Optimization of Virus Propagation Model in Multi Hop Cellular Hybrid Network Based on Network Attack

Fang Wu, Lanmei Qian, Huanxiao Xu, Xiaodan Cai, Hongyun Chen and Chao Zhou
School of Computer and Information Engineering, Nantong Institute of Technology, Nantong, Jiangsu, China

Keywords: Network Attack, Cellular Network, Virus Transmission.

Abstract: Aiming at the problems of poor management effect and low security of the current multi hop cellular hybrid network virus identification, this paper proposes a multi hop cellular hybrid network virus propagation model optimization method based on network attack, mines and identifies the computer virus propagation model categories based on network attack characteristics, constructs a multi hop cellular hybrid network virus propagation evaluation algorithm, The multi hop cellular hybrid network virus propagation model based on network attack can reduce the probability of computer suffering from network virus and ensure the security of user's computer network.

1 INTRODUCTION

The rise and rapid popularization of the Internet has brought more and more benefits to people's social and economic interests, but it has also created broader and favorable living conditions for the survival and spread of viruses. Due to the type and complexity of the network, and a variety of new viruses emerge in endlessly[1]. Therefore, in the current computer virus environment, how to effectively prevent and reduce the harm caused by network attacks to users has become a major focus of the current computer virus research. At present, the research on the propagation mode of network virus mostly adopts the method of bioengineering to imitate its propagation mechanism in the biosphere and build a differential mathematical model of network virus diffusion. Based on the characteristics of network attack, a virus identification method in Sir mode is proposed. However, the state transition rate of each node must be fixed in the whole network. Because the spread of network virus has many random and dynamic characteristics, in the traditional mathematical model of network virus propagation, it is difficult to analyze it accurately because it is only a regular variable[2]. When a network attack virus appears, users usually have different protection and protection: some users will use the network attack identification method to detect it and repair it to strengthen the network defense. Some people will install a patch on the website before being invaded by the virus, so that they have a certain resistance to the virus, while some people will leave the website temporarily before being invaded by the virus, and will reconnect to the website after the network recovers to normal. This is the so-called "repeated infection". Due to the errors in the mathematical model of computer virus propagation in the past and the lack of specific analysis of repeated infection, an optimization method of multi hop cellular hybrid network virus propagation model based on network attack is proposed[3].

2 CONSTRUCTION OF VIRUS PROPAGATION MODEL IN MULTI HOP CELLULAR HYBRID NETWORK

2.1 Identification of Computer Virus Transmission Model

Most viruses take network information as the target of attack, causing interference to network information and making it unable to work normally; If the distribution form of the file is damaged, the file name will be disconnected from the content of the file[4]. In addition, it will also cause the hard disk to be idle, because it will be copied continuously, which will greatly occupy the hard disk and arbitrarily modify the files; Since it takes up the cache time, many

Wu, F., Qian, L., Xu, H., Cai, X., Chen, H. and Zhou, C.
Optimization of Virus Propagation Model in Multi Hop Cellular Hybrid Network Based on Network Attack.
DOI: 10.5220/0011961400003612
In *Proceedings of the 3rd International Symposium on Automation, Information and Computing (ISAIC 2022)*, pages 566-573
ISBN: 978-989-758-622-4; ISSN: 2975-9463

viruses will be copied continuously after being started and exist in the cache, resulting in insufficient cache; For example, in the previous CIH, the BIOS file of the host was tampered with. Most network infections are caused by the connection with other network nodes. Every hour, the contact between the infected node and other nodes is called contact[5]. In the whole network, the connection rate is determined by the number of nodes in the whole network. Intrusion detection is an active defense technology, which can detect and respond in time when the multi hop cellular hybrid network is in danger. Its detection process is as follows (see Figure 1).

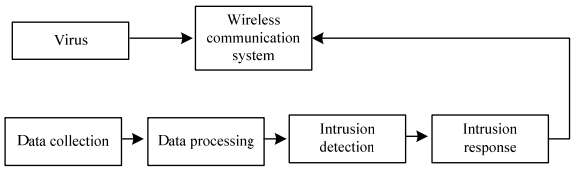

Figure 1: Network attack identification and detection process

Through the analysis of the above contents, we can draw the following conclusions: the process of virus invasion and diffusion in multi hop cellular networks mainly includes four stages: first, data acquisition, second, data processing, third, invasion, and fourth, response[6]. Aiming at the spread and spread of the virus, it is divided into four types: normal, abnormal, repaired and attacked. The adjustable parameter is the strength P of insulation measurement. The infection mode can be divided into two steps, i.e. "before control" and "after control", as shown in Figure 2 below.

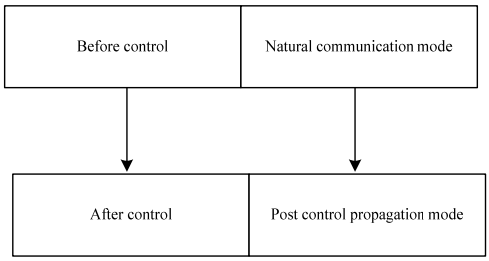

Figure 2: Schematic diagram of virus transmission sections

The network attack model is a virus that is close to natural diffusion, and the control after control is a difference equation based on the isolation strength after intervention. If the infected boundary cannot be immunized with the contaminated boundary, a certain degree of virus infection will occur, which is called "effective contact"[7]. This index reflects the infection of each infected state node to other state nodes, which is related to other factors, such as the diffusion strength of the network, the network connectivity of the infected node, and the network status. Generally, in a network node, there are susceptible States, infected States, immune states, potential states, and so on[8]. Therefore, in different modes, the probability of infection will also be different in the same state node. Since the spread of network virus is often hidden, the SEIR mode adds the hidden node to the Sir propagation mode. It is assumed that there is a virus with the virus in the node, but the virus in the node is not activated. Therefore, the node can carry the virus and also transmit the virus to other nodes[9]. After the infected state node is eliminated, there is a great chance that it will have permanent immunity to the virus, and then convert it into a node that can be infected. The situation transition of a typical SEIR mode is shown in Figure. 3:

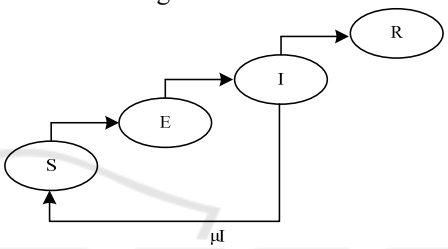

Figure 3: The SEIR model

In the identification of network attack, we must first find out the node of the attack subnet, then construct its location according to the location of the node, and determine its accuracy; On this basis, the fester algorithm is used to encrypt the password file to resist malicious intrusion and enhance the security performance of the system. If the basic position and parameter group of the network node:

$X=\{(a_1,b_1),(a_2,b_2),\cdots,(a_m,b_m)\}$, where (a_m,b_m) represents the location from the node to the m-th malicious attack. The attacked network node will change (a_m,b_m) before the end of the attack, it can be used to shorten the distance from the node and display the wrong location before the end of the attack[10]. When the child node transmits a data packet from a to B, it will also intercept the data packet, thereby causing interference; cause data B cannot receive the transmitted point by data A , expand at this time Y_m , N intercept the data received from the subnet, and then determine the location of the attack according to the characteristics of the attack, so as to build a node location model.

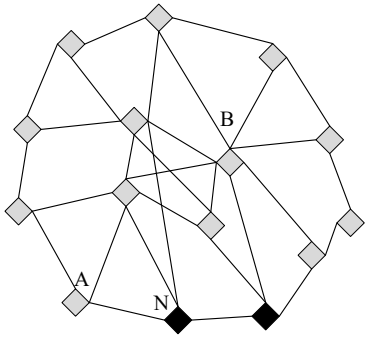

Figure 4: Location identification of malicious nodes

As can be seen from Fig. 4 that the real coordinates of the malicious node are (a, b), but the displayed error location is (a_m, b_m), In this case, the positioning accuracy of the malicious node will be reduced. Under normal conditions, the distance between point A and point B is:

$$S_{AB}=N(a_m,b_m)\sum X+Y_m/vt \tag{1}$$

According to the formula: V is A to B speed of point data packet transmission; t is A to B time taken to point the packet[11]. Assume that the proportion of malicious nodes in all nodes is, and all sub network nodes are M, then M selected from network nodes N node combination of is: $D=C_M^N-1$, Among the D selection combinations, the probability that at least one combination does not include malicious nodes is :

$$p'=S_{AB}-\left[M-C_M^N(1-Np)^N\right]^D \tag{2}$$

According to p',determine M, after that, a new combination mode is selected, and the distance between two nodes is calculated by this method, and it is regarded as a node to be processed. A new method is adopted to replace the actual position for accurate calculation:

$$E=\frac{\left(S_{AB}-\sqrt{(a_j-a_m)^2+(b_j-b_m)^2}\right)}{p'(N-M)}-V \tag{3}$$

In the formula: (a_j,b_j) select the sub network node coordinates of the jth scheme. Through the above reasoning, the node position in the attack sub network can be obtained, and the accuracy of its position can be obtained[12]. Because of the differences in network structure, network congestion, bandwidth, delay, traffic and protocol, and network nodes, the network propagation and interaction are greatly restricted. Therefore, it is necessary to further apply the stochastic mathematical model to the mathematical modeling of computer virus propagation to overcome the uncertainty of computer virus propagation.

2.2 Evaluation Algorithm of Virus Propagation in Wireless Network

Since the original Sir contains the delayed virus diffusion mode, this paper further improves the SIR model. A new method is proposed to study the spread of virus in Sir mode. Add the attack delay of the network terminal to this mode τ, That is, during the period from the beginning of the spread to the intervention, the expenses needed to combat the infection are recorded as b, The time is denoted by s, β represents the influence of the virus, η represents how many viruses are affected at t, λ represents how much immunity to the virus[13]. In order to build a new improved model, we assume that the latest one will be infected or affected by the virus, but the number will remain unchanged every other period, indicating the number of entries and greater than 0, γ indicating that its resistance to the virus also exceeded 0; The ratio of those susceptible to infection to those infected is 0 or more; At this time, the infected ones can be used to calculate the probability of virus as $A(t)$; This means that its resistance to this virus is also above 0; The proportion of computers susceptible to virus infection exceeds 0; At this time, the infected computer has the opportunity to perform computer operations, represented by u; A fixed speed used to express. Accordingly, the Sir improved communication mode is used to express:

$$w=E(1-p')b\mu s-\beta\eta\tau+\lambda \tag{4}$$

$$\varpi=\beta\eta s-(\mu+\gamma+\alpha)^2+uA(t)-\tau z \tag{5}$$

If the virus attacks the Internet, it will τ when conducting a network attack, n represents the cost required for conducting a network attack, and the above mode is optimized to τ and γ If we regard these variables as vectors for optimal solution, then any τ is necessary to satisfy: $\tau\le\gamma\le u$, and η is necessary to satisfy: $0\le\eta\le1$. This model does not consider the prevention (pre immune response) of network users as existence, that is, from the fragile environment to the transferred environment[14]. According to the data of the national system emergency management system, the failure to repair

and prevent software vulnerabilities on time is an important factor causing network attacks. The proliferation and mutation of network viruses will make the security of the network and the security awareness of users constantly improve, and the upgrading and downloading of the network will also gradually increase. The spread of the virus depends on its own characteristics and network topology. The distribution law of the disease in the epidemic process of China was discussed to provide scientific basis for formulating prevention and control measures in the future[15]. There are three traditional immune methods for complex network viruses: random, target and acquaintances. For a complex network, it needs a lot of manpower and material resources to establish a network with certain immune protection ability. Therefore, using randomization is a very easy strategy to achieve[16]. The key is to immunize only a specific network node. The random immune algorithm can get the same treatment on the larger node and the lower node in the network. If the concentration of an immune node in the network is g, the immune threshold is:

$$g_c = \eta - \frac{g\varpi}{w\lambda} \tag{6}$$

While the steady-state infection density was:

$$\rho_g = R\sigma\left(\frac{g_c - \varepsilon}{1-\varepsilon}\right), \varepsilon \le g_c \tag{7}$$

Optimization parameters ε is the cost of network attackm R is the incubation period of computer virus, σ is the wait time for network attack. See Table 1 for details of simultaneous optimization of these three parameters:

Table 1: Optimization of network attack cost, computer virus latency and network attack

Serial number:	Initial value of attack cost, waiting time and latency	Total number of infected computers under initial conditions	Optimized attack cost, waiting time and latency	The combined maximum of infected computers
A	0.5, 0.4, 1.6	35.08	0:56,0:32,1:46	38.72
B	0.2, 1,1	20.18	0:56,0:87,0:87	38.32

The collected data are not all used to detect the transmission route of the virus, so preliminary screening, missing value processing, noise elimination, attribute selection, data standardization and standardization processing must be carried out[17]. See Figure 5 for details:

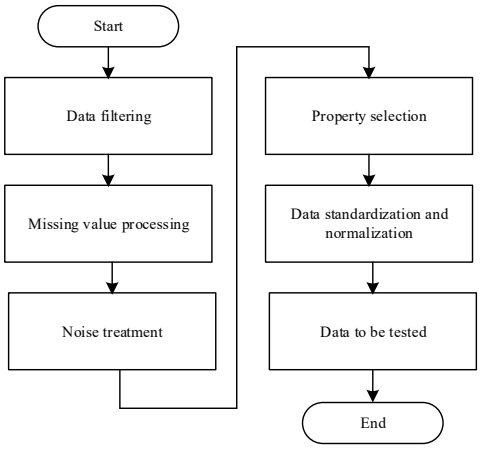

Figure 5: Data processing process

These data cannot be completely used to detect the infection path of the virus, so preliminary screening, missing value processing, noise elimination, attribute selection, data standardization and standardization processing are required[18]. Not all access networks are secure, and there may be viruses. There is a probability that the data will be infected after entering the system, which makes the system infected[19]. It is also possible that after connecting to the system, a firewall is set up to let the virus enter a new system.

2.3 Construction of Network Virus Propagation Model

In the multi hop hybrid network, intrusion detection is an important research content. On this basis, intrusion detection is carried out based on the network. This method has good self-adaptive learning performance, but it may also have problems such as local optimization and slow convergence[20]. Therefore, this paper first adopts an improved method based on genetic algorithm to solve these two problems. The optimized procedure is shown in Figure 6.

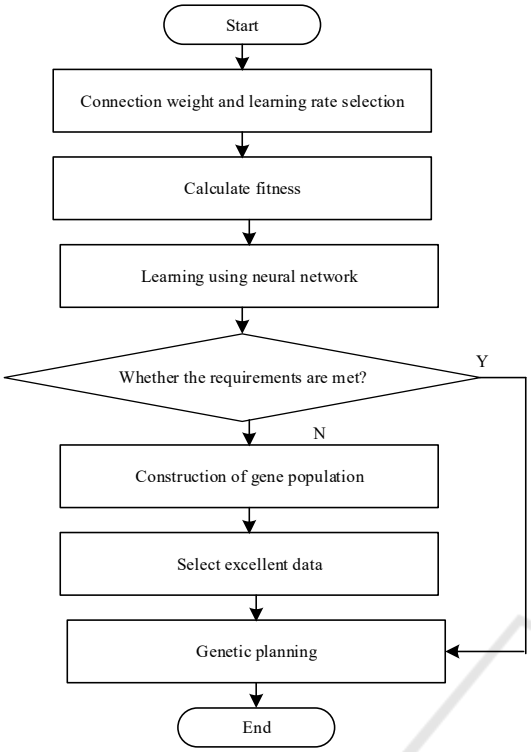

Figure 6: Network virus interception and virus identification rate

The biggest difference between this mode and the existing virus diffusion mode is that the connection between networks can only be used once at most. In the past, it has been found that in complex networks, more attention has been paid to the topology and properties of simple networks. But in social networks, user behavior plays a very important role. In a social network, if a node continuously sends messages containing the virus to neighboring nodes, it will strengthen the vigilance of other users. Therefore, few people will convey the same message to their neighbors. On this basis, an improved algorithm based multi hop cellular network virus intrusion propagation path identification model is proposed.

(1) A small part of the collected samples were randomly extracted and used as preliminary training, thus laying a theoretical foundation for the identification of the transmission path of multi hop cellular virus infection.

(2) Part of the data of a group of original training sets is extracted, and then the optimal solution is obtained by genetic algorithm.

(3) Adjust the network based on the optimal conclusion.

(4) In a wireless communication system, network detection is performed.

(5) According to the conclusion of the test, continuously upgrade the knowledge and training database.

(6) The detection of the invasion and diffusion pathway of the virus was completed.

Assuming that the multi hop cellular hybrid network in the attack path stores data in the form of P, the previous data will be covered by the subsequent multi hop network. When the attack network reaches the attack network, the correct attack path will include:

$$P'=\mathrm{P}\left(1-P\right)^{L} \tag{8}$$

It can be seen from the calculation results that in the case of multi hop and multi-point, the probability of occurrence in the packet is not the same in the case of multi hop and multi-point, which requires classification of the attacked IP. After classification, the form of IP file title is shown in Figure 7.

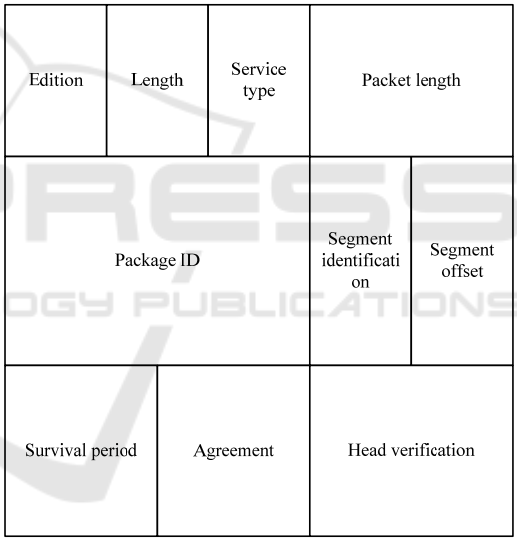

Figure 7: format of data transmission header after identification

As shown in the figure 7, the biggest feature of the immune resource allocation problem of some specific objects in the scale-free network is the distribution and imbalance of the number of nodes in the network. In the network, most of the nodes are very small, but some large nodes become hubs. Once infected, the nodes linked to it will be directly infected. By immunizing these nodes, the boundary between them and the nodes can be removed, which can greatly reduce the spread path of the virus and realize the immunity to the human body. In the multi hop cellular hybrid network, a random labeling method is used to represent. When the random number is lower than a

given value of X, a labeled information can be generated to track the control target in the high-speed network. This mode also reloads the operating system to represent its infection rate. In addition, the network worm cooperation of the model will cause users to kill virus or reinstall, and will make the network return from the infected state to the vulnerable environment. In order to simplify the model, this reinfection rate includes the mechanical reinfection rate caused by the user's adaptive habits and the mechanical reinfection rate caused by arbitrary reasons, so as to ensure network security.

3 ANALYSIS OF EXPERIMENTAL RESULTS

In order to verify the recognition effect of the model in this paper, the propagation of network viruses was discussed through MATLAB 2019 software. If the simple calculation of k = 0.5814 holds, then according to the hervez stability criterion τ =0, the virus equilibrium point is asymptotically stable locally, and the nodes in each state start to increase from the initial value, then start to decrease after reaching the peak, and finally slowly return to the equilibrium state and tend to be stable.

Figure 8 is a graph showing the change of the number of infected nodes in the regular network and the random network over time.

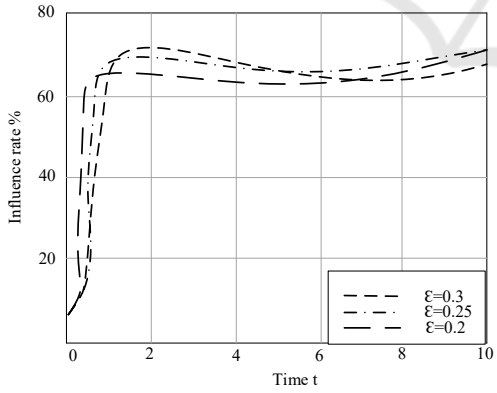

Figure 8: Effect of immune strategy on infected nodes in this model

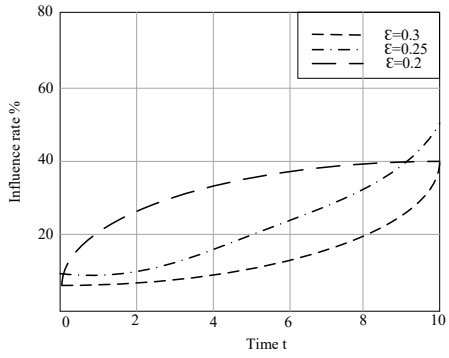

Figure 9: Impact of immune strategy on infected nodes in traditional neural network model

It can be seen from the figure that in the same environment, compared with the traditional neural network model, the model in this paper has a relatively high impact rate on the infected nodes in the actual application process, so as to better ensure the network operation safety. Meanwhile, with the increase of antibody concentration, that is, the effectiveness of vaccination, the time that patients have been infected will be shorter, and the peak number will be less. In each immune mode, when the network is in a stable state, the number of infected nodes will show a stability of L, which means that when the effectiveness of the immune strategy is improved, when the network is in a stable state, the number of infected nodes will gradually decrease, which means that the number of threatened nodes will gradually decrease. Therefore, when dealing with network viruses, we should take appropriate preventive measures, such as setting firewalls and anti-virus software, to enhance the immunity of the network. To ensure network security, the time evolution law of infected nodes under different latency delays of network attack viruses is further studied, as shown in the following Figure 10:

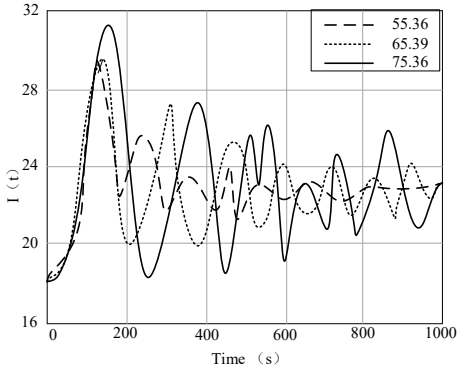

Figure 10: Time evolution of infected nodes under different latency delays of network attack virus

It can be seen from the Fig. 10 that the latency of the system μ It will play a certain role in the occurrence and spread of the disease. With the extension of the incubation period and the large-scale spread of the virus, the speed of its spread will gradually accelerate. Over time, the number of the largest infected nodules decreased, meaning that its transmission range became smaller. Therefore, when a network virus is infected, it will attack immediately, without continuous waiting or lasting too long. Then, it will be detected early, thus reducing the damage to the system. Based on the results in FIG. 10, the comparison records of detection results of several common methods are shown in Table 2:

Table 2: Calculation results of model operation efficiency

Experimental sample data (PCs.)	This method (%)	Based on artificial immune method (%)	Based on data mining method (%)	Machine learning based method (%)
100	99	91	88	87
200	99	90	86	85
300	98	90	87	83
300	98	90	88	85
400	99	89	85	83
500	97	88	84	81
600	97	89	85	82
700	97	87	84	82
800	97	89	85	81
900	98	88	83	81
1000	98	87	83	81
Average value (%)	97.9	88.9	85.2	82.6

It can be seen from the table that the algorithm is used to detect the virus intrusion propagation path in multi hop cellular network, and the detection rate reaches 97.9%; The artificial immune method is used to identify the intrusion path of multi hop cellular hybrid network, and the accuracy of identification is 88.9%; By using data mining technology, the virus intrusion path of multi hop cellular hybrid network is detected, and the recognition accuracy reaches 85.2%; The comparison with the above methods shows that this method has a good recognition effect, can detect the intrusion of virus and ensure the security of the network.

4 CONCLUSIONS

In this paper, we study the repeated cases in the process of network virus propagation, and use the original network attack to express the transition rate between various states, so as to obtain a new multi hop cellular network virus propagation detection model. From the simulation results, this model can well reflect the spread of the virus, so as to ensure the security of network operation.

ACKNOWLEDGEMENTS

This work is sponsored by: (1) the team for science &technology and local development service of Nantong Institute of Technology under Grant No. KJCXTD312; (2) the science and technology planning project of Nantong City under Grant No.JCZ20172,JCZ20151,JCZ20141,JCZ21084,JCZ21025,JCZ21033; (3)the second batch of industry university cooperation collaborative education projects of the Ministry of education in 2021 under Grant No.202102594016.

REFERENCES

LIAN Jing, FANG Siyu, ZHOU Ya-u. (2020). Model Predictive Control of the Fuel Cell Cathode System Based on State Quantity Estimation. Computer Simulation, 37(07):119-122.

Wang H, Li W. (2021). DDosTC: A transformer-based network attack detection hybrid mechanism in SDN. Sensors, 21(15): 5047.

Oliveira N, Praça I, Maia E, Sousa O. (2021). Intelligent cyber attack detection and classification for network-based intrusion detection systems. Applied Sciences, 11(4): 1674.

DU Chunhui. (2020). Optimization design of video monitoring system on fully-mechanized mining face. Industry and Mine Automation,46(8):94-100.

Ren H, Deng J, Xie X. (2022). Grnn: generative regression neural network−a data leakage attack for federated learning. ACM Transactions on Intelligent Systems and Technology (TIST), 13(4): 1-24.

Kong X, Ge Z. (2021). Adversarial Attacks on Neural-Network-Based Soft Sensors: Directly Attack Output. IEEE Transactions on Industrial Informatics, 18(4): 2443-2451.

Zaripova D A.(2021). Network security issues and effective protection against network attacks. International Journal on Integrated Education, 4(2): 79-85.

Do Xuan C, Dao M H.(2021). A novel approach for APT attack detection based on combined deep learning model. Neural Computing and Applications,33(20): 13251-13264.

HU Liwei, FAN Zijian, ZHANG Suhang, et al.(2021). Risk Propagation Mechanism and Application of Urban Traffic Congestion Factors Based on Complex Networks. Journal of Transportation Systems

Engineering and Information Technology, 21(2):224-230.

Chaudhari R, Deshpande M. (2022). A Systematic Review of DoS Attack Prevention Techniques on Delay Tolerant Network. JOURNAL OF ALGEBRAIC STATISTICS, 13(3): 3412-3428.

YING Weiqiang, LUO Shijian, ZHANG Lingyan. (2021). Delay Control Model of Unbuffered Digital System Based on Neural Network. Computer Simulation, 38(11):249-253.

LI Yong, DONG Sixiu, ZHANG Qiang, et al.(2021). Research on the Hierarchy of Node Influence in Attention Flow Network. Computer Engineering, 47(8):109-115,123.

Osman M, He J, Mokbal F M M, Zhu N. (2021). Artificial neural network model for decreased rank attack detection in RPL based on IoT networks. Int. J. Netw. Secur, 23(3): 496-503.

Yang L, Song Q, Wu Y.(2021). Attacks on state-of-the-art face recognition using attentional adversarial attack generative network. Multimedia tools and applications, 80(1): 855-875.

Ahmad F, Ahmad A, Hussain I, Muhammad G, Uddin Z, AlQahtani S A. (2021). Proactive Caching in D2D Assisted Multitier Cellular Network. Sensors, 22(14): 5078.

Fekih M, Bellemans T, Smoreda Z, Bonnel P, Furno A, Galland S.(2021). A data-driven approach for origin–destination matrix construction from cellular network signalling data: a case study of Lyon region (France). Transportation, 48(4): 1671-1702.

Sheu T L, Wu Y J, Lin Y H.(2021). An Analytical Model for a Sectored Cellular Network with Embedded Small Cells. Journal of Computer and Communications, 9(11): 128-149.

Abdalla A S, Yingst A, Powell K, Gelonch-Bosch A, Marojevic V. (2022). Open source software radio platform for research on cellular networked UAVs: It works. IEEE Communications Magazine, 60(2): 60-66.

Ali S M R, Sarkar M Z I. (2022). Enhancing Security in Correlated Nakagami-m Fading Cellular Network Using SC and SSC Diversity Combining. Wireless Engineering and Technology, 13(1): 1-17.

Borralho R, Mohamed A, Quddus A U, Vieira P, Tafazolli R.(2021). A survey on coverage enhancement in cellular networks: Challenges and solutions for future deployments. IEEE Communications Surveys & Tutorials, 23(2): 1302-1341.