Research on Network Security Risk Assessment Method Based on Improved Analytic Hierarchy Process

Gang Wang
(Corresponding author: Gang Wang)
Shaanxi Police College, China
No. 1, Qiyuan 2nd Road, Weiyang District, Xi'an, Shaanxi 710021, China
Email: gwiays@126.com
(Received Mar. 29, 2019; Revised and Accepted July 13, 2020; First Online Apr. 25, 2021)

Abstract

Risk assessment can help understand network security. This paper mainly analyzed the analytic hierarchy process (AHP) method, improved the AHP method with the fuzzy operator, applied the improved AHP method to risk assessment, and took a local network as an example to evaluate its network security risk. The results showed that the probability of low risk in the network was the highest, 28%. Among the indicators established, the more important ones were transmission relay failure, software, and hardware failure, no data backup, *etc.*. The above aspects should be strengthened in the network security construction. The experimental analysis results verify the effectiveness of the improved AHP method in risk assessment, which provides some reliable bases for the formulation of defense strategy.

Keywords: Analytic Hierarchy Process; Fuzzy Operator; Network Security; Risk Evaluation

1 Introduction

With the popularity of the Internet [8], it plays a more and more important role in people's life and work and provides great convenience to many fields, such as politics, economy, entertainment, *etc.* [2]; however, the issue of network security is also becoming more prominent: the number of spam mails increases rapidly, harmful information spreads faster, and the attack means of hackers also becomes more complex and diversified [10]. The increasing network security incidents have brought a great threat to society and the economy, and the network security issues have been paid more attention to by researchers [5, 7, 15, 20].

Risk assessment can help managers understand the current and future risks of the network [1] and provide some reliable bases for establishing defense strategies, which are more conducive to the safe operation of the network. The method of risk assessment has also been widely concerned by researchers [14]. Xu *et al.* [22] designed a method based on non-cooperative differential game theory, which regarded the process of risk assessment as a differential game of optimal resource control. The experiment found that the method was feasible. Deng *et al.* [4] proposed a method based on the rough set and gene expression program to mine security risks and predicted and analyzed risk levels. The experiment showed that the method had a high mining efficiency and strong practicability.

Wang *et al.* [21] improved the factor analysis of information risk (FAIR) with the Bayesian network and obtained a FAIR-BN model. The experiment showed that the model was more accurate, flexible and extensible, and had the potential to provide solutions for decision-making. Based on the network penetration test, Sun *et al.* [19] generated an attack graph, calculated the attack probability of the atomic node, used the Markov chain to calculate the attack transition probability, and selected the best attack path to realize the evaluation of network security risks. The simulation results showed that the method could make an objective response to the actual situation of the network. Based on the analytic hierarchy process (AHP) and fuzzy operator, this paper designed an improved AHP method, applied it to risk assessment, and made an experimental analysis to understand the reliability of the method. This paper makes some contributions to the better realization of network security.

2 Risk Assessment Method

At present, the commonly used risk assessment methods can be divided into four types.

1) Qualitative analysis method: Based on the work experience and theoretical knowledge of the assessors, the risk level is divided according to some evaluation standards and similar cases in the past. However, this method generally has strong personal subjectiv-

ity. The specific methods include the historical comparison method, expert evaluation method [25], *etc.*

2) Quantitative analysis method: Risk factors were represented by specific values. With strong objectivity, this method can help people to observe and analyze the evaluation results clearly. The specific methods include fuzzy comprehensive evaluation method [24], back-propagation (BP) neural network [23], grey model [3], *etc.*

3) Qualitative and quantitative analysis combined method: The quantitative method is applied for quantifying the risk factors that can be quantified, and the qualitative method is used for analyzing the factors that cannot be quantified. The combination can more comprehensively describe the whole evaluation process.

4) Model evaluation method: The method evaluates the whole system with the model analysis tool. This method can find out the unknown vulnerable points and the security risks in the system. The specific methods are information flow model, fault tree model [17], graph model [13], *etc.*

The risk of network security involves software, hardware, environment, *etc.* [6], which is generally analyzed from three aspects. The first aspect is assets. Assets refer to valuable information, data, and resources, and risk assessment is related to the importance of assets. The second aspect is threats. Threats refer to the possibility of causing negative impacts on assets based on weakness, for example, threats from viruses and hackers. Risk assessment is related to the possibility of threats. The third aspect is vulnerabilities. Vulnerabilities refer to the weak links of assets that may be threatened, such as the deficiency of network software, hardware and defense measures. Once the deficiencies are used, assets will be damaged. Risk assessment is related to the severity of vulnerabilities.

3 Improved AHP Method

3.1 Basic Principle of AHP

AHP is a multi-criteria decision-making method [16]. In the risk assessment of network security, many factors are difficult to quantify; therefore, it is necessary to adopt appropriate methods to evaluate the importance of these factors to realize the assessment of network risk. There are four steps in AHP.

1) Building a hierarchical structure model:
Building a model aims to analyze the risk problem in detail. Generally speaking, the model includes three layers, as shown in Figure 1. The target layer has only one element, which is the predetermined goal of the problem. The criterion layer refers to a series of intermediate links involved in achieving the goal. The scheme layer is the optional scheme and measures needed to achieve the goal.

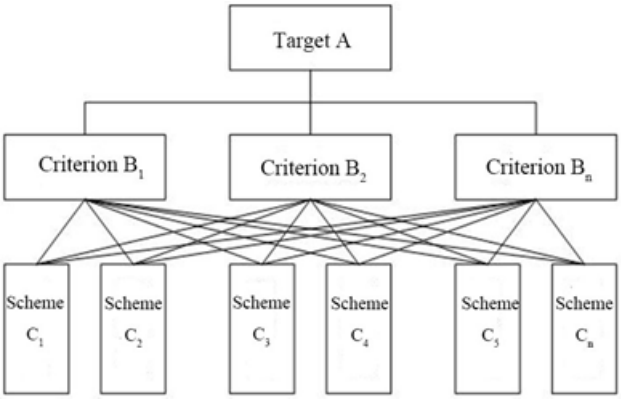

Figure 1: A hierarchical structure model

2) Establishing a judgment matrix:
AHP requires to calculate the relative importance of different factors layer by layer and quantify it into a judgment matrix. For example, scheme B is associated with criterion A of the last layer. The judgment matrix can be written as:

$$A\_B = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{bmatrix}$$

where b_{ij} is the importance of b_i and b_j relative to A. AHP adopts the Saaty1-9 scale to quantitatively describe the value, as shown in Table 1. The value can be obtained through the Delphi method.

3) Calculating single hierarchical arrangement:
Firstly, all the elements are normalized; then, they were added up according to the row, and $\bar{w_i} = \sum_{i=1}^{n} \bar{b_{ij}}$ is obtained, where $\bar{w_i}$ refers to the feature vector of the matrix and $\bar{b_{ij}}$ is the element obtained after normalization. $\bar{w_i}$ is normalized again, and weight $w_i = \frac{\bar{w_i}}{\sum_{j=1}^{n} \bar{w_i}}$ is obtained. The weight of every layer is calculated; then, the result of a single hierarchical arrangement is obtained. However, in the actual calculation process, there may be some inconsistency in the matrix; thus, it is necessary to check the consistency of the matrix after the calculation.

Firstly, a consistency test index (CI) is established, $CI = \frac{\lambda_{\max} - n}{n-1}$, where $\lambda_{\max}$ refers to the maximum feature value of the matrix. $CR = \frac{CI}{RI}$ is calculated, where RI refers to the average random consistency index. The values given by Satty are shown in Table 2. If the calculated result is $CR \leq 0.1$, the matrix has consistency; otherwise, the matrix needs correction.

Table 1: The Saaty1-9 scaling method

Importance scale	Explanation
1	b_i is no less important than b_j
3	b_i is a little important than b_j
5	b_i is significantly more important than b_j
7	b_i is strongly more important than b_j
9	b_i is extremely more important than b_j
2, 4, 6, 8	The median values of the above judgment
Reciprocal	The ratio of the importance of b_j to the importance of b_i is $b_{ji} = \frac{1}{b_{ij}}$

Table 2: Comparison table of consistency check

Matrix Order	RI
1	0
2	0
3	0.58
4	0.90
5	1.12
6	1.24
7	1.32
8	1.41
9	1.45

4) Calculating total hierarchical arrangement:
After calculating the single hierarchical arrangement and performing a consistency test on the matrix of each layer, all the factors of every layer are calculated. Based on the combined weight of the target layer, the total hierarchical arrangement is performed.

3.2 Improved AHP

AHP can not directly estimate the risk level. This paper improves AHP with the fuzzy operator. In the risk assessment, the risk is divided into five levels, namely very low (VL), low (L), medium (M), high (H), and very high (VH). The membership of different indicators is represented by the Gaussian membership function, and the formula is as follows:

$$\begin{aligned} f_{VL}(x) &= e^{-\frac{x^2}{2\times 0.1^2}} \\ f_L(x) &= e^{-\frac{(x-0.25)^2}{2\times 0.1^2}} \\ f_M(x) &= e^{-\frac{(x-0.5)^2}{2\times 0.1^2}} \\ f_H(x) &= e^{-\frac{(x-0.75)^2}{2\times 0.1^2}} \\ f_{VH}(x) &= e^{-\frac{(x-1)^2}{2\times 0.1^2}} \end{aligned}$$

Then, the membership matrix of the criterion layer can be written as:

$$R = \begin{bmatrix} f_{VL}(x_1) & f_L(x_1) & f_M(x_1) & f_H(x_1) & f_{VH}(x_1) \\ f_{VL}(x_n) & f_L(x_n) & f_M(x_n) & f_H(x_n) & f_{VH}(x_n) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ f_{VL}(x_m) & f_L(x_m) & f_M(x_m) & f_H(x_m) & f_{VH}(x_m) \end{bmatrix}$$

According to the criterion layer weight W_i and matrix R_i, a fuzzy evaluation matrix is obtained:

$$D_i = W_i \times R_i$$

According to the level one fuzzy comprehensive evaluation matrix and based on the target layer weight W, a level two membership matrix is established, written as:

$$\begin{aligned} S &= \begin{bmatrix} S_1 \\ S_2 \\ \vdots \\ S_n \end{bmatrix} \\ &= \begin{bmatrix} W_1 \times D_1 \\ W_2 \times D_2 \\ \vdots \\ W_n \times D_n \end{bmatrix} \end{aligned}$$

The level two fuzzy comprehensive evaluation matrix of the target layer can be written as:

$$A = W \times S,$$

i.e., the final risk level.

4 Experimental Analysis

Taking a local network as an example, the improved AHP was applied to the risk assessment of network security. The risk level has five levels, and the division is shown in Table 3.

First of all, the corresponding hierarchical structure model needed to be established. Considering the assets, threats, and vulnerabilities of the network, the corresponding scheme layer indicators were determined. A total of 15 indicators were determined. The established model is shown in Table 4.

Table 3: Risk classification

Value-at-risk	0-0.2	0.2-0.4	0.4-0.6	0.6-0.8	0.8-1
Level	VL	L	M	H	VH

Five network security experts were invited to determine the weight. First, the judgment matrix of the criterion layer relative to the target layer was established by the 1-9 scaling method, as shown in Table 5.

According to Table 5,

$$A\_B = \begin{bmatrix} 1 & 1/3 & 5 \\ 3 & 1 & 7 \\ 1/5 & 1/7 & 1 \end{bmatrix}$$

Through calculation, the maximum feature value $\lambda_{\max}$ of the matrix is 3.06, and the RI value is 0.52; then, its consistency indicator is:

$$CR = \frac{CI}{RI} = \frac{3.06 - 3}{3 - 1} = 0.03 < 0.1,$$

which shows that the obtained matrix satisfies the consistency. After normalization, the weight of each layer is obtained:

$$\begin{aligned} C_1 &= 0.28 \\ C_2 &= 0.65 \\ C_3 &= 0.07 \end{aligned}$$

, , . The weight of each layer is calculated one by one using the same method. After the consistency test, the final results are shown in Table 6.

It was seen from Table 6 that the weight of threat was the largest in the criterion layer, followed by asset and vulnerability, which indicated threat brought the greatest risk in the network and was the most important in risk assessment. Among the indicators of the scheme layer, in addition to the three indicators related to assets, the indicators with higher weight were C6 (transmission relay failure), C11 (no data backup), and C12 (no relay link protection), which indicated that these indicators had important impacts on the risk in the risk assessment.

Then, the experts evaluated the indicators and took the average values. The results are shown in Table 7.

According to Table 7, based on the level one fuzzy comprehensive evaluation, the evaluation results of different risk factors are obtained:

$$\begin{aligned} B_1 &= (0.15\ 0.22\ 0.15\ 0.31\ 0.07) \\ B_2 &= (0.17\ 0.32\ 0.21\ 0.08\ 0.01) \\ B_3 &= (0.17\ 0.21\ 0.22\ 0.09\ 0.04) \end{aligned}$$

On this basis, the total fuzzy evaluation results are calculated. Finally, the risk evaluation result of the network is:

$$A = [0.17\ 0.28\ 0.15\ 0.08\ 0.02].$$

The probability of risks in this network is shown in Figure 2.

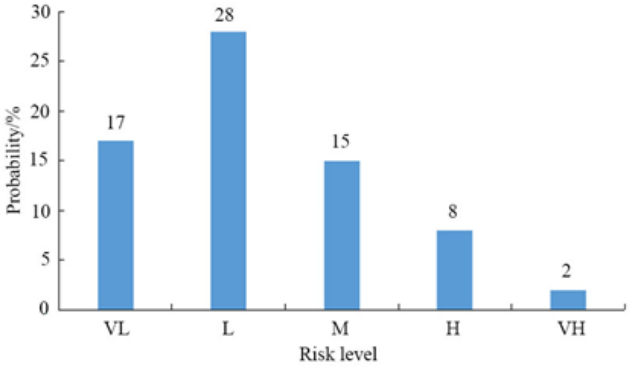

Figure 2: Network security risk level

As shown in Figure 2, the probability of the very low risk in the local network was 17%, the probability of the low risk was 28%, the probability of the medium risk was 15%, the probability of the high risk was 8%, and the probability of the very high risk was 2%. Overall, the probability of the low risk in the network was the highest, but there was also the possibility of the high risk. Therefore, it is necessary to strengthen the protection of the network and realize the safe operation of the network through technologies such as intrusion detection.

5 Discussion

Network security refers to protecting network hardware, software, and information data from being damaged or leaked due to unexpected and malicious factors to ensure uninterrupted network service. For network security, many technologies and methods have been applied, such as firewall [18], intrusion detection [9], situation awareness [11], data encryption [12], *etc.* However, before arranging these methods, the security risk of the network needs to be evaluated first to understand the security situation of the network better and make a reasonable arrangement.

In this study, the AHP method was improved to make it have a good application in the network security risk assessment. An experiment analysis was carried out by taking a local network as an example. The evaluation results of the improved AHP method showed that the network assets had an important impact on the network security, and the probability of the high risk in assets was highest, 31%, and the weight was 0.28. The above results showed that the protection of assets was a very important part of network security. From the perspective of threat, it was found that the most important threat was transmission relay failure. In the local network, its transmission depended on the transmission network. However, due to the mismatch of optical power, the transmission process

Table 4: The hierarchical structure model

Target layer	Criterion layer	Scheme layer
Network security risk assessment index system A	Asset B1	Deliberate theft C1
		Deliberately tamper with C2
		File missing C3
	Threat B2	Hardware and software failure C4
		Operation failure C5
		Transmission relay fault C6
		Malicious code C7
		Hacker attacks C8
	Vulnerability B3	Equipment aging C9
		Unprotected core disk C10
		No dada backup C11
		No relay link protection C12
		Insufficient anti-virus measures C13
		Insufficient anti-attack capability C14
		Multiple links are connected by C15

Table 5: The judgment matrix of level one indicators

	B1	B2	B3
B1	1	1/3	5
B2	3	1	7
B3	1/5	1/7	1

Table 6: Determination of indicator weight

Criterion layer	Weight	Scheme layer	Weight
B1	0.28	C1	0.33
		C2	0.33
		C3	0.33
B2	0.65	C4	0.22
		C5	0.16
		C6	0.32
		C7	0.15
		C8	0.15
B3	0.07	C9	0.11
		C10	0.09
		C11	0.27
		C12	0.25
		C13	0.05
		C14	0.05
		C15	0.18

Table 7: Expert risk assessment results

Scheme Layers	Assessment Results				
	VL	L	M	H	VH
C1	0.12	0.24	0.57	0.05	0.02
C2	0.33	0.25	0.31	0.07	0.04
C3	0.18	0.21	0.41	0.1	0.1
C4	0.22	0.44	0.21	0.08	0.05
C5	0.23	0.31	0.23	0.15	0.08
C6	0.05	0.2	0.2	0.55	0
C7	0.26	0.25	0.27	0.15	0.07
C8	0.31	0.27	0.25	0.09	0.08
C9	0.22	0.26	0.24	0.18	0.1
C10	0.07	0.45	0.21	0.21	0.06
C11	0.05	0.12	0.11	0.67	0.05
C12	0.08	0.11	0.05	0.48	0.28
C13	0.21	0.23	0.22	0.21	0.13
C14	0.22	0.21	0.25	0.18	0.14
C15	0.23	0.21	0.24	0.15	0.17

might be interrupted frequently. Also, with the development of urban construction, the growth of construction engineering has aggregated artificial cutting, which led to frequent transmission failures. Another threat with high weight was hardware and software failure; therefore, in the construction of network security, it is necessary to replace the damaged equipment in time and increase the maintenance and management of network equipment to reduce such risks.

Overall, for network threats, the probability of the low risk was the highest, 32%. Finally, from the perspective of vulnerability, it mainly showed the possibility of the medium risk, 22%. The relatively important vulnerabilities are "no data backup" and "no relay link protection". Therefore, it is necessary to strengthen the management of these two items, i.e., setting up a good protection link for the relay link in the network and strengthen the data backup, to reduce the security risk of the network. On the whole, the overall risk of the local network studied was low. According to the results of risk evaluation, the proposed network security measures include:

1) Reducing the human-made cable damage to avoid transmission relay failure;

2) Strengthening the backup of important data;

3) Improving the ability to prevent viruses and attacks and deploying the corresponding firewall and intrusion detection system.

In this study, although some achievements have been made in the research of network security risk assessment, there are still some shortcomings, which need to be solved in future workd. For example, the division of risk hierarchy should be divided in more detail to more comprehensively describe the security risk of the network; the AHP method should be further optimized to reduce the subjectivity of expert evaluation; the correctness of the method should be verified in more data sets.

6 Conclusion

Aiming at the risk assessment of network security, this study designed an improved AHP method and applied it to a local network. Through an evaluation by the improved AHP method, it was found that the probability of the low risk in the network was high, 28%, followed by the very low risk, 17%. Then, according to the risk of the network, the network security measures were discussed. The results show that the improved AHP method has a good performance in risk assessment and can be further promoted and applied in practice.

References

[1] O. O. Abimbola, B. Akinyemi, T. Aladesanmi, G. A. Aderounmu, K. B. Hamidja, "An improved stochastic model for cybersecurity risk assessment," *Computer and Information Science*, vol. 12, no. 4, pp. 96, 2019.

[2] N. Athavale, S. Deshpande, V. Chaudhary, J. Chavan, S. S. Barde, "Framework for threat analysis and attack modelling of network security protocols," *International Journal of Synthetic Emotions*, vol. 8, no. 2, pp. 62-75, 2017.

[3] J. Chen, Z. Zhou, Y. Tang, Y. He, S. Zhao, "Research on network security risk assessment model based on grey language variables," in *IOP Conference Series: Materials Science and Engineering*, vol. 677, no. 4, pp. 042074, 2019.

[4] S. Deng, D. Yue, X. Fu, A. Zhou, "Security risk assessment of cyber physical power system based on rough set and gene expression programming," *IEEE/CAA Journal of Automatica Sinica*, vol. 2, no. 4, pp. 431-439, 2015.

[5] A. Dewanje and K. A. Kumar, "A new malware detection model using emerging machine learning algorithms," *International Journal of Electronics and Information Engineering*, vol. 13, no. 1, pp. 24–32, 2021.

[6] D. Henshel, M. G. Cains, B. Hoffman, T. Kelley, "Trust as a human factor in holistic cyber security risk assessment," *Procedia Manufacturing*, vol. 3, pp. 1117-1124, 2015.

[7] S. Islam, H. Ali, A. Habib, N. Nobi, M. Alam, and D. Hossain, "Threat minimization by design and deployment of secured networking model," *International Journal of Electronics and Information Engineering*, vol. 8, no. 2, pp. 135–144, 2018.

[8] A. Kak, "Computer and network security," *Friend of Science Amateurs*, vol. 31, no. 9, pp. 785-786, 2017.

[9] M. J. Kang, J. W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *Plos One*, vol. 11, no. 6, pp. e0155781, 2016.

[10] Z. M. King, D. S. Henshel, F. Liberty, L. Flora, M. G. Cains, B. Hoffman, C. Sample, "Characterizing and measuring maliciousness for cybersecurity risk assessment," *Frontiers in Psychology*, vol. 9, 2018.

[11] Y. B. Leau, A. A. Khudher, S. Manickam, S. Al-Salem, "An adaptive assessment and prediction mechanism in network security situation awareness," *Journal of Computer Science*, vol. 13, no. 5, pp. 114-129, 2017.

[12] J. Li, "A symmetric cryptography algorithm in wireless sensor network security," *International Journal of Online Engineering*, vol. 13, no. 11, pp. 102, 2017.

[13] S. Liu, Y. Liu, "Network security risk assessment method based on HMM and attack graph model," in *17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD'16)*, Shanghai, pp. 517-522, 2016.

[14] T. Ncubukezi, "A Proposed: Integration of the monte carlo model and the bayes network to propose cyber security risk assessment tool for small

and medium enterprises in South Africa," *International Journal of Computer Science and Information Security*, vol. 3, no. 18, pp. 152-155, 2020.

[15] E. U. Opara, O. A. Soluade, "Straddling the next cyber frontier: The empirical analysis on network security, exploits, and vulnerabilities," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 10–18, 2015.

[16] A. A. Salo, R. P. Hämäläinen, "On the measurement of preferences in the analytic hierarchy process," *Journal of Multi-Criteria Decision Analysis*, vol. 6, no. 6, pp. 309-319, 2015.

[17] M. Sarbayev, M. Yang, H. Wang, "Risk assessment of process systems by mapping fault tree into artificial neural network," *Journal of Loss Prevention in the Process Industries*, vol. 60, pp. 203-212, 2019.

[18] X. Song, "Firewall technology in computer network security in 5G environment," *Journal of Physics Conference Series*, vol. 1544, pp. 012090, 2020.

[19] F. Sun, J. Pi, J. Lv, T. Cao, "Network Security risk assessment system based on attack graph and Markov chain," *Journal of Physics Conference Series*, vol. 910, pp. 012005, 2017.

[20] A. Tayal, N. Mishra and S. Sharma, "Active monitoring & postmortem forensic analysis of network threats: A survey," *International Journal of Electronics and Information Engineering*, vol. 6, no. 1, pp. 49–59, 2017.

[21] J. Wang, M. Neil, N. Fenton, "A bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model," *Computers & Security*, vol. 89, pp. 101659, 2019.

[22] H. T. Xu, R. J. Lin, "Resource allocation for network security risk assessment: A non-cooperative differential game based approach," *China Communications*, vol. 04, no. v.13, pp. 136-140, 2016.

[23] Z. Xu, J. Li, S. Xiao, Y. Yuan, "Study on security risk assessment of power system based on BP neural network," *Journal of Computational and Theoretical Nanoscience*, vol. 13, no. 8, pp. 5277-5280, 2016.

[24] B. Yi, Y. P. Cao, Y. Song, "Network security risk assessment model based on fuzzy theory," *Journal of Intelligent and Fuzzy Systems*, vol. 38, no. 4, pp. 3921-3928, 2020.

[25] A. Youssef, "A delphi-based security risk assessment model for cloud computing in enterprises," *Journal of Theoretical and Applied Information Technology*, vol. 98, no. 1, pp. 151-162, 2020.

Biography

Wang Gang, born on Oct 8,1976, holds a master's degree and is an associate professor of shaanxi police college. He is interested in network security and big data.