Application of nonlinear recursion equation in network security risk detection

Abstract: In order to solve the problem of recursion equation in network security, the author proposes an application of network security risk detection. The search efficiency of the artificial intelligence planning algorithm is better than the traditional attack graph generation method, designed and implemented a planning engine for security risk assessment, according to the application problem definition, design data processing methods and grammar translation modules; efficient planning algorithms for penetration plan planning are selected and the analysis of the risk association process is completed. First, the development status and challenges of network security are summarized, and then, the research status of existing risk assessment methods is analyzed, the research ideas are introduced, and the main research results are given; the organizational structure is listed at the end. In the optimized parallel algorithm for recursive equations, when using P processors to solve a class of recursive equations of size N, the speedup of this algorithm is $O(p)$, where $1 > p > 0.1$ is an arbitrarily small positive number. Using the advantages of neural networks dealing with nonlinearity and complexity to predict the network security situation based on the improved recurrent neural network, the experimental results prove that the proposed method has high operation efficiency, low error and high accuracy compared with the actual value.

Keywords: recursion equation, network security, risk detection, application

1 Introduction

In recent years, with the continuous development of artificial intelligence technology, it has been widely used in various fields including cybersecurity. From this point of view, it comprises a lot of content, and the most important is the expert system. Through the application of this system, it is integrated with the intrusion detection technology to improve the detection of viruses and prevent the intrusion of viruses to the greatest extent. After the application of this technology, an expert system can be built into the network. This system contains the experience of a large number of experts and uses it as a knowledge base, when external information invades. The expert system will be retrieved using a type of information. By comparing with the expert experience information and judging the specific situation of the information, whether it is good information or virus information, if it is the former, it can enter normally, and its information is imported into the expert system; then, the network is protected. In addition to the intrusion detection system, artificial neural network technology is also applied. Through experimental evidence, such as massively parallel processing, good rod performance, distributed storage, and the computational time complexity of the network are almost similar; being zero makes the neural network solving nonlinear equations a strong advantage. This method is also widely used in other fields. The ability of fast learning can be realized by constructing neural network with field programmable gate array. And the design cycle is short and the system speed is fast. With high reliability, the whole system can be integrated into a single chip. This technology is developed based on the human nervous system; its resolution is very high, and even if the intrusion information contains noise, it can be found and effectively applied, while improving the reaction efficiency, strengthening the processing of intrusion signals and providing important help for network security operation as shown in Figure 1.

2 Literature review

Network security risk assessment is an important method of active defense, which can complete the security risk identification of complex network environments such as
enterprise networks, helping effectively organize various security protection means for comprehensive defense and ensuring corporate network security. Network security, usually refers to the security of the computer network, can also refer to the security of the computer communication network. This network is a system that connects several computers with independent functions through communication equipment and transmission media and realizes the information transmission and exchange between computers under the support of communication software.

It mainly researches the risk process analysis method based on the artificial intelligence planning method and existing risk assessment method based on attack graph. An attack graph generation engine is designed and implemented using the Fast-forward planning algorithm. Furthermore, on the basis of the risk process analysis, the risk impact index RI is innovatively proposed based on the maximum attack reward expectation; it has shown good results in the risk assessment for the actual network. With the deepening of network security research, more and more scholars realize that the
The best way to secure a system is to switch perspectives, consider how an attacker would break into the system, in an attack-oriented way, establish a scientific and reasonable model for the target network and attackers, and show the possible intrusion process of the attackers, to conduct a qualitative and quantitative evaluation of network security, know the implementation of network security hardening measures, etc. [1].

Knowledge-based risk assessment methods are mainly based on experience obtained from security experts and are used to solve risk assessment problems in similar scenarios. The advantage of this approach is that it can directly provide the recommended protection measures, structural framework and implementation plan. Bum-Joon proposed a risk data model called risk data repository, in which all data related to information security in the organization are defined and stored, and can continuously add new data reflecting the security status of the information system to expand “knowledge.” It can be used to infer the information security risks faced by the system at present or in the future [2]. Bauer, G proposed a “good practice”-based approach to knowledge assessment. The approach develops an abuse and misuse reporting database and an extended information security framework. Thousands of safety cases over the past 30 years are stored in the database. The information security framework is used to assist users in formulating comprehensive and correct organizational security policies [3]. In 2002, Bauer, G proposed a security tool Net-Map64 [4] for modeling, information discovery and analysis of the network. Relying on a concrete network that is not limited by network layers, it is able to integrate network information at all levels [5]. In 2005, He X proposed a rule-based topological vulnerability analysis method [6]. The method expresses individual attacks as a rule-based system of transfer rules and defines a non-interfering rule set. The optimized vector computing of recursive equations is also now threatening the security of traditional encryption algorithms. Quantum communication and quantum computing are the two most widely used technologies in the field of network security, and they are also the most closely related to network security. Ashton Webster proposed the use of Privilege Graphs to describe the process of intruder privilege escalation. The nodes of the privilege graph represent the set of privileges possessed by users and user groups, and the connections between the nodes represent the transfer of privileges caused by vulnerability exploitation, it reflects the user who has the permission of the starting node, using the existing vulnerability can obtain the authority represented by the target node, and different paths to the attack target represent different processes of the intruder to carry out the attack [7]. Frantzen proposed an analysis technique based on Petri nets to model network vulnerability, where the location represents the security state of the entity, and the transition represents the change of the state; the reasons for state change include input events, commands or data, and the positions and transitions are connected by directed arcs [8].

Based on the current research, the author proposes an application of network security risk detection. Security risk assessment discards the idea of passive defense and identifies its own assets and vulnerabilities before the attack threat occurs, simulates and characterizes potential threats, conducts risk estimation for possible threats, and then formulates security protection and remediation measures. Therefore, network security risk assessment is an important security protection method to ensure national security and protect enterprise assets, and it is also a research hotspot in academia [9].

3 Application of recursive equation in network security risk detection

3.1 Concept of cybersecurity risk

In the information security risk assessment specification promulgated by our country, the composition of network security risk assessment is shown in Figure 2. The main content is aimed at the interaction between threats and vulnerabilities, vulnerability, the impact relationship with assets, and the possible loss caused by security threat events and threats under the two effects, quantifying the risk.

3.2 Research status of network security risk assessment and detection technology

Network security risk assessment, control and prediction technology, by analyzing the vulnerabilities of network systems, the threats they face, and the security measures adopted, comprehensively perceives the security risks faced by the network and provides corresponding solutions to ensure the normal operation of the network, which is a means of qualitative and quantitative analysis of network security; it is a fine measurement of network security and the overall process of determining, controlling, and mitigating security incidents affecting network security.
resources. The process includes three levels of network security risk assessment, network security risk control and network security risk prediction [10]. At present, there are more and more studies on these three levels at home and abroad, but the corresponding technical framework has not yet been perfected, and the research on specific evaluation models and evaluation algorithms is still in its infancy and lacks systematic quantitative analysis tools and supporting platforms; it is very necessary to do in-depth research on these issues. Next, the research status of this problem is introduced from the three aspects of network security risk assessment, control and prediction.

### 3.3 Status quo of network security risk assessment

The research on security risk generally revolves around risk assessment and risk management, the former assesses and predicts the possibility and impact of system losses under the interaction of existing assets, vulnerabilities and threats; the latter uses the risk calculation results of the former to construct a security patching strategy, adjusts the defense configuration of the system, and then reduces the risk to an acceptable level. The two complement each other and complete the overall mastery and control of system security risks to ensure system security.

Network security risk assessment mainly focuses on a comprehensive analysis of various factors of the system, calculation and evaluation of risks, generally divided into qualitative analysis and quantitative analysis. For the qualitative analysis such as model-based security risk assessment, the researchers proposed methods such as attack tree fault tree, privilege graph and attack graph to deduce the vulnerability correlation of the network and demonstrate potential threat paths. The quantitative analysis focuses on the single-point risk calculation for different levels of assessment objects, and the overall comprehensive risk calculation, generally starting from the harm of single-point vulnerability and the possibility of vulnerability being exploited, for example, the Bayesian method, D–S evidence theory method, etc., is used to determine the risk probability. Then, based on considering the value of inherent assets, single point VaR and composite VaR are calculated to assist risk management.

The diversity, complexity and security threats of network systems continue to escalate, uncertain network security problems emerge in an endless stream, traditional single-function protection methods such as firewalls and intrusion detection, and the new means and technical methods are not enough to defend against advanced network attacks, and comprehensive strategies and methods of active defense must be considered in order to be integrated and prevent problems before they occur [11]. As an important measure of active defense, network security risk assessment has been widely used in the field of network information; it has been highly valued by the government, enterprises, military and scientific research institutions, and established a series of evaluation standards such as ITSEC and ISO/IEC 13335. The method has played a guiding and promoting role in the development of network security risk assessment technology. Based on the specifications and guidance given by the standard, methods and technologies for specific implementation have been widely carried out in academia and industry: continuous innovation, using failure mode impact analysis in the preparation stage of risk assessment; logic analysis method; Dephi method in qualitative analysis; analytic hierarchy process analytic hierarchy process in quantitative analysis. In terms of risk assessment
tools, there has been a knowledge-based risk assessment system CycSecurity; MulVAL systems based on logical reasoning are constantly emerging.

3.4 Development status of network security technology

The root of the network security problem is the vulnerability of the network system itself, if a system without any vulnerability can be designed; then, all security problems can be solved easily; eliminating system vulnerabilities has long been studied as the most primitive line of defense for system security. At the beginning of computer technology, system designers adopted various technical and management measures. They are all used to design safe systems, but the practice has proved that it is impossible to design an safe system. Any artificial system inevitably has various weak links, but if the vulnerability of the system can be detected and repaired in time, then various security hazards can be reduced [12]. The purpose of vulnerability detection technology is to detect computer network systems, or network equipment performing security-related detection, in order to identify security risks and vulnerabilities that may be exploited by hackers; network administrators can repair and reduce potential threats on time before failures occur. Vulnerability detection technology mainly includes host detection technology, operating system detection technology, access control rule detection technology, port scanning technology and vulnerability identification technology. With the rise of mobile Internet, the development of cloud computing, industrial control and other technologies, the difference between internal and external networks is gradually weakened, and the business is gradually pulled to the external network processing. Especially in the past, banks, governments and other institutions, only counter business, can also be processed online, and network security is becoming more and more serious.

3.5 Application advantages of artificial intelligence technology in the field of network security risk detection

1) Accurately handle network information

The use of artificial intelligence technology in the field of network security can fully demonstrate the advantages and characteristics of the use of artificial intelligence technology, improve the efficiency of network security management, and ensure network security [13]. Compared with traditional network security management technology, artificial intelligence technology has great advantages in processing network security information. It can use functions similar to those of human intelligence to deal with some unknown network security problems; the accuracy of network security information processing is high. A large amount of ambiguous information or vocabulary will be generated during network operation, which will cause certain difficulties in network security management. The application of artificial intelligence technology can process such network security information using fuzzy logic reasoning, and quickly searching and processing it, so as to obtain a good processing effect [14].

2) Strong learning and processing ability

The biggest advantage of artificial intelligence technology in the field of network security is that it can self-learn; this is a function that traditional network security technology does not have. In the process of specific application, the application of artificial intelligence technology can find effective information in massive network data information, and the processing efficiency of data information is very high. In the process of applying artificial intelligence technology in the field of network security, the given data information can be used for self-reasoning and learning, finding the law and method of data information search, so as to accurately find effective information in a very short period of time and improve the efficiency of network security management.

4 Experiments and research

4.1 Design of network security risk detection system

4.1.1 Hardware design

The hardware of the network security risk detection system based on the N-gram algorithm includes a data preprocessing module and a collaborative analysis module [15]. The data preprocessing module is mainly responsible for processing captured data packets with security risks and consists of a detection engine and a packet decoder [16]. For the collected data packets, the actual elements contained in the packets are first decoded by the packet
decoder, and the specific decoder workflow is shown in Figure 3.

The packet decoder first concatenates the decoded data, builds a network stack, and then decodes the protocol elements in a way that moves from the bottom layer to the top layer. Finally, each decoded packet is combined into a data structure and sent to the detection engine for analysis [17].

The main function of the detection engine is to check the decoded data packets, test whether there are suspicious behaviors that threaten network security, and modify the suspicious behaviors. Since some packets can disguise themselves through methods such as payload transformation, before checking for suspicious behavior, the detection engine first needs to modify the rules of the data packet. In addition to this, the detection engine is able to normalize traffic patterns to accurately match packet characteristics [18].

4.1.2 Collaborative analysis module

The collaborative analysis module is mainly composed of a collaborative collector, a collaborative analyzer, a collaborative sensor and a collaborative manager. The specific module diagram is shown in Figure 4.

In the collaborative analysis module, the collaborative collector is mainly responsible for receiving the relevant detection data of each node, reported to the synergy analyzer through the synergy sensor.

4.2 Optimized vector parallel algorithm for recursive equations

The author presents a parallel method for solving this kind of recursive equations; the algorithm combines the idea of recursive multiplication (RD) and the idea of vertical and horizontal processing (V–H).

In the overvoltage protection algorithm, we assume that the number of processors is \( p \), the scale of the recurrence equation is \( N \), and \( N = mk \). The algorithm is divided into three steps: The task is divided into \( mk \) segments, and the size of each segment is \( k \).

1) The \( mk \) segment is calculated serially at the same time, and the relative value of each segment is obtained.
2) For the relative endpoint values of each segment obtained in step 1, the RD method is applied to find the final endpoint value of each segment.
3) Each segment uses the endpoint value of the upper segment obtained in step 2 as the initial value for simultaneous serial calculation, and the final result is obtained.

The specific algorithm is as follows:

For \( t = 1 \), then \( k - 1 \);
For \( i = 0 \), then \( p - 1 \)

The recurrence equation defined by the author is a formal description of a large class of recurrences; therefore, the time taken to calculate the functions \( f, g, \) and...
4.3 Security risk assessment methods

Since qualitative risk calculations only use estimates such as “high,” “medium” and “low” to determine the level of risk, it is difficult to establish a comprehensive method of overall risk; there are too many subjective factors, and the difference is large. In order to measure and quantify the risk calculation more accurately and facilitate the comparison and synthesis, the National Bureau of Standards provides a basic risk calculation method as shown in formula (1) [20].

\[
\text{ALE} = \sum_{i=2}^{m} M(O_i) \times F_i. \tag{1}
\]

If we estimate the size of this intermediate variable, estimates will jump, because when \( m = 14 \), the result has hundreds of 100 million, 100 million digits, each number has 14 bits long, and to get \( m = 15 \) results, we need to store \( m = 14 \) results in memory variables for iterative calculation, no matter what format, almost will encounter a single machine memory limitations, if the arrangement combination number continues to increase; the result will memory overflow. Where \( n = \{0, 1, 2, \ldots\} \) is the set of risk sources existing in the target system, \( I(0) \) is the quantified value of the loss caused by each risk 0 and \( F \) represents the risk 0; the possibility of occurrence – generally used probability representation. In this way, ALE can be used as the risk quantification value of the target system; this calculation method is scientific and objective and has been widely adopted since then. As for how to establish the loss caused by risk and the probability of risk occurrence, later generations began to carry out a series of researches on the probability of attack and the loss or impact caused by attack [21]. Generally, the target network to be investigated is calculated and analyzed at the level of risk, which is divided into three levels: component level (service level), host level, and network level (system level) for weight accumulation; let \( v \) denote an attacking node for a certain service, and \( P(v) \) denote the attack success probability; then, the service risk is expressed as shown in formula (2).

\[
\text{Risk}_{\text{serv}}(V) = p_v(V) \times (\lambda_C \cos t_{-\text{C}}(V) + \lambda_I \cos t_{-I}(V)) \tag{2}
\]

4.4 Cyber risk assessment model

4.4.1 Basic concepts

Network security risk assessment is an assessment of computer networks and the services running on them, according to the external attack data in the computer network and the impact of its own vulnerability on network assets, and comprehensively analyzes the security of each link of the computer network, thereby assessing the security of the entire network. It is the foundation of the network security management system, by understanding the current risk of the system and assessing the degree of security threat and impact that the risk may bring, so as to reduce the risk of the system to an acceptable level; it provides a direct basis for reducing network risks and implementing risk management [22].

Network security risk assessment can be done by mapping its assessment steps to those of a network attack, in order to achieve anti-network security risk assessment; the assessment steps can be matched with the steps of network attacks, so as to achieve the purpose of preventing the network from being attacked. Network attacks are generally the purpose of remote information collection, data analysis, remote attacks, and local attacks on the network. A network attack is generally composed of several steps, such as remote information collection, data analysis, remote attack, local attack, and local information collection, the network security risk assessment is composed of several steps such as data collection, data attack, and local information collection; it is a process of data collection, data processing and data analysis, which mainly includes three stages: information collection, data association and fusion processing, and comprehensive assessment. The method of processing and data analysis mainly include three stages: information collection, data association and fusion processing, and comprehensive evaluation; the general steps are local information collection, data analysis, remote data collection, data analysis, and comprehensive evaluation. From the above-mentioned two-step analysis, it can be seen that the steps of risk assessment and network attack are opposite. Therefore, the two-step analysis of network security risk assessment shows that risk assessment and the steps of network attack are contrary. Therefore, the
research on network security risk assessment is closely related to network attacks [23–27]. The studies assessed are closely related to cyberattacks as shown in Figure 5.

4.5 Experimental method and process

In order to verify the performance of the network security risk detection system based on the N-gram algorithm, experiments are carried out. First, the experimental environment server of the network security risk detection system is configured based on the N-gram algorithm, including server hardware configuration and server software configuration; the hardware configuration is shown in Table 1.

The software configuration is shown in Table 2. Real network data as is taken as experimental data, and boundary value processing is performed on it to form typical experimental data. The experimental data after processing are shown in Table 3.

The experimental data are input into the network security risk detection system based on the N-gram algorithm, and the network security risk detection is performed based on the server [28]. In order to ensure the fairness and effectiveness of this experiment, the traditional network security risk detection system and the network security risk detection system based on the N-gram algorithm proposed by the author are jointly tested, comparing the packet inspection performance of various network security risk detection systems. The basis for judging the performance of data packet detection is mainly the average detection time of various types of data packets. The author selects five kinds of data packets for experiments, when the sum of the average detection time of various types of data packets is smaller, this proves that its packet detection performance is stronger. On the contrary, it proves that its packet detection performance is worse.

5 Conclusion

In this study, we propose a fast square for a system of nonlinear equations. Then, this method can solve the unknown parameters quickly and accurately. Pass through Matlab software simulation and quartusII hardware
simulation can demonstrate this method is correct, and the design is reasonable. A fast square for a system of nonlinear equations is proposed in this article. Then, this method can solve the unknown parameters quickly and accurately. This article studies the network security risk assessment based on the nonlinear programming method. The main work and innovations include the following two aspects:

1) Studying the evaluation model, main process and general method of network security risk assessment, and analyzing and summarizing the shortcomings of network security risk assessment. At the same time, in-depth study of network security scenario scenario modeling, especially the scenario modeling method based on the planning problem model is carried out; it summarized the network security scenario model results for the establishment of methods for intelligent planning problems at the emergence stage and further analyzed and researched the application of intelligent planning in the field of network security.

2) A network security model CSC-Model for artificial intelligence planning is proposed, on the basis of general vulnerability utilization modeling; multi-level factors of attack and defense are included, comprehensive network model, attack method library and attacker behavior model, building network scene models capable of exhibiting fine-grained vulnerability exploitation actions. The concept of attack agent, which is used to simulate the actual network penetration behavior of the attacker, is mainly put forward and further transformed the network scene modeling into the establishment of application for security planning problems; it includes the planning domain that describes each ontology of the scene and the problem domain required to model the risk-related process for specific goals. The challenge of network security needs to establish zero-trust security prevention and control framework based on a dynamic minimum authorization strategy, complicate network connection matrix, intelligent threat governance framework with multi-dimensional detection, accurate analysis, linkage response, intelligence enabled, security governance framework of the data life cycle with flexible scalable and business adaptive, and continuous precipitation of digital assets, building global threat intelligence ecology and coping with unequal attack and defense resources. The future trend needs government departments, network security enterprises, network security experts and other parties to form intelligence synergy, data collaboration, ability, jointly build cyberspace governance and collaborative defense capability system, promote global threat intelligence sharing, and build a global threat intelligence ecology, hand in hand to build cyberspace destiny community, power sustainable security operation.

**Acknowledgment:** The author thanks Anhui University Blockchain Application Integration sub center (2020qkl17), and He Jun Technical Skill Master Studio (2020dszgs17).

**Funding information:** The author states no funding involved.

**Author contributions:** The author has accepted responsibility for the entire content of this manuscript and approved its submission.

**Conflict of interest:** The author states no conflict of interest.

### References

1. Zhao D, Song H, Li H. Fuzzy integrated rough set theory situation feature extraction of network security. J Intell Fuzzy Syst. 2021;40(1):1–12.
2. Ashoor AS, Kazem A, Gore S. An interactive network security for evaluating linear regression models in cancer mortality analysis and self-correlation of errors by using durbin-watson tests in babylon/iraq. J Phys Conf Ser. 2021;1804(1):112–27.
3. Einy S, Oz C, Navaei YD. The anomaly- and signature-based ids for network security using hybrid inference systems. Math Probl Eng. 2021;2021(9):1–10.
4. Liang W, Xie S, Cai J, Xu J, Qiu M. Deep neural network security collaborative filtering scheme for service recommendation in intelligent cyber-physical systems. IEEE Internet Things J. 2021;PP(99):1.
5. Vajjha H, Sushma P. Techniques and limitations in securing the log files to enhance network security and monitoring. Solid State Technol. 2021;64(2):1–8.
6. He X. Research on computer network security based on firewall technology. J Phys Conf Ser. 2021;1744(4):42–7.
7. Zhao J. Research on network security defence based on big data clustering algorithms. Int J Inf Comput Secur. 2021;15(4):343–4.
8. Jiang L. On the relationship between computer firewall technology and network security. J Phys Conf Ser. 2021;1744(3):132–7.
9. Togay C, Kasif A, Catal C, Tekinedogan B. A firewall policy anomaly detection framework for reliable network security. IEEE Trans Reliab. 2021;71(1):339–47.
10. Du Z. Network security model based on active and passive defense hybrid strategy. Converter. 2021;64(2):46–51.
11. Zhan K. Design of computer network security defense system based on artificial intelligence and neural network. J Intell Fuzzy Syst. 2021;20(9):1–13.
[12] Wang X, Na C, Wei B, Zhou M. Research and implementation of key technologies of network security system software. J Phys Conf Ser. 2021;1992(3):32–95.
[13] Li Y, Li X. Research on multi-target network security assessment with attack graph expert system model. Sci Program. 2021;2021(3):1–11.
[14] Zhang L, Chen Z, Yang S. Application of artificial intelligence in computer network security. J Phys Conf Ser. 2021;1865(4):42–9.
[15] Jiang C. Network security and ideological security based on wireless communication and big data analysis. Wirel Commun Mob Comput. 2022;2022(3):1–6.
[16] Li C, Sun X, Zhang Z. Effective methods and performance analysis of a satellite network security mechanism based on blockchain technology. IEEE Access. 2021;9(3):113558–65.
[17] Yang X, Zhu A. Research on computer network security emergency response systematization. J Physics Conf Ser. 2021;1771(1):12–22.
[18] Yang H, Zeng R, Xu G, Zhang L. A network security situation assessment method based on adversarial deep learning. Appl Soft Comput. 2021;102(8):107–6.
[19] Chapman P. Defending against insider threats with network security's eighth layer. Comput Fraud Security. 2021;2021(3):8–13.
[20] Kong D, Li H, Dong H. Research on network security situation assessment technology based on fuzzy evaluation method. J Phys Conf Ser. 2021;1883(1):102–8.

[21] Sallam RA, El-Sheikh MMA, El-Saedy EI. On the oscillation of second order nonlinear neutral delay differential equations. Math Slov. 2021;71(4):859–70.
[22] Zhu B, Wang Y, Zhang H, Xie X. Fuzzy functional observer-based finite-time adaptive sliding mode control for nonlinear systems with matched uncertainties. IEEE Trans Fuzzy Syst. 2021;30(4):918–32.
[23] Melliani S, Mfadel AE, Chadli LS, Elomari M. Stability of intuitionistic fuzzy nonlinear fractional differential equations. Notes Intuitionistic Fuzzy Sets. 2021;27(1):83–100.
[24] Hillier C, Balyan V. Error detection and correction on-board nanosatellites using hamming codes. J Electr Comput Eng. 2019;2019(6):1–15. doi: 10.1155/2019/3905094.
[25] Babalola OP, Balyan V. Efficient channel coding for dimmable visible light communications system. IEEE Access. 2020;8:215100–6. doi: 10.1109/ACCESS.2020.3041431.
[26] Balyan V, Daniels R. Resource allocation for NOMA based networks using relays: cell centre and cell edge users. Int J Smart Sens Intell Syst. 2020;13(1):18.
[27] Balyan V. Outage probability of cognitive radio network utilizing non orthogonal multiple access. 7th International Conference on Signal Processing and Integrated Networks (SPIN); 2020 Feb 27–28; Noida, India. IEEE; 2020. p. 751–5.
[28] Sun J, Shen B, Qi J, Liu Y. Stubborn \( h^\infty \) state estimation for nonlinear distributed parameter systems subject to measurement outliers. Int J Robust Nonlinear Control. 2022;32(1):13–28.