INTERNATIONAL JOURNAL OF CIRCUITS, SYSTEMS AND SIGNAL PROCESSING
DOI: 10.46300/9106.2022.16.66 Volume 16, 2022

A Sensing Method of Network Security Situation Based on Markov Game Model

Bingjie Lin, Jie Cheng, Jiahui Wei, Ang Xia

State Grid Information & Telecommunication Branch, Beijing 100053, China

Received: June 11, 2021. Revised: December 23, 2021. Accepted: January 12, 2022. Published: January 14, 2022.

***Abstract*—The sensing of network security situation (NSS) has become a hot issue. This paper first describes the basic principle of Markov model and then the necessary and sufficient conditions for the application of Markov game model. And finally, taking fuzzy comprehensive evaluation model as the theoretical basis, this paper analyzes the application fields of the sensing method of NSS with Markov game model from the aspects of network randomness, non-cooperative and dynamic evolution. Evaluation results show that the sensing method of NSS with Markov game model is best for financial field, followed by educational field. In addition, the model can also be used in the applicability evaluation of the sensing methods of different industries' network security situation. Certainly, in different categories, and under the premise of different sensing methods of network security situation, the proportions of various influencing factors are different, and once the proportion is unreasonable, it will cause false calculation process and thus affect the results.**

***Keywords*—Markov game model, fuzzy comprehensive evaluation, sensing method, network security situation**

I. INTRODUCTION

Nowadays, the Internet, as an essential tool, has been widely applied in various aspects of human life. The sensing model of network security situation has become a hot issue. Meanwhile, network security has become a hidden danger for work and life. Thus, study on the sensing of network security situation is particularly important. As early as the end of the last century, international scholars had studied the sensing of network security situation from the perspective of sensor data fusion. The research results can reduce managers' thinking time of security and strengthen network managers' cognition awareness of security. In addition, some researchers applied this into the network security protection of national defense, military and transport management[1,2]. And until the beginning of the 21st century, relevant scholars studied the security situation prediction of large network, and functions of identification, prevention and alarming are produced for stealthy and deliberate hacker attacks[3].

Because of the severe uncertainty and obvious randomness of NSS, Kan Guangyuan builds the sensing model of NSS by using gray prediction model. The principle is to conduct integrated computation on the information entropy to get the predicted value, and calculate the risk index at the same time, so as to reflect the perceptibility of network security situation [4]. For large networks, the commonly used data mining method is to analyze a number of information entropy sequences, summarize the rules, and complete the level classification of NSS by combining with the entropy of existing network attack cases. On the basis of the traditional sensing models, Hu He, et al. propose Markov game model, which can predict network attacks much earlier, and also can judge high-frequency false alarm[5]. In addition, Markov game model is also applicable in the prediction of NSS, which will be further studied in this paper.

This paper first describes the basic principle of Markov model and then the necessary and sufficient conditions for the application of Markov game model. And finally, taking fuzzy comprehensive evaluation model as the theoretical basis, and having agriculture, health care, education and finance as the research objects, this paper analyzes the application fields of the sensing method of NNS with Markov game model from the aspects of network randomness, non-cooperative and dynamic evolution.

II. MARKOV GAME MODEL

Markov game model is the combination product of Markov chain and game theory. In game theory, balance is an important goal. This theory avoids the human impact on event probability. Markov chain shows that situations occurring in the future are only related to the present instead of the past events, indicating the randomness of the event. In the sensing of network security situation, Markov game model can properly express the randomness of security incidents.

Network security issues are the offensive and defensive problems of the network, and the state determination of the attacker and defender is the sensing of network security situation [6,7]. Therefore, a combination series of seven variables is applied as expression quantity,

$$ADSG = (N, S, A, D, P, R, V) \tag{1}$$

where N is the number of personnel participating in attack and defense, and if the number of attackers (or defenders) is larger than two, it is defined as system attack (or defense). However,

in the calculation, they can be combined together, and the number of offensive and defensive sides is both defined as 1. S represents the confrontation situation of both offensive and defensive sides. Different confrontations can be represented by $\{S_1, S_2, \cdots S_k\}$. A represents the aggressive behavior of the attacker. Different attacks are recorded as $\{a_1, a_2, \cdots a_M\}$, and under a confrontation case S_k, aggressive behavior $A_k \subset A$ and $\bigcup_{k=1}^{M} A_k = A$. D represents the defensive behavior of defensive side. Different defensive behaviors are referred to as $\{d_1, d_2, \cdots d_N\}$, and under a confrontation case S_k, defensive behavior $D_k \subset D$ and $\bigcup_{k=1}^{N} D_k = D$. P represents the variation probability of the confrontation situation of the two parties. $P: 0 \le S \times A \times D \times S \le 1$. R represents the earnings of both sides, which can be obtained by the calculation of $S \times A \times D$, denoted as $R_h(s,a,d)$. V acts as the rationality judgment of the behaviors of both sides. The total profit value is used as the objective function, and can be written as

$$V(S,A,D) = R(S,A,D) + \beta \sum_{s'} P(S,A,D,S')V(S') \quad (2)$$

where $\beta \sum_{s'} P(S,A,D,S')V(S')$ represents the future earnings of both sides, and β is the discount rate of future earnings.

Under a confrontation case S_k, the strategies of offensive and defensive sides are recorded as

$$\pi_k^a = \left(\pi_k^a(a_1), \pi_k^a(a_2), \cdots, \pi_k^a(a_i)\right)$$
$$\pi_k^d = \left(\pi_k^d(d_1), \pi_k^d(d_2), \cdots, \pi_k^d(d_j)\right)$$

, and then the necessary and sufficient conditions that the strategies of both sides can be equal probability events are

Any π_i^a can meet $V_a\left(\pi_i^{a^*}, \pi_i^{d^*}\right) \ge V_a\left(\pi_i^a, \pi_i^{d^*}\right)$,
Any π_i^d can meet $V_a\left(\pi_i^{a^*}, \pi_i^{d^*}\right) \ge V_a\left(\pi_i^{a^*}, \pi_i^d\right)$.

In addition to this necessary and sufficient condition, the application of Markov game model requires the randomness, non-cooperative and dynamic evolution of the attack and defense of network. Therefore, the sensing method of NSS with this model cannot be applied in the network security prediction of all fields. In the following section, fuzzy comprehensive evaluation method is applied to evaluate the application field of this sensing method.

III. Fuzzy Comprehensive Evaluation

Suppose there are n factors related to the objects to be evaluated, recorded as $U = \{u_1, u_2, \cdots, u_n\}$, which is called factor set[8]. And suppose there are totally m comments that may appear, recorded as $V = \{v_1, v_2, \cdots, v_m\}$, which is called evaluation set. Because the position of each factor is not the same, their roles are different, and thus measurement standard, namely weight, appears, recorded as $A = \{a_1, a_2, \cdots, a_n\}$.

A. Steps of Comprehensive Evaluation

Steps of fuzzy comprehensive evaluation are listed as follows. [9]

Step1. Set factor set $U = \{u_1, u_2, \cdots, u_n\}$.

Step2. Set evaluation set $V = \{v_1, v_2, \cdots, v_m\}$.

Step3.Conduct single factor evaluation, and obtain $r_i = \{v_{i1}, v_{i2}, \cdots, v_{im}\}$.

Step 4.Construct comprehensive evaluation matrix

$$R = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1m} \\ r_{21} & r_{22} & \cdots & r_{2m} \\ \vdots & \vdots & & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nm} \end{bmatrix}$$

Step5.Construct comprehensive evaluation for weight $A = \{a_1, a_2, \cdots, a_n\}$, and calculate $B = A \circ R$, and make evaluations based on maximum membership principle.

B. Model

Model I: $M(\bullet, +)$ is weighted average type.

The computing method is

$$b_j = \sum_{i=1}^{n} a_i \bullet r_{ij} \left(j = 1,2,\cdots,m\right) \quad (3)$$

This model takes all influencing factors into consideration in accordance with the importance of various factors, which is suitable for the case requiring the optimal comprehensive evaluation.

Model II: $M(\wedge, \oplus)$ is taking small upper bound and type.

$$b_j = \min\left\{\left(1, \sum_{i=1}^{n}\left(a_i \wedge r_{ij}\right)\right)\right\}\left(j = 1,2,\cdots,m\right) \quad (4)$$

In the application of this model, it should be particularly noted that the value of a_i should not be too large, otherwise the situation that all b_j is 1 may occur; the value of a_i should not be too small, otherwise the situation that b_j is equal to the sum of each a_i may occur.

Model I : $M(\wedge, +)$ is average balance type.

The computing method is

$$b_j = \sum_{i=1}^{n}\left(a_i \wedge \frac{r_{ij}}{r_0}\right)\left(j = 1,2,\cdots,m\right) \quad (5)$$

$r_0 = \sum_{k=1}^{n} r_{kj}$.

The model established in this paper uses the operator of determining type of principal factor.

C. Evaluation Case

By considering network security issues of different fields, factor set $U=\{u_1,u_2,u_3\}$ is established, in which u_1 represents randomness, u_2 represents non-cooperative, and u_3 represents dynamic evolution. Evaluation set $V=\{v_1,v_2,\cdots,v_m\}$ is established, in which v_1 represents agriculture, v_2 represents health care, v_3 represents education, and v_4 represents finance.

50 network security experts are randomly selected to evaluate the three characteristics of four industries (full mark: 100). Meanwhile, the impact of the three characteristics on the results is investigated, and the evaluation results can be obtained after dealing with the survey results, which are shown in Figure 1 and Figure 2.

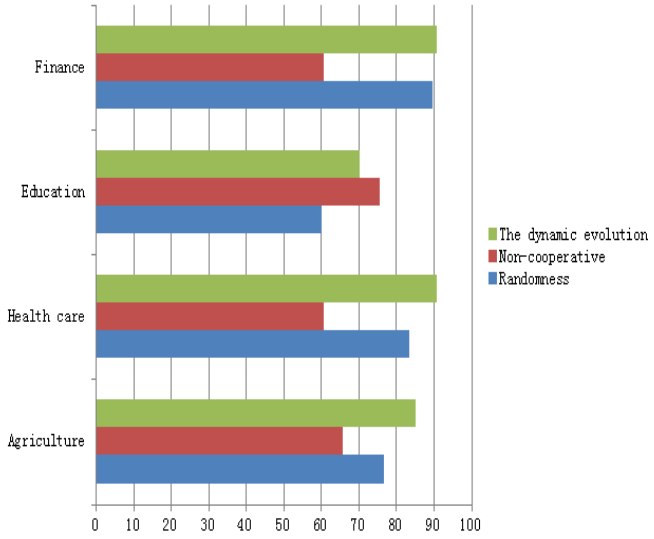


Figure 1. Industry characteristics indicators

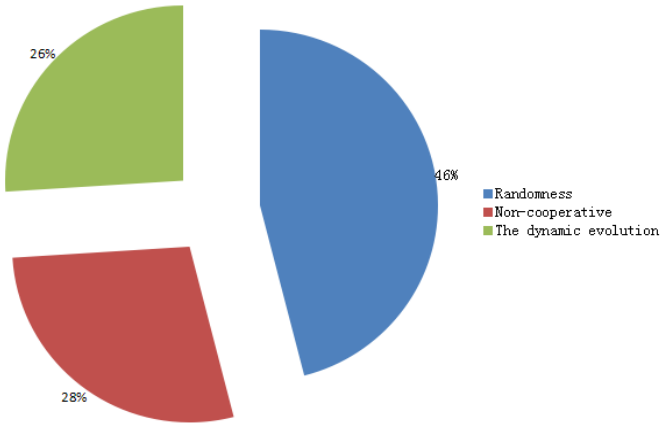


Figure 2. The importance of characteristics indicators

According to the data in Figure 1, comprehensive evaluation matrix R is established.

$$R=\begin{bmatrix}0.2477 & 0.2693 & 0.1941 & 0.2889\\ 0.2503 & 0.2309 & 0.2876 & 0.2313\\ 0.2527 & 0.2693 & 0.2088 & 0.2693\end{bmatrix}$$

It can be known from Figure 2 that the evaluation weight is $A=(0.46,0.28,0.26)$. Based on Model I——$M(\wedge,\vee)$, respectively calculate the two weights, and obtain

$$B=A\circ R=(0.2527,0.2693,0.28,0.2889)$$

Calculation results show that the sensing method of NSS with Markov game model is best for financial field, followed by educational field.

IV. Test and Discussion

In summary, the NSS prediction model in this paper is shown in Figure 3.

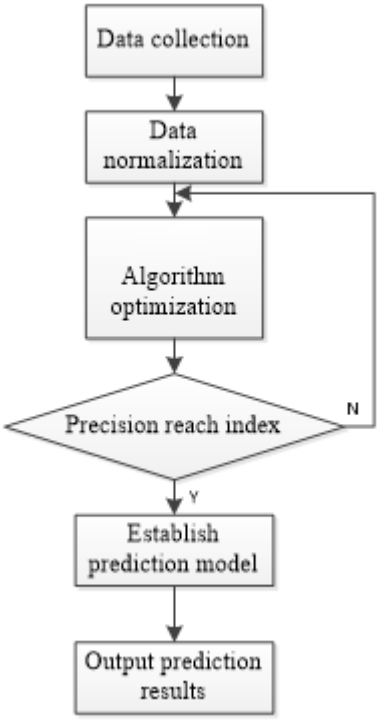
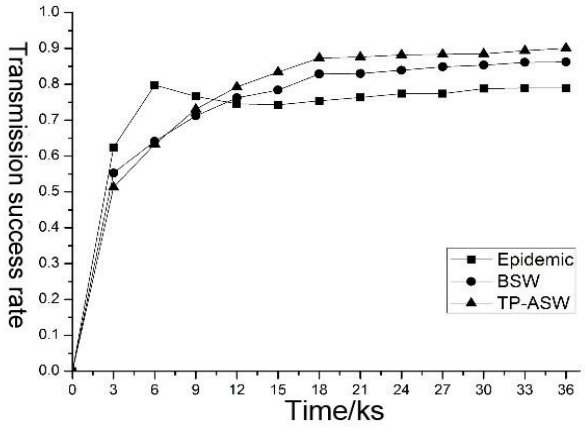
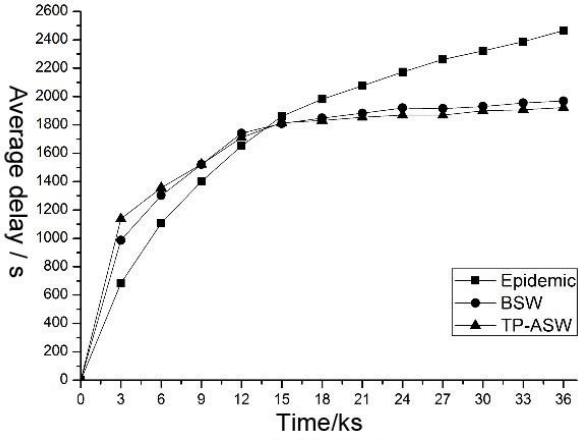


Figure 3. Network security situation prediction model process

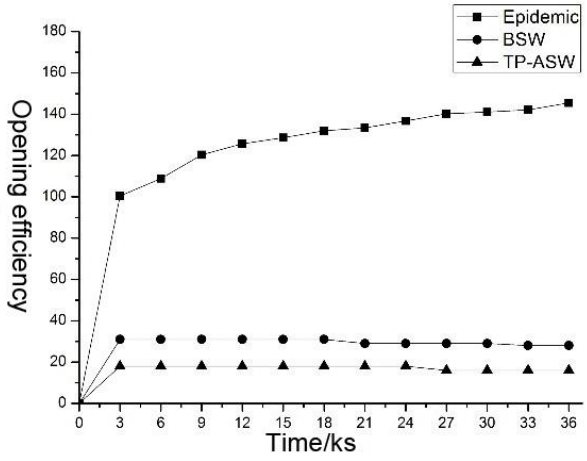
The method of the paper is compared with the block feature detection method and the fuzzy access method. TP-ASW is the method of the paper, Epidemic is the block feature detection method, and BSW is the fuzzy access method. The comparison result is obtained, as shown in Fig. 4.



(a) Transmission success rate



(b) Average delay



(c) Overhead rate

Figure 4. The performance test comparison

Compare the prediction results of the three methods, as shown in Figure 5.

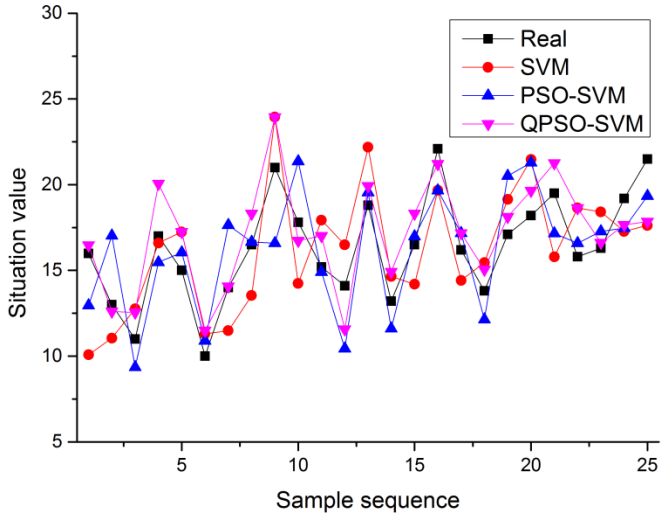


Figure 5. Comparison of prediction results

The error comparison is shown in Figure 6. It can be seen from Figure 6 that the error of this method is lower than that of PSO-SVM at most sample points.

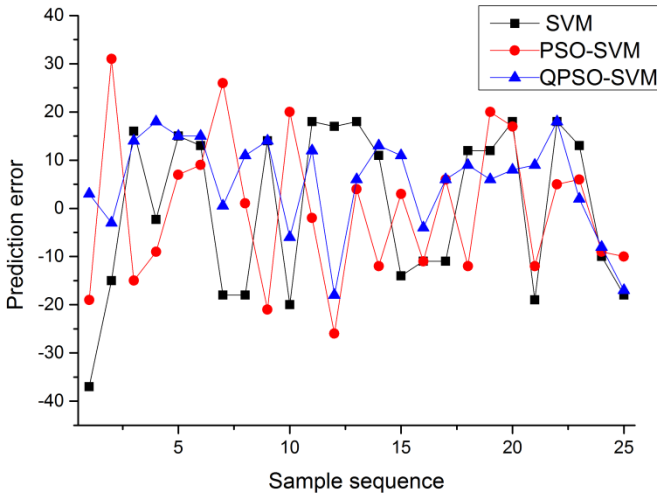


Figure 6. Prediction error contrast

In order to compare the results of these methods more clearly, the evaluation criteria of the four methods are given. The comparison results are shown in Table 1. It can be seen from the table that all indexes of the method proposed in this paper are higher than SVM, QPSO-SVM and PSO-SVM methods.

Table 1. Error comparison of four model prediction indexes

Prediction Model	Max error	Min error	Mean error
SVM	42.8%	2.31%	15.53%
PSO-SVM	32.1%	1.05%	12.52%
QPSO-SVM	18.9%	0.52%	9.86%
Markov game			

V. Conclusion

This paper evaluates the application situation of the sensing method of NSS with Markov game model in the fields of agriculture, health care, education and finance by using fuzzy comprehensive evaluation method. It can be obtained from the calculation results and the actual situation that the model established in this paper can accurately evaluate the applicability of this sensing method in the four fields. In addition, the model can also be used in the applicability evaluation of the sensing methods of different industries' network security situation. Certainly, in different categories, and under the premise of different sensing methods of network security situation, the proportions of various influencing factors are different, and once the proportion is unreasonable, it will cause false calculation process and thus affect the results. Therefore, it is necessary to re-set the proportion of each item. Evaluation results show that the sensing method of NSS with Markov game model is best for financial field, followed by educational field.

Although the redundant data is eliminated and the data processing efficiency is improved, the research on data continuity is not deep enough. In the future research process, we should strengthen the continuity research in information security situation prediction.

References

[1] Xing J , Zhang Z . Prediction model of network security situation based on genetic algorithm and support vector machine. *Journal of Intelligent and Fuzzy Systems*, 2021(3):1-9.

[2] D Zhao, Song H , Li H . Fuzzy integrated rough set theory situation feature extraction of network security. *Journal of Intelligent and Fuzzy Systems*, 2021, 40(1):1-12.

[3] Yang H , Zeng R , Xu G , et al. A network security situation assessment method based on adversarial deep learning. *Applied Soft Computing*, 2021, 102(8):107096.

[4] Zhu Y , Du Z . Research on the Key Technologies of Network Security-Oriented Situation Prediction. *Scientific Programming*, 2021, 2021:1-10.

[5] Zhan K . Design of computer network security defense system based on artificial intelligence and neural network. *Journal of Intelligent and Fuzzy Systems*, 2021(9):1-13.

[6] Du Z . Network Security Model Based on Active and Passive Defense Hybrid Strategy. *Converter*, 2021:45-51.

[7] Wang C , Zhao Z , Wang F , et al. A Novel Malware Detection and Family Classification Scheme for IoT Based on DEAM and DenseNet. *Security and Communication Networks*, 2021, 2021(11):1-16.

[8] Andreatos A . Redesigning Engineering Assessment during the Covid-19 Lockdown. A case study in Computer Networking and Network Security. *Technium Social Sciences Journal*, 2021, 15,pp.2582-2589.

[9] Zhao Y , Huang L , Smidts C , et al. Finite-horizon Semi-Markov Game for Time-sensitive Attack Response and Probabilistic Risk Assessment in Nuclear Power Plants. Reliability Engineering. *System Safety*, 2020, 201:106878..

[10] Gwa B , Gt A , Jd B , et al. Distributed Reinforcement Learning Algorithm of Operator Service Slice Competition Prediction Based on Zero-Sum Markov Game - ScienceDirect. *Neurocomputing*, 2021., vol. 6, no. 6, pp.7824-7829.

[11] Mohit Borthakur, Anagha Latne, and Pooja Kulkarni, "A comparative study of automated PCB defect detection algorithms and to propose an optimal approach to improve the technique," *International Journal of Computer Applications*, vol. 114, no. 6, pp.27-33, 2015.

[12] R Alsaleh, Sayed T . Markov-game modeling of cyclist-pedestrian interactions in shared spaces: A multi-agent adversarial inverse reinforcement learning approach. *Transportation Research Part C Emerging Technologies*, 2021, 128(2), pp.426-432.

[13] S. Sridevi, G. Muralidharan, and C. Nandha kumar, "Online inspection of printed circuit board using machine vision," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 3, no. 3, pp.230-238, 2014.

[14] Bahrami M , Toghraee M , Heidarian A . Heart Attack Detection in Internet of Things: Modeling with Health Markov Game Theory. *CiiT International Journal of Biometrics and Bioinformatics*, 2020, 12(2):25-30.

[15] Sharat Chandra Bhardwaj, "machine vision algorithm for PCB parame ters inspection" in *National Conference on Future Aspects of Artificial intelligence in Industrial Automation,* 2012, pp.20-24.

[16] Chen G H, Hua-Jie L I, Fang X W. "Research of the Vision Positioning System of Surface Mounting Machine Based on Phase Congruence and Hough Circle Transform". *Science Technology & Engineering*, vol.27, no.11, pp.59-63, 2015.

[17] Salih Burak Göktürk, Lale Akarun, H. Isil Bozma. "Automated inspection of PCB's using a novel approach" In *Processing of IEEE-Eurasip Workshop on Nonlinear Signal and Image. DBLP*, Antalya , 1995, pp.180-184.

[18] Salah Bourennane, Caroline Fossati, Robust Denoising Method based on Tensor Models Decomposition for Hyperspectral Imagery, *WSEAS Transactions on Signal Processing*, Volume 15, 2019, Art. #4, pp. 20-29.

[19] Rafeek Mamdouh, Hazem M. El-Bakry, Alaa Riad, Nashaat El-Khamisy, Converting 2D-Medical Image Files "DICOM" into 3D- Models, based on Image Processing, and Analysing their Results with Python Programming, *WSEAS Transactions on Computers*, Volume 19, 2020, Art. #2, pp. 10-20.

Bingjie Lin, graduated from Peking University with a master's degree in Electronics and Communication Engineering in 2019, is currently working in State Grid Information & Communication Branch as the Security Analysis specialist of the Network Security Monitoring Center. Her main research directions is Information Security.

Jie Cheng, graduated from Beijing University of Posts and Telecommunications (BUPT) with a master's degree in Computer Technology and Application in 2007, is currently working in State Grid Information & Communication Branch as a senior engineer of the Network Security Monitoring Center. His main research directions is Information Security.

Jiahui Wei, graduated from North China Electric Power University with a master's degree in Computer Application Technology in 2018, is currently working in State Grid Information & Communication Branch as the Security Analysis specialist of the Security Monitoring Division of the Network Security Monitoring Center. His main research directions is Information Security.

Ang Xia, graduated from North China Electric Power University with a master's degree in Information and Communication Engineering in 2020, is currently working in State Grid Information & Telecommunication Branch as the assistant of the Internet Security Monitoring Center. Her main research directions are network information security and theory of information and communication.