each terminal can only access one slice in the network k at most, and equation (13) indicates that the number of access terminals of all slices in the network k does not exceed the maximum number of terminals $M_{\max}^{k}$ that the network k can accommodate, and equation (14) indicates that the data transmission rate of terminal i accessing slice j is not lower than its minimum rate requirement $D_{\min}^{i}$.

Aiming at the objective function under multiple constraints, this paper uses ant colony optimisation algorithm to solve it. Ant colony algorithm is an optimisation algorithm to simulate the foraging process of ants. During the movement of each ant, it will release a pheromone on its path, providing a learnable positive feedback for subsequent ants to find the optimal solution. Finally, the optimal solution is found by adjusting the pheromone and iterating the algorithm. The core flow of the algorithm is shown in Figure 5.

The ant colony algorithm mainly includes the following steps:

1 Initialisation parameters: the start time is $t = 0$, the number of iterations is $N = 0$, the maximum number of iterations is $N'_{\max}$, and the number of ants is N''. If the number of parameters to be optimised is 2 (this is, network selection parameters $C_{i,j}^{k}$ and $Q_{i,j}^{k}$), it is recorded as p_1 and p_2, and the corresponding values are n'' non-zero random numbers in their value range, which are expressed as the set G_{pi} ($1 \le i \le 2$). We set that the initial pheromone of any element j' in G_{pi} is $\tau_{j'}(G_{pi})(0) = 0$, and the amount of pheromone change at this time is $\Delta\tau_{j'}(G_{pi}) = 0$ ($1 \le j' \le n''$).

2 Activating all ants: each ant n' ($n' = 1, 2, \ldots, N''$) will start from the set G_{pi} and select the j'^{th} element from each set in turn until all ants reach the food source. Among them, the probability that ants choose any element j' as the forward path is defined as follows:

$$P\left(\tau_{j'}^{n'}, \left(G_{pi}\right)\right) = \frac{\tau\left(G_{pi}\right)}{\sum_{j'=1}^{n''} \tau_{j'}\left(G_{pi}\right)} \tag{15}$$

3 Iterative optimisation: if we assume that t time units have been experienced in the above ant foraging process, the foraging time and the number of iterations are updated to: $t = t + t'$ and $N' = N' + 1$, respectively. When the whole ant colony finishes selecting an element in G_{pi}, the value of the parameter selected by each ant at present is brought into the comprehensive benefit function of equation (11) for calculation, and the current optimal solution is recorded, and then the pheromone of each element in all sets G_{pi} is updated in turn. The update rule is:

$$\tau_{j'}^{n'}\left(G_{pi}\right)\left(t+t'\right) = \left(1-\rho_{j'}\right)\tau_{j'}\left(G_{pi}\right)(t) + \Delta\tau_{j'}\left(G_{pi}\right) \tag{16}$$

$$\Delta\tau_{j'}\left(G_{pi}\right) = \sum_{n'=1}^{n''} \Delta\tau_{j'}^{n'}\left(G_{pi}\right) \tag{17}$$

$$\tau_{j'}^{n'}\left(G_{pi}\right)=\begin{cases}Q/e^{n'}, & \text{Ant } n' \text{ selected elements from the set } G_{pi}\\ 0, & \text{Other situations}\end{cases} \tag{18}$$

In equation (16), $\rho_{j'}$ ($0 \le \rho_{j'} \le 1$) represents the volatilisation rate of pheromone j'. In equation (18), $\tau_{j'}^{n'}(G_{pi})$ represents the pheromone released by the n'^{th} ant on the j'^{th} element of G_{pi} in this cycle. If ant n' selects element j', then $\tau_{j'}^{n'}(G_{pi})=\frac{Q}{e^{n'}}$. If it does not select the element, $\tau_{j'}^{n'}\left(G_{pi}\right)=0$. Among them, Q is a constant that regulates the update speed of pheromone, and $e^{n'}$ represents the comprehensive benefit value calculated when the element selected by the n'^{th} ant is used as the input variable of equation (11). Finally, the algorithm repeats steps 2 and 3 until all ants converge to one path or reach the maximum number of iterations $N'_{\max}$ to output the optimal solution, that is, the optimal slice resource allocation strategy $T_i'=\{T_{i,1}^k,T_{i,2}^k,...,T_{i,J}^k\}, i\in M, k\in N$ of terminal i. At this point, the algorithm ends.

4 Model test analysis

4.1 Simulation environment

According to the simulation model established in Figure 4 of this paper, the comparative experiment and analysis of related indexes are carried out on MATLAB simulation platform.

Considering that in the process of network slice selection, the load degree of the target network slice will affect the service experience of the end user. There are also 1,000 mobile terminals placed in the scene, in which the ratio of security terminals to low-security terminals is 8:2. At the same time, if the terminals are blocked for a long time when switching to the target slice, resulting in too high handover delay, it will directly affect the service satisfaction of users. In addition, another key factor causing excessive handover delay is often related to the time complexity of handover algorithm. Therefore, this section takes the network slice load rate, access blocking rate, user satisfaction, system throughput and the time overhead of the algorithm as the performance indicators of the network slice selection algorithm. The simulation parameters are shown in Table 1.

Table 1 Simulation parameters

Wireless network technology	*Transmit power (dBm)*	*Path loss factor (dBm)*	*Coverage radius (m)*	*Total bandwidth (MHz)*	*Maximum capacity (pcs)*
Macrocell	29	41	Full coverage	23	162
Microcellular	17	42	227	10	36
Picocells	23	43	162	10	28
WLAN	16	39	81	8	16

4.2 Results

After executing SDNTS-NSA algorithm, the number of access terminals in the two kinds of slices and the corresponding security types of access terminals are counted.

Figure 6 reflects the relationship between the terminal access situation and the number of terminals in the slice. It can be seen from the figure that as the number of terminals increases, the number of access terminals in both types of slices shows an upward trend, and the number of terminals in shared slices has always far exceeded the number of terminals in independent slices. Through simple calculation, it can be found that in the process of increasing the number of terminals from 0 to 1000, 800 terminals are connected to shared slice and 200 terminals are connected to independent slice.

Figure 6 Number of access terminals in slice (see online version for colours)

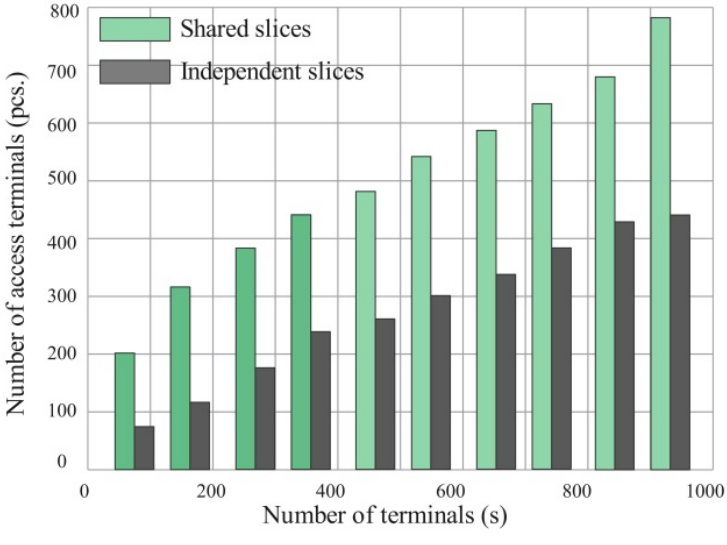


Figure 7 Security types of access terminals in slices (see online version for colours)

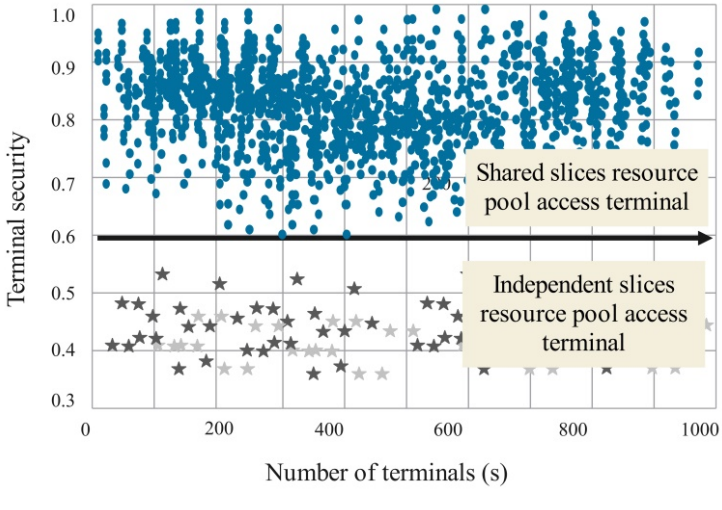
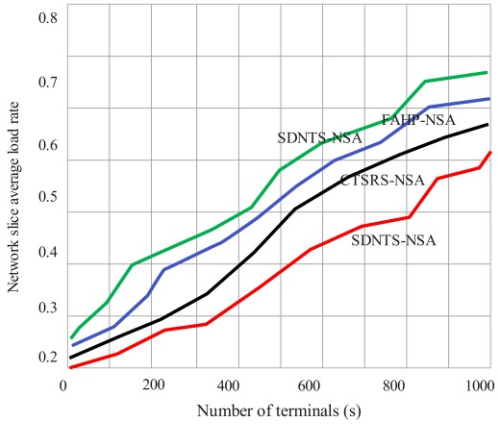
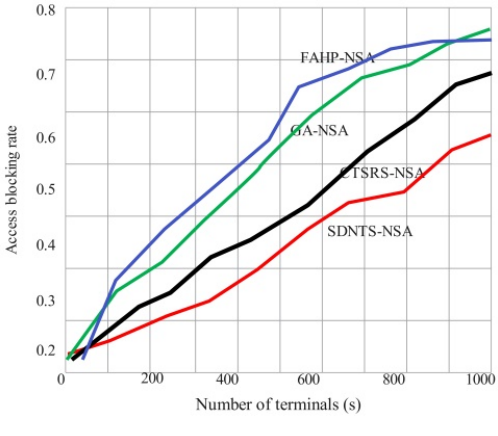


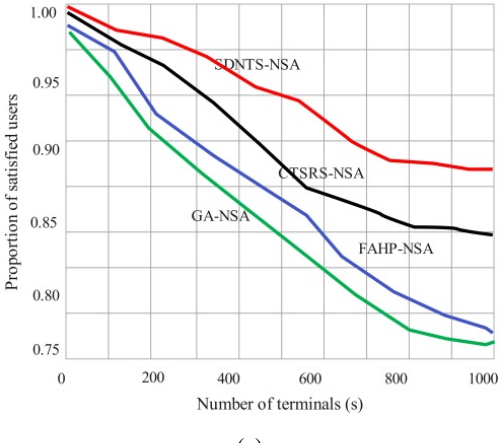
Figure 8 Comparison results of algorithm parameters, (a) average load rate of network slice (b) access blocking rate (c) proportion of satisfied users (see online version for colours)



(a)



(b)



(c)

Figure 7 shows the relationship between the security type of access terminals in the two types of slice resource pools (the security degree higher than 0.6 indicates a secure terminal, otherwise it is a low-security terminal) and the number of terminals. It can be clearly seen from the figure that the security degree of the access terminals in the shared slice resource pool is above the blue dotted line (the security degree is 0.6), so they are all secure terminals. The access terminals in the independent slice resource pool are all under the blue dotted line, which is a low-security terminal.

Through comparison of several algorithms, the parameters of network slice average load rate, access blocking rate, and user satisfaction ratio are counted, and the results are shown in Figure 8.

4.3 Analysis and discussion

Based on the above two sets of experiments in Figures 6 and 7, it can be concluded that in the simulation scenario with 800 secure terminals and 200 low-security terminals, the algorithm proposed in this paper ensures that all secure terminals are connected to shared slices, while all low-security terminals are connected to independent slices, thus taking advantage of the isolation of independent slice resources to reduce the impact of low-security terminals on secure terminals in the network environment, and improving the service security and experience quality of terminals.

Figure 8(a) reflects the relationship between the average load rate of network slices and the number of terminals. With the increase of the number of terminals, the access terminals occupy a large amount of network slice resources, so the average load rate of network slices of the four algorithms shows an upward trend. However, it is not difficult to find that the average load rate of network slices in SDNTS-NSA algorithm is obviously lower than that of the other three algorithms, and the rising speed is relatively slow. This is because the SDNTS-NSA algorithm adopts an adaptive slice adjustment mechanism when selecting networks, which can dynamically adjust according to the load of slices in each network, and reduce the probability of a large number of terminals accessing the same type of slice at the same time, thereby reducing the average load rate of network slices.

As shown in Figure 8(b), the relationship between the access blocking rate of the four algorithms and the number of terminals is presented. At the beginning, when the number of terminals is small, the network slicing resources are sufficient, so all four algorithms keep a low access blocking rate. However, with the increasing number of terminals, the access blocking rate of the four algorithms began to rise rapidly.

It can be seen from Figure 8(b) that the FAHP-NSA algorithm has the largest blocking rate, while the SDNTS-NSA algorithm proposed in this paper has always been lower than the other three algorithms. Especially, after the number of terminals reaches 500, the access blocking rate of SDNTS-NSA algorithm has more obvious advantages. Because the SDNTS-NSA algorithm not only considers the access blocking rate when selecting the network, but also reduces the interference caused by low-security terminals to network resources and slows down the malicious consumption of network resources by dividing independent slices, the SDNTS-NSA algorithm can maintain a lower access blocking rate.

In the process of selecting network slices, access blocking and handover failure will greatly reduce the user's service experience. Therefore, this paper defines an indicator that the sum of the number of blocks and the number of handover failures when the

terminal accesses the slice is higher than the number of handover triggers per unit time. If this indicator is less than 1%, it is defined as a satisfied user.

As shown in Figure 8(c), when the number of terminals is less than 200, the proportion of satisfied users of the SDNTS-NSA algorithm and the CTSRS-NSA algorithm is equivalent and very close to 1. The reason is that both of them focus on network selection indexes related to terminal service quality in the process of handover decision-making.

As more terminals join the network, the proportion of satisfied users in each algorithm begins to decrease. The reason is that a large number of terminals will consume more network slicing resources, which drastically reduces the resources that slices can provide services for terminals, increases the probability of access blocking and handover failure, and then reduces the service satisfaction of users. The downward trend of SDNTS-NSA algorithm is significantly lower than that of the other three algorithms. The reason is that the SDNTS-NSA algorithm comprehensively considers the user's network selection requirements and the resource load of each network slice, ensuring that the algorithm can allocate resources reasonably, which plays a key role in alleviating access congestion and handover failure. However, the CTSRS-NSA algorithm only considers the security of the terminal before accessing the network, and there is still the behaviour that the terminal continues to attack the network after successful access. When a large number of terminals select networks, the performance of CTSRS-NSA algorithm is weaker than that of SDNTS-NSA algorithm in blocking and handover failure. Therefore, the proportion of satisfied users of the algorithm proposed in this paper decreases more slowly and can maintain a high level.

Network research has been vigorously carried out, and in the face of increasingly diverse application scenarios, it is not only necessary to explore new technologies, but also to take into account all technologies since the 4th. Based on this, this paper proposes a multi-layer ultra dense heterogeneous network model to address the issues of high throughput and explosive traffic demand in communication networks, targeting the ubiquitous hotspots in the future. This model is a preliminary exploration of 5G network deployment based on existing 5G technology. A detailed analysis was conducted on the performance characteristics of D2D networks and cellular networks that constitute ultra dense heterogeneous networks, and a careful study was conducted on the physical layer security of the network. An effective communication security solution was proposed for this model. The model in this article considers the scalability of subsequent application processes, and its practicality can be further verified through practical case studies.

5 Conclusions

The previous network selection algorithms will not be able to solve the above problems well because of the great changes in the network environment. In addition, the security threats faced by the network will have an inevitable impact on the performance of handover algorithms and network resources. Therefore, how to design network selection algorithm, improve the level of network access security, and improve the user's experience quality in the process of network selection has become a hot issue in current research.

In this paper, before and after the terminal accesses the network, considering the impact of terminal security on the performance of handover algorithm and the quality of user experience, two network selection algorithms are designed respectively, which are used to improve the level of network access security, alleviate network congestion and increase user service satisfaction. When studying the problem of network selection, this paper mainly aims at the problem that terminal security brings to the handover performance degradation of previous network selection algorithms. However, due to limited research time and personal energy, and the problems considered in the research process are not comprehensive enough, in the follow-up research work, network security can be regarded as a key performance index of network selection in the handover decision process, so as to further improve the quality of user experience and network security level.

Acknowledgements

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

References

Davila-Frias, A. and Yadav, O.P. (2022) 'All-terminal network reliability estimation using convolutional neural networks', *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, Vol. 236, No. 4, pp.584–597.

Gelenbe, E., Domanska, J., Fröhlich, P., Nowak, M.P. and Nowak, S. (2020) 'Self-aware networks that optimize security, QoS, and energy', *Proceedings of the IEEE*, Vol. 108, No. 7, pp.1150–1167.

Ho-Van, K. and Do-Dac, T. (2020) 'Security enhancement for energy harvesting cognitive networks with relay selection', *Wireless Communications and Mobile Computing*, Vol. 2020, No. 1, pp.8867148–8867160.

Iwendi, C., Rehman, S.U., Javed, A.R., Khan, S. and Srivastava, G. (2021) 'Sustainable security for the internet of things using artificial intelligence architectures', *ACM Transactions on Internet Technology (TOIT)*, Vol. 21, No. 3, pp.1–22.

Khoshafa, M.H., Ngatched, T.M., Ahmed, M.H. and Ibrahim, A. (2020) 'Improving physical layer security of cellular networks using full-duplex jamming relay-aided D2D communications', *IEEE Access*, Vol. 8, No. 1, pp.53575–53586.

Li, Q., Hou, J., Meng, S. and Long, H. (2020) 'GLIDE: a game theory and data-driven mimicking linkage intrusion detection for edge computing networks', *Complexity*, Vol. 2020, No. 1, pp.7136160–7136170.

Liu, F., Huo, W., Han, Y., Yang, S. and Li, X. (2020) 'Study on network security based on PCA and BP neural network under green communication', *IEEE Access*, Vol. 8, No. 2, pp.53733–53749.

Luo, X., Liu, Y., Chen, H.H. and Guo, Q. (2020) 'Physical layer security in intelligently connected vehicle networks', *IEEE Network*, Vol. 34, No. 5, pp.232–239.

Mansouri, M. and Leghris, C. (2020) 'A use of fuzzy TOPSIS to improve the network selection in wireless multiaccess environments', *Journal of Computer Networks and Communications*, Vol. 2020, No. 1, p.3408326.

Marabissi, D., Mucchi, L. and Morosi, S. (2021) 'User-cell association for security and energy efficiency in ultra-dense heterogeneous networks', *Sensors*, Vol. 21, No. 2, p.508.

Miao, Z. and Wang, Y. (2019) 'Physical-layer-security-oriented frequency allocation in ultra-dense-networks based on location information', *IEEE Access*, Vol. 7, p.90190–90205.

Park, S., Kim, D., Park, Y., Cho, H., Kim, D. and Kwon, S. (2021) '5G security threat assessment in real networks', *Sensors*, Vol. 21, No. 16, pp.5524–5535.

Shandilya, S.K., Upadhyay, S., Kumar, A. and Nagar, A.K. (2022) 'AI-assisted computer network operations testbed for nature-inspired cyber security based adaptive defense simulation and analysis', *Future Generation Computer Systems*, Vol. 127, No. 1, pp.297–308.

Shim, K., Do, T.N., Nguyen, T.V., da Costa, D.B. and An, B. (2021) 'Enhancing PHY-security of FD-enabled NOMA systems using jamming and user selection: performance analysis and DNN evaluation', *IEEE Internet of Things Journal*, Vol. 8, No. 24, pp.17476–17494.

Singh, D., Bhanipati, J., Biswal, A.K., Samanta, D., Joshi, S., Shukla, P.K. and Nuagah, S.J. (2021) 'Approach for collision minimization and enhancement of power allocation in WSNs', *Journal of Sensors*, Vol. 2021, No. 1, p.7059881.

Srinivasu, P.N., Bhoi, A.K., Nayak, S.R., Bhutta, M.R. and Woźniak, M. (2021) 'Blockchain technology for secured healthcare data communication among the non-terminal nodes in IoT architecture in 5G network', *Electronics*, Vol. 10, No. 12, pp.1437–1448.

Sun, N., Li, T., Song, G. and Xia, H. (2021) 'Network security technology of intelligent information terminal based on mobile internet of things', *Mobile Information Systems*, Vol. 2021, No. 1, pp.6676946–6676956.

Tadić, S., Krstić, M., Roso, V. and Brnjac, N. (2020) 'Dry port terminal location selection by applying the hybrid grey MCDM model', *Sustainability*, Vol. 12, No. 17, pp.6983–6992.

Verma, S., Kawamoto, Y. and Kato, N. (2020) 'A network-aware Internet-wide scan for security maximization of IPV6-enabled WLAN IoT devices', *IEEE Internet of Things Journal*, Vol. 8, No. 10, pp.8411–8422.

Wang, F., Yang, N., Shakeel, P.M. and Saravanan, V. (2024) 'Machine learning for mobile network payment security evaluation system', *Transactions on Emerging Telecommunications Technologies*, Vol. 35, No. 4, pp.e4226–e4235.

Yan, P., Zou, Y., Ding, X. and Zhu, J. (2020) 'Energy-aware relay selection improves security-reliability tradeoff in energy harvesting cooperative cognitive radio systems', *IEEE Transactions on Vehicular Technology*, Vol. 69, No. 5, pp.5115–5128.

Zhang, W. and Peng, C. (2021) 'Indefinite mean-field stochastic cooperative linear-quadratic dynamic difference game with its application to the network security model', *IEEE Transactions on Cybernetics*, Vol. 52, No. 11, pp.11805–11818.

Zhu, A., Ma, M., Guo, S., Yu, S. and Yi, L. (2021) 'Adaptive multi-access algorithm for multi-service edge users in 5G ultra-dense heterogeneous networks', *IEEE Transactions on Vehicular Technology*, Vol. 70, No. 3, pp.2807–2821.