Research Article

Link Security Situation Identification Method Based on the Ad Hoc Network of Medical Units

Yifu Zeng,1 Qingquan Chen,2 Ling Yao,3 Jiajing Zhuang,3 Zhixuan Huang,1 Shuhan Huang,4 Honghua Zeng,1 and Riguang Zhong5

1The Second Affiliated Hospital of Fujian Medical University, China
2The School of Public Health, Fujian Medical University, China
3The School of Clinical Medicine, Fujian Medical University, China
4Zhongshan College of Dalian Medical University, China
5AngeLong (Fujian) Medical Technology Co., Ltd., China

Correspondence should be addressed to Honghua Zeng; zyf@fyey.cn and Riguang Zhong; carebeing@outlook.com

Received 14 February 2022; Revised 4 March 2022; Accepted 26 March 2022; Published 6 May 2022

1. Introduction

In recent years, the informatization of medical institutions has become a general trend. On the one hand, it is the rapid development of Internet medical treatment, and on the other hand, the informatization and standardization of medical procedures are strengthened. Informatization not only effectively improves the work efficiency of medical units and meets the needs of patients for medical treatment but also lays a good foundation for the sustainable development of units. At the same time, information construction and development are also facing many network security problems, including patients’ personal privacy information being stolen and external hackers invading the internal network. Traditional medical units have very weak intention of Intranet security construction, and patient information is more likely to be used illegally and cause great losses. Therefore, the network security identification and monitoring of the internal self-organizing network in medical units have become part of the research hotspots.

A network link security situation awareness method based on the Radial Basis Function (RBF) neural network was proposed [1]. The neural network model is optimized by a hybrid hierarchical genetic method to improve global search ability and realize security situation awareness. A fuzzy reasoning method was proposed [2] to realize automatic identification of security situation and deduces link attack correlation and risk.

The above methods lay a good foundation for the research of network link situation security identification
but also have some shortcomings. For example, the data source is single, and there is no quantitative processing of the identification results, so the results obtained are not intuitive. In view of the above defects, this paper uses set pair analysis theory to identify the network link security situation. Set pair analysis is an algorithm dealing with the quantitative similarity and difference of uncertain systems [3], in which set pair represents a set of correspondence between two sets which have some relation. The idea of situation identification by this method is to analyze the system composed of set pair [4], find out the expression of connection number and the calculation method of identity and difference, and analyze the set pair situation, so as to obtain the security situation of the network link [5]. Because this method can deal with the uncertainty caused by fuzzy, random, and incomplete information, it is especially suitable for the security situation identification of the internal network of medical units.

2. Analysis on the Structure and Characteristics of the Ad Hoc Network in Medical Units

In traditional data center construction, there are usually three layers of network structure, which are called access layer, aggregation layer, and core layer. As shown in Figure 1, the access layer switches generally connect to servers and aggregation layer switches connect to access layer switches and generally provide other services, such as firewalls, IPS, and WAF. Generally, the aggregation layer is the demarcation point between L2 and L3. The L2 network
is below the aggregation switch, and the L3 network is above the aggregation switch. Core layer switches generally provide high-speed forwarding of packets in and out of the data center and simultaneous forwarding of communications between multiple aggregation switches in the data center.

In this system, the physical layer uses the transmission medium to provide the physical connection for the access control and realizes the encoding, decoding, receiving, and sending of signals. The link layer is responsible for establishing and maintaining data connections, as well as wireless links for management and traffic control.

3. Network Link Security Situation Identification Based on Set Pair Analysis

3.1. Situation Element Acquisition. Situation elements are obtained from logs and warning events of various anomaly detection devices and security devices, and attack types are divided into network detective, host service, and network resources [6, 7]. Specific attacks are as follows:

(1) Port scan

Ports belong to the connection terminal, play the role of a carrier, and also are the main object of attack and scanning. When scanning begins, the attacker transmits a large number of data packets to the host and analyzes the running and open ports on the target host in combination with the receiving and response status. Because all systems have certain security vulnerabilities, attackers can research targeted attack strategies according to the scanning results.

(2) UDP flood

The User Datagram Protocol (UDP) flood attack is also called a flood attack. This attack uses UDP, which eliminates the need for connection construction and authentication during data transmission. During the attack, the attacker sends abnormal data packets in batches, which consumes the network resources of the attacked host by occupying bandwidth. In addition, the host is too busy processing data packets to take care of normal connections, resulting in system crash [8].

(3) Web DoS attack

A Denial of Service (DoS) attack transmits massive data in correct format but not within normal services to the host. The host does not distinguish normal services from abnormal services. Due to limited resources, some normal business was refused [9]. However, due to the gradual
improvement of server performance, a small number of packets of attackers can no longer damage the server, so the attackers jointly send DoS attacks to the host, which is the so-called distributed denial service attack.

(4) Illegal access request

Illegal request indicates the network access that does not comply with communication policies and rules. Collecting security data of this part is of great significance for network link security situation identification.

With the increase in the number of users, the network data is gradually huge. How to extract effective information from the huge network system is the basis of situation identification. To this end, the situation element acquisition framework is constructed as follows.

In this paper, the hierarchical situation element acquisition model is used to analyze the situation elements, as shown in Figure 2. The acquisition method is divided into global analysis and local analysis and follows the principle of local before the whole to realize the acquisition of elements.

3.2. Feature Vector Property Selection. The main goal of network link security situational awareness is to obtain characteristic information of network operation [10], analyze the relationship between these information, and obtain the degree of influence on network security situation. In view of the above common attack events, the following factors are selected as feature vector attributes in this paper.

(1) Transmittance factor

The transmit rate factor can determine how many packets a node generates and transmits per unit time. Assume $S_n(t)$ represents the number of data packets generated by node $n$ within time slot $t$. When the network environment is relatively stable, $S_n(t)$ is also relatively stable. If the average value of $S_n(t)$ is much higher than $S_n$, it indicates that node $n$ has the possibility of launching DoS attacks. Otherwise, node $n$ may fail. The expression of the transmittance factor is as follows:

$$S_{Tr}(t) = \frac{n \times S_n(t)}{\sum S_j(t)},$$  \hspace{1cm} (1)$$

where $n$ is the number of sending times.

(2) Forwarding factor

The forwarding rate factor can judge the level of packets forwarded by nodes. Assume that $R_k(t)$ is the number of packets received by node $k$ in time slot $t$ and $T_k(t)$ is the number of packets sent by node $k$ at the same time. If $T_k(t)$ is much higher than the average value of $T_k(t)$, it indicates that node $k$ has the possibility of launching black-hole attacks. The calculation formula of the forwarding factor is as follows:

$$S_{Tr}(t) = \frac{n \times T_k(t)}{R_k(t)}.$$  \hspace{1cm} (2)$$

(3) Data source dispersion factor

Data source dispersion can evaluate data dispersion. Assume that $R_{NS}(n)$ represents the number of neighbor nodes in the first $n$ packet received by node $k$ and $N$ represents the total number of nodes [11]. A large number of $R_{NS}(n)$ indicates that nodes are suspected of launching hexenbiest Sybil attacks. The description formula of the discrete factor is as follows:

$$S_{DS}(n) = \frac{R_{NS}(n)}{N}. \hspace{1cm} (3)$$

(4) Node aggregation factor

The aggregation factor is an indicator to measure the concentration degree of the node’s next hop. Assume that $S_j(n)$ represents the total number of the first $n$ packets transmitted by node $k$ to the $j$-th neighbor node and $S_{pk}(n)$ represents Max ($S_{pk1}(n), S_{pk2}(n), S_{pk3}(n), ...$). If the value of $T_{Ak}(n)$ is lower than the average value of $T_{NA}(n)$, the node $k$ is suspected of launching attacks, and the definition is as follows:

$$T_{Ak}(n) = \frac{S_{pk} \times n}{T_{NA}(n)}.$$  \hspace{1cm} (4)$$

The features of ad hoc network link state data are extracted by the above factors, and the network link security situation identification model is constructed based on these features.

3.3. Security Situation Identification Model. The node records and distinguishes all received and sent data packets in time slot $t$, and the data information vector passing through the node in this period is expressed as $D = (d_1, d_2, d_3, ..., d_n)$. The data vector $D$ and the elements in the feature information vector set $M = \{M_1, M_2, ..., M_i\}$ constitute identical-discrepancy-contrary system (IDCS). Suppose that the relationship between $D$ and $M_k$ in the $x$-th component is expressed as $\mu_k^x$, according to the set pair analysis principle, the equation for describing the system is as follows:

| Table 1: Coefficient and set pair relations. |
|---------------------------------------------|
| Set pair potential distribution | Value of $a$, $b$, and $c$ |
| $0 \leq \varphi_a \leq \epsilon_{same}$ | $a = 0$, $b = c = 0$ |
| $\epsilon_{same} \leq \varphi_n \leq \epsilon_{counter}$ | $b = 1$, $a = c = 0$ |
| $\epsilon_{counter} \leq \varphi_n \leq 1$ | $c = 1$, $a = b = 0$ |
between information is a large value indicates a high degree of contrast and the larger the value is, the stronger the uncertainty degree is. A larger value is and the more similar the two data are. The degree of connectedness can be divided into the sum of a finite number of connectedness factors. The discrete multivariate relation degree of the data vector \( D \) and the feature information vector \( M_k \) is expressed as follows:

\[
\mu_k = \frac{\omega_1 \mu_k^1 + \omega_2 \mu_k^2 + \cdots + \omega_n \mu_k^n}{n},
\]  

(7)

The following formula can be obtained from equation (7):

\[
\mu_k = \frac{1}{n} \sum_{i=1}^{n} \omega_i \left[ a_i b_i c_i \right] \begin{bmatrix} 1 \\ i \end{bmatrix} + \sum_{i=1}^{n} \omega_i b_k^i, 
\]  

(8)

Because there is an inverse relationship between the identical degree and degree of opposition, so \( j < 0 \), therefore equation (7) can also be converted into the following form:

\[
\mu_k = \frac{\sum_{i=1}^{n} \omega_i \left( a_k^i - |j| c_k^i \right) + \sum_{i=1}^{n} \omega_i b_k^i}{n}, 
\]  

(9)

where \( \sum_{i=1}^{n} \omega_i \left( a_k^i - |j| c_k^i \right) \) and \( \sum_{i=1}^{n} \omega_i b_k^i \) represent the determined and undetermined parts of the correlation expression, respectively. When the known part of the formula is different, a larger value indicates a higher correlation degree, indicating that the two states are more similar. If the determined part is the same [13], a larger value of the undetermined part indicates a lower correlation degree, indicating that the two states have obvious differences; when the same degree of different operating states is lower than the difference degree, 

The relationship between the degree of identity, difference, and opposition in the expression of the degree of connection is shown in Table 1.

If the \( x \)-th component vector is a discrete variable, when \( z_x^d = z_x^m \), then \( a = 1, b = c = 0 \); otherwise, \( c = 1, a = b = 0 \), so the sensitivity of \( x \) to the whole vector is \( \omega_x \). Combined with the identical-conflicting properties of the set pair analysis, the degree of connectedness can be divided into the sum of a finite number of connectedness factors. The discrete multivariate relation degree of the data vector \( D \) and the feature information vector \( M_k \) is expressed as follows:

\[
\mu_k = \frac{\omega_1 \mu_k^1 + \omega_2 \mu_k^2 + \cdots + \omega_n \mu_k^n}{n},
\]  

(7)

The following formula can be obtained from equation (7):

\[
\mu_k = \frac{1}{n} \sum_{i=1}^{n} \omega_i \left[ a_i b_i c_i \right] \begin{bmatrix} 1 \\ i \end{bmatrix} + \sum_{i=1}^{n} \omega_i b_k^i, 
\]  

(8)

Because there is an inverse relationship between the identical degree and degree of opposition, so \( j < 0 \), therefore equation (7) can also be converted into the following form:

\[
\mu_k = \frac{\sum_{i=1}^{n} \omega_i \left( a_k^i - |j| c_k^i \right) + \sum_{i=1}^{n} \omega_i b_k^i}{n}, 
\]  

(9)

In the formula, \( a_k^i \) represents the degree of sameness between the data vector \( D \) and the feature vector \( M_k \) in the \( x \)-th component; the larger the value is, the higher the value is and the more similar the two data are. \( b_k^i \) represents the degree of difference between the two components; the larger the value is, the stronger the uncertainty degree is and the larger the value is. \( c_k^i \) represents the degree of opposition; a large value indicates a high degree of contrast between information \( i \) and \( k \).

If the \( x \)-th component is a continuous variable, the set pairs of vector \( D \) and \( M_k \) on the \( x \)-th component can be expressed as

\[
\varphi(x) = \frac{|z_x^d - z_x^m|}{(z_x^d + z_x^m)},
\]  

(6)

where \( z_x^d \) and \( z_x^m \), respectively, represent the value of the \( x \)-th component vector \( D \) and \( M_k \). Take \( \varepsilon_{\text{same}} \) and \( \varepsilon_{\text{contrary}} \) as set pair potential critical values, and \( 0 \leq \varepsilon_{\text{same}} < \varepsilon_{\text{contrary}} \leq 1 \) [12].

### Table 2: Server topology weight data.

| Server type | Topology weight | Standard weight |
|-------------|-----------------|-----------------|
| Server 1    | 0.3             | 0.3             |
| Server 2    | 0.3             | 0.3             |
| Server 3    | 0.4             | 0.4             |

### Table 3: Main link topology weight.

| Link        | Topology weight | Standard weight |
|-------------|-----------------|-----------------|
| Link 1      | 0.4             | 0.4             |
| Link 2      | 0.2             | 0.2             |
| Link 3      | 0.4             | 0.4             |

**Figure 3:** Topology diagram of simulation experiment.
that is, \(1/n \sum_{i=1}^{n} \omega_{i} (\hat{a}_{i} - \hat{b}_{i}) < 0\), in this case, the node tends to be in an uncertain state. The \(\omega\) value is calculated, and the connection degree of each element in the data vector and feature information vector set is calculated, respectively; \(\mu = \text{Max}(\mu_{1}, \mu_{2}, \cdots, \mu_{l})\); then, the network link state tends to be in the \(x\)-th state in the feature vector set.

We set the reference feature vector \(S = \{R_{1}, R_{2}, \cdots, R_{l}\}\), where \(R_{i}(i = 1, 2, \cdots, l)\) represents the proportion of the total number of nodes in the \(i\)-th state in the feature vector to the total number of nodes; the situation vector to be measured is \(s = \{r_{1}, r_{2}, \cdots, r_{l}\}\), where \(r_{i}(i = 1, 2, \cdots, l)\) describes the proportion of the \(i\)-th state node in the whole node [14]. The security situation value of the network link to be tested can be expressed by the formula of network security entropy:

\[
\rho = \frac{\sum_{i=1}^{l} \partial_{i} \times (R_{i} - U_{i})^{2}}{\sum_{i=1}^{l} \partial_{i} \times (R_{i} - r_{i})^{2}},
\]

(10)

where \(U_{i}\) represents the percentage of the number of nodes in the \(i\)-th state in the total number under the condition of absolute insecurity and \(\partial_{i}\) represents the weight of components. The higher the \(\rho\) value is, the more secure the network link is, and the preliminary identification of the network link security situation is realized.

In a statistical period, each attack event may have multiple events \(e\). The attack hazards of multiple events of the same type will be accumulated when the security factor situation is calculated. Therefore, the quantitative identification formulas of network detective security element situation \(P_{D}\), host service element situation \(P_{S}\), and resource element situation \(P_{N}\) are as follows:

\[
P_{D} = h_{D} \times \sum_{e \in E_{t}} (H_{e} \times I_{e}),
\]

(11)

\[
P_{S} = h_{S} \times \sum_{e \in E_{t}} (H_{e} \times I_{e}),
\]

(12)

\[
P_{N} = h_{N} \times \sum_{e \in E_{t}} (H_{e} \times I_{e}),
\]

(13)

where \(h_{D}\) represents the situation factor of network detective security factor, \(h_{S}\) represents the situation factor of host service factor, \(h_{S}\) represents the situation factor of resource factor, \(H_{e}\) represents the possibility of attack, \(I_{e}\) represents the attack intensity, and \(h_{i}\) represents the attack harm factor.

4. Simulation Experiment and Result Analysis

In order to prove the performance of the proposed network link security situation recognition method, a network as shown in Figure 3 is constructed for the simulation experiment. This includes network facilities such as server nodes, routers, firewalls, and switches. The node performance information can be collected in real time to obtain the performance information of each link.

The server weight data and link weight values in Figure 3 are shown in Tables 2 and 3, respectively.

As can be seen from Tables 2 and 3, the weight values of server topology and main link topology are the same as the corresponding standard weights, respectively, indicating that network link security situation has good identification performance.

In order to facilitate the administrator to make decisions, the identification results are quantified. In the situation calculation of security elements, hazard coefficients of various attack events are determined based on management experience, as shown in Table 4.

The recognition results of the proposed method are compared with the expected results, as shown in Table 5.

As can be seen from Table 5, there is no significant difference between the security situation value identified by the proposed method and the expected output value. Only in the ninth simulation process, there is a certain deviation in the classification of security level, which is due to the existence of certain interference information in the process of situation factor acquisition.
5. Discussion

In recent years, with the rapid development of Internet, medical care and health service informatization level gradually strengthens while the risk of network security increases as well. The medical unit network is vulnerable to all kinds of network attacks, which not only gives rise to the information leakage of patient privacy but also hinders the further development of medical informatization. It has become a hot research topic currently.

In this paper, a link security situation identification method is proposed by analyzing the internal network structure of medical units and combining with set pair analysis theory. The simulation results show that the proposed model can well identify the risk levels of different links in the internal network of medical units and provide valuable suggestions for preventing network attacks.

Note that if predictive control algorithms in this field [15–17] may be implemented, the network security and managers’ decision-making ability would be further enhanced.

6. Conclusion

In order to strengthen network security and improve managers’ decision-making ability, a research on security situation identification based on set pair analysis is proposed. By collecting situation elements and extracting features, a situation recognition model is established. Simulation results show that there is little difference between the security situation values identified by this method and the expected output values. However, the acquisition process is completed manually. In the future research, automatic acquisition and preprocessing of situation elements will be realized to further reduce the identification of interference factors. In addition, the experimental environment is limited, so whether the situation recognition method based on set pair analysis can be applied to the internal network of large-scale medical units remains to be further studied.

Data Availability

Data can be available on request from the authors due to privacy/ethical restrictions.

Conflicts of Interest

There are no competing interests associated with the manuscript.

Authors’ Contributions

Honghua Zeng and Riguang Zhong were responsible for the conception and design and approval and accountable for the results of the study. Yifu Zeng was responsible for the interpretation, drafting, critical revision, and data interpretation. Qingquan Chen was responsible for the analysis and critical revision. Ling Yao, Jiajing Zhuang, Zhixuan Huang, and Shuhan Huang were responsible for the data interpretation. All authors have read and approved the manuscript.

References

[1] X. Li, M. Wu, L. Gang, Y. Yong, and L. Shi, “On-line identification of biomass fuels based on flame radical imaging and application of radical basis function neural network techniques,” IET Renewable Power Generation, vol. 9, no. 4, pp. 323–330, 2015.
[2] M. Husak, J. Komarkova, E. Bou-Harb, and P. Celeda, “Survey of attack projection, prediction, and forecasting in cyber security,” Communications Surveys & Tutorials, IEEE, vol. 21, no. 1, pp. 640–660, 2019.
[3] X. H. Yang, J. He, C. L. Di, and J. Q. Li, “Vulnerability of assessing water resources by the improved set pair analysis,” Thermal Science, vol. 18, no. 5, pp. 1531–1535, 2014.
[4] Z. Zhang, P. Qiao, Q. Qi, J. Xu, and Z. Zheng, “Study on the multi-factor degree set pair analysis fuzzy evaluation model based on entropy weight [C]3rd,” International Conference on Biomedical Engineering and Informatic, IEEE, 2010, vol. no. 7, pp. 2979–2984, 2010.
[5] H. M. Yang, C. Y. Zhang, R. T. Liang, and F. Tian, “Set pair social network analysis model [J],” Applied Mechanics and Materials, pp. 50–51, 2011.
[6] L. Shen and Z. Wen, “Network security situation prediction in the cloud environment based on grey neural network [J],” Journal of Computational Methods in Sciences and Engineering, vol. 19, pp. 1–15, 2018.
[7] A. Sundararajan, T. Khan, A. Moghadasi, and A. I. Sarwat, “A survey on synchronphasor data quality and cybersecurity challenges, and evaluation of their interdependencies [J],” Modern Power Systems and Clean Energy, vol. 7, no. 3, pp. 449–467, 2019.
[8] Y. Shi, Y. Renfa Li, and X. P. Zhang, “An immunity-based time series prediction approach and its application for network security situation,” Intelligent Service Robotics, vol. 8, no. 1, pp. 1–22, 2015.
[9] W. Liang, J. Long, Z. Chen et al., “A security situation prediction algorithm based on HMM in mobile network [J],” Wireless Communications & Mobile Computing, vol. 2018, pp. 1–11, 2018.
[10] G. Xu, Y. Cao, Y. Ren, X. Li, and Z. Feng, “Network security situation awareness based on semantic ontology and user-defined rules for Internet of things,” IEEE Access, vol. 5, pp. 21046–21056, 2017.
[11] R. Xi, X. Yun, and Z. Hao, “Framework for risk assessment in cyber situational awareness,” IET Information Security, vol. 13, no. 2, pp. 149–156, 2019.
[12] Y. Shi, T. Li, W. Chen, and Y. M. Fu, “Network security situation prediction using artificial immune system and phase space reconstruction,” Applied Mechanics & Materials, vol. 44–47, pp. 3662–3666, 2010.
[13] H. Zhang, Y. Yi, J. Wang, N. Cao, and Q. Duan, “Approach and algorithm for generating appropriate doped structures for high-throughput materials screening,” Computers, Materials & Continua, vol. 150, no. 3, pp. 381–389, 2018.
[14] X. Liu, Y. Jiguo, W. Lv, D. Yue, and Y. W. Yinglong Wang, “Network security situation: from awareness to awareness-control,” Journal of Network and Computer Applications, vol. 139, pp. 15–30, 2019.
[15] K. K. L. Wong, “Bridging game theory and the knapsack problem: a theoretical formulation,” Journal of Engineering Mathematics, vol. 91, no. 1, pp. 177–192, 2015.
[16] H. Zhengzhou, L. Kaihua, L. Zhuo, and Y. Liu, “Named data networking with neural networks for intelligent image processing information systems,” Enterprise Information Systems, vol. 1-16, 2020.

[17] L. Wei, S. Wan, J. Guo, and K. K. L. Wong, “Novel hierarchical selected ensemble classifier with bioinformatics application,” Artificial Intelligence in Medicine, pii, vol. S0933-3657, no. 16, pp. 30576–30579, 2017.