2023 IEEE 2nd International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA) | 978-1-6654-6253-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/EEBDA56825.2023.10090710

Research on Network Information Security Model Based on Computer Artificial Intelligence Technology

Jiali Xiao*
Beijing University of Technology ZHUHAI & USM
Zhuhai City, Guangdong Province, China
02062@bitzh.edu.cn

Yifeng Li
Beijing University of Technology Zhuhai
Zhuhai City, Guangdong Province, China
l13829828383@126.com

Tian Yan
Beijing University of Technology Zhuhai
Zhuhai City, Guangdong Province, China
tianyan2022@126.com

Lihua Li
Beijing University of Technology ZHUHAI & USM
Zhuhai City, Guangdong Province, China
02062@bitzh.edu.cn

***Abstract*—This paper proposes a security assessment method based on rough set theory for flood DDoS attacks. It realizes real-time quantitative assessment of security threats. The hardware structure of network communication early warning system is designed by taking FTGUI-20003-1B processor and warning signal lamp as an example. In this paper, the sensor technology is introduced to acquire the state characteristics of the communication network. Rough set theory is introduced to identify network security state. It divides the communication network link into the communication channel composed of multiple nodes and identifies the security state of the communication network. The simulation results show that the intrusion detection capability of this method is strong and the reliability and stability of security detection are good.**

Keywords—computer, artificial intelligence, network information security, rough set algorithm, situational awareness

I. INTRODUCTION

In recent years, with the frequent occurrence of events threatening network security, a large number of computers are invaded by viruses and trojans, and the security of computer networks is faced with severe challenges, and the situation of network security is not optimistic. In order to enhance the capacity of computer network security and protection, network managers although by installing intrusion detection systems, firewalls, antivirus software and other measures to build a road safety defense, but with the increase of network complexity and uncertainty, these protective units just passively or in some way with a single method for isolation of protection, And cannot work together, it is difficult to have a good protection effect in the large-scale network; At the same time, a large number of security logs and alarm information are generated constantly in the process of protection, which makes the management personnel unable to quickly and efficiently analyze the important changes in network security, and also unable to predict future attacks and potential threats [1]. How to change the passive network security protection into the active one in the dynamic complex network, so as to analyze and evaluate the changes of network security quickly and effectively, is the focus of future network security research. The author takes the rough set as the analysis tool, organizes and summarizes the air traffic control safety risks, and optimizes the selection of early warning indicators on the basis of the attribute reduction of the rough set, so as to reduce subjectivity and improve the early warning accuracy.

II. DESIGN OF NETWORK INFORMATION SECURITY SYSTEM

A. Hardware Design

In order to meet the high-performance operation requirements of the system, the processor model selected in this design is FTGUI-20003-1B, which is a derivative version of the 12th generation Intel Core. Its structure, comprehensive performance and energy efficiency are significantly better than those of earlier versions, and it can realize collaborative processing of multipath tasks in practical applications. The processor is integrated with a special artificial intelligence engine and has a >14.0 core hardware thread. When it is connected with the Windows11 operating system, it can realize balanced processing and load of dynamic tasks in the process of task processing, ensuring high efficiency and low energy consumption in the operation. Based on the existing components of FTGUI-20003-1B processor, an AI acceleration chip is built in to ensure that the processor can timely process multi-link network communication data, even if the data link transmission information exceeds its expectations, it can avoid the overload of the processor [2]. In order to meet the early warning requirements of the system, the indicator resistance with large resistance is usually selected to ensure that the current flowing through the early warning signal lamp is kept in a small state. Normally, warning lights are connected by a lamp holder, lampshade, lamps and lanterns, line-based components, such as signal consists of leds, need to communicate with front-end TG - 200 sensor connection, and placed in locations such as evident in the dashboard, to ensure that the lights can play or a warning effect in use.

B. Software Design

Under the support of the hardware equipment, the sensor technology is introduced to obtain the state characteristics of the communication network. In this process, it is necessary to ensure that the obtained status information has the characteristics of high quality. Only when this feature is satisfied, can the reliability of subsequent early warning of communication network anomalies be ensured. At present, there are many technologies that can be used to extract its

state information, most of which may have certain interference in application. However, the sensor technology selected in this paper can eliminate some invalid information and redundant information in the state information at the initial collection stage, even though the collected information still inevitably carries noise information. However, this part of information can also be solved in subsequent processing [3]. Therefore, after the preliminary acquisition of the state information of the communication network based on sensor technology, it is necessary to describe its characteristics by dividing the state of the network security and the level of the network security. The rough set algorithm is used in this study.

Fuzzy set theory and rough set theory have extended classical set theory in dealing with uncertainty and imprecision problems. The comparison and fusion of the two theories has always been an interesting topic. Suppose (U,R) is the approximate space, R is the equivalence relation on the domain U, F is a fuzzy set, then $\forall F \in \mathcal{F}(U)$, the upper and lower approximation $\overline{apr}_R(F)$ and $\underline{apr}_R(F)$ of the fuzzy set F on the space (U,R) are a pair of fuzzy sets:

$$\begin{aligned} \mu_{\overline{apr}_R F}(x) &= \sup\{\min[\mu_F(y), \mu_R(x,y)] \mid y \in U\}, \\ \mu_{\underline{apr}_R F}(x) &= \inf\{\max[\mu_F(y), 1-\mu_R(x,y)] \mid y \in U\}. \end{aligned} \quad (R-F)(1)$$

$(\underline{apr}_R(F), \overline{apr}_R(F))$ is called the rough fuzzy set of fuzzy set F on U. Rough-Fuzzy model extends the approximate object from crisp set X to fuzzy set F.

If the equivalence relation R is further extended to the fuzzy similarity relation R, then there is a fuzzy approximation space $(U,\mathcal{R})$. $\forall F \in \mathcal{F}(U)$, the upper and lower approximation $\overline{apr}_{\mathcal{R}}(F)$ and $\underline{apr}_{\mathcal{R}}(F)$ of fuzzy set F on space $(U,\mathcal{R})$ are a pair of fuzzy sets:

$$\begin{aligned} \mu_{\overline{apr}_{\mathcal{R}} F}(x) &= \sup\{\min[\mu_F(y), \mu_{\mathcal{R}}(x,y)] \mid y \in U\}, \\ \mu_{\underline{apr}_{\mathcal{R}} F}(x) &= \inf\{\max[\mu_F(y), 1-\mu_{\mathcal{R}}(x,y)] \mid y \in U\}. \end{aligned} \quad (F-R)(2)$$

$(\underline{apr}_{\mathcal{R}}(F), \overline{apr}_{\mathcal{R}}(F))$ is called the fuzzy rough set of fuzzy set F on U. Fuzzy-rough model not only extends the approximate object from crisp set X to Fuzzy set F, but also extends the equivalence relation R on the theoretic domain to fuzzy similarity relation R.

From the formula (R-F), (F-R), it is obvious that rough fuzzy set is a special case of fuzzy rough set. The classical rough set is also a special case of the Rough fuzzy set whose approximate object is the crisp set. In order to better understand this conclusion, let's look at another definition of rough set.

As mentioned earlier, rough sets are described by upper and lower approximations, which are sometimes called weak-strong member functions of rough sets. Using μ_X, μ_R to represent the member functions of X and R, note that the eigenfunction representation of the set description (i.e.: $\mu_X(y) = 1$, if $y \in X$.

The above equation is also a pair of fuzzy sets. By observing the formulas (R) and (R-f), it is obvious that the classical rough set is a special case of rough fuzzy set when the approximate object is crisp set X. Since the rough set, rough fuzzy sets and fuzzy rough set is a fuzzy set, then they must can be expressed in the form of - cut sets

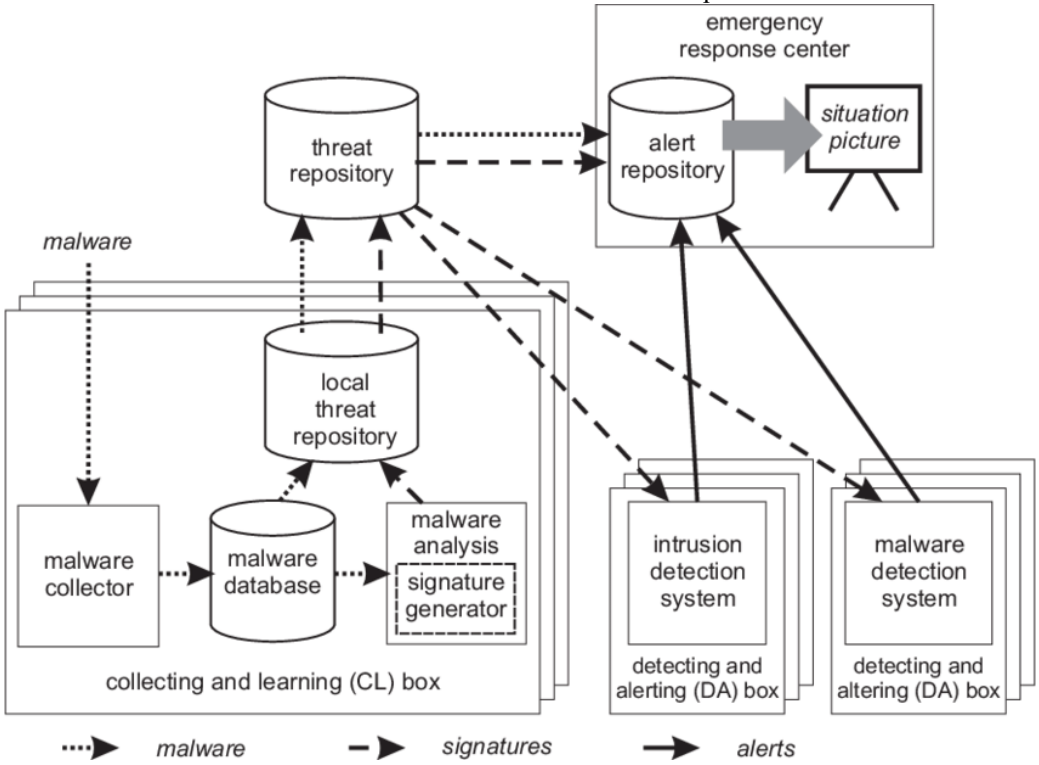

Fig. 1. Communication network anomaly and warning process

III. Establish a communication network anomaly warning mechanism

After the above design is completed, the communication network anomaly early warning mechanism is established to carry out the communication network anomaly early warning. The anomaly and early warning process is shown in Figure 1.

According to the process shown in Figure 1 above, the communication network anomaly warning is carried out. When the communication network anomaly and risk are identified, the risk information needs to be extracted, and the warning level and category are divided by refining the risk information. The establishment of network security posture architecture is the key to the application of network security posture technology and directly affects the application effect of network security posture system performance [4]. By combining the JDL model with the network security situational awareness model given by Endsley, and conducting quantitative research on the association management between architecture components, this paper designs the system framework of network security situational awareness, as shown in Figure 2. The system structure is mainly hierarchical structure, intuitive and simple.

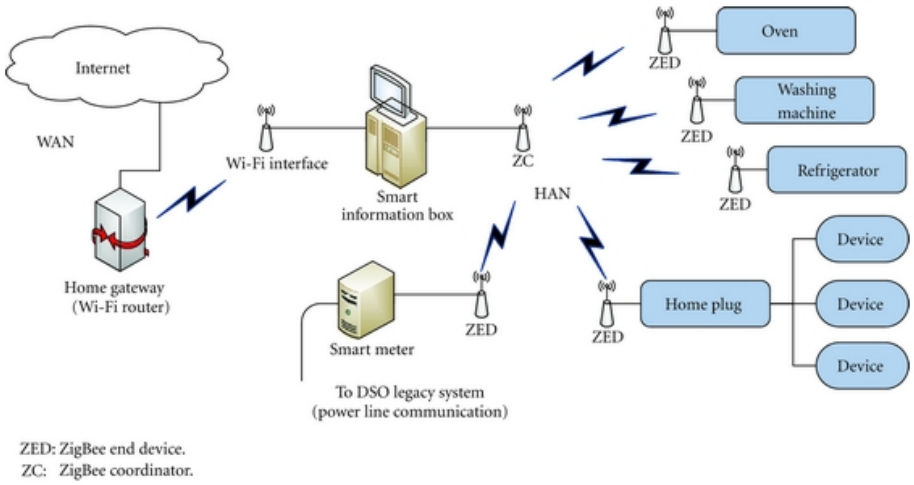

Fig. 2. Network security architecture

A. Collection and preprocessing of original data

The network security situational awareness system collects all kinds of related log data from various network protection software, such as firewalls, intrusion detection systems and antivirus software distributed in the network system. However, these data contain a lot of redundant data, error and false alarm information, and the data formats are different, it is impossible to use these data directly for information mining and analysis [5]. The pre-processing technology should screen and reduce the different data information from different software, and carry out unified conversion and storage of data in heterogeneous data formats, so as to prepare the data for future security assessment and early warning.

B. Event Association

Data fusion and mining technology is used to conduct correlation analysis on the collected data, eliminate redundant data information, and extract and integrate the associated data information that poses a threat to network security.

C. Response and warning

According to the situation of network security situation as a result, not only to the impending network security incident response and defensive measures, accordingly achieve the function of active defense, but also through the history of network security situational awareness and the current network security situational awareness data comparison and analysis, and the trend of the security situation of anticipation, it provides decision and reference for future network security management.

D. Network Security situation visualization

The traditional form of text data cannot directly and clearly feedback the network security situation results to users. The network security situation system displays a large number of abstract and boring current network security situation data in the form of dynamic graphics through the visual display function, which is convenient for users to view and improves the visibility and intuitiveness of data display.

IV. System inspection

Figure 3 shows the sample information transmitted by enterprise informatization network. The first 200 sampling points were selected and 300 Monte Carlo experiments were used to defend the network security of enterprise informatization [6]. The least square and deep convolutional neural methods were used as experimental comparison methods to obtain the detection output of virus intrusion information, as shown in Figure 4.

According to the analysis of Figure 4, the output frequency of security defense detection of enterprise informatization network by the least square method fluctuates greatly, mainly between -20 and 10MHz, while that of the deep convolutional neural method mainly ranges between -10 and 10MHz, which fluctuates greatly [7]. The output frequency of enterprise information network security defense detection using the proposed method is stable at

about 0MHz, which has high stability. It can be seen that the method proposed in this paper can realize the stable operation of enterprise informatization network security defense system. On this basis, the accuracy of the three methods for virus intrusion detection is tested, and the comparison results are shown in Figure 5.

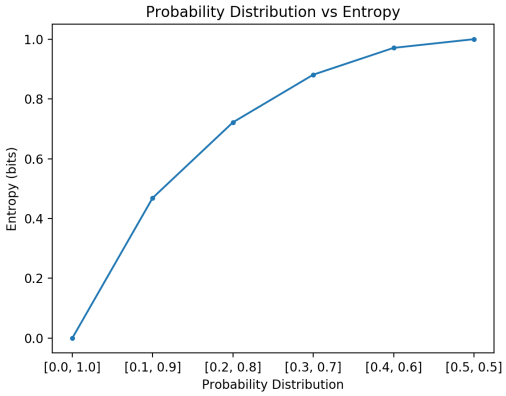

Fig. 3. Network transmission information of enterprise informatization

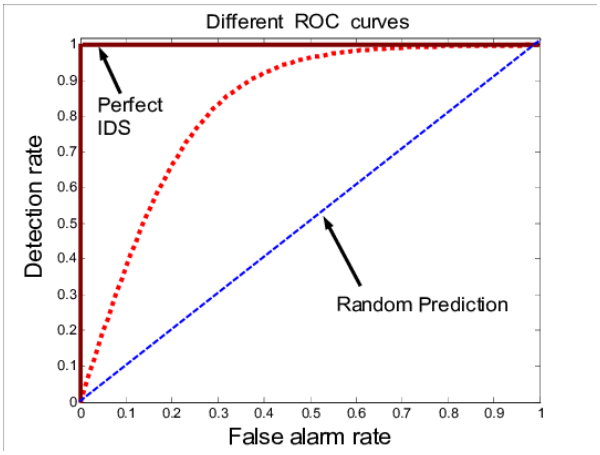

Fig. 4. Output of enterprise information network virus intrusion detection

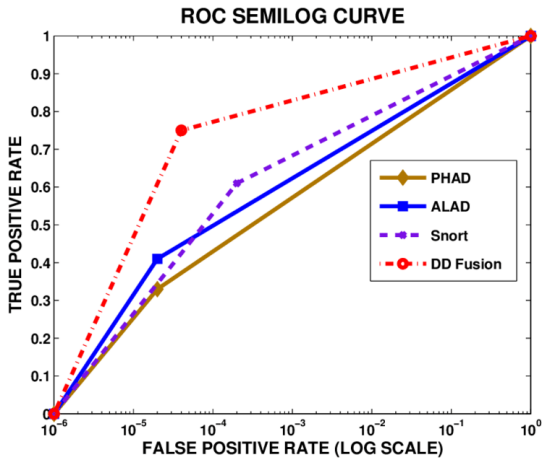

Fig. 5. Accuracy test of virus intrusion detection

The analysis of Figure 5 shows that the average detection accuracy of the least squares method is 79%, the average detection accuracy of the deep convolutional neural method is 75%, and the average detection accuracy of the method proposed in this paper for the enterprise informatization network security defense is 96%. The method proposed in this paper can effectively detect the virus intrusion of the enterprise information network, and effectively improve the enterprise information network security defense ability.

V. Conclusion

This paper presents the threat of applying rough set algorithm to DDoS attack

The degree evaluation method can reasonably evaluate the security threat status of the system in real time, and when the attack starts, the situation value rises rapidly, which plays a role of timely alarm. Empirical analysis shows that the calculation results of this method are accurate, but the accuracy and performance of the least squares support vector machine model are highly related to the selection of operation parameters, in order to further improve the accuracy and operation speed of the algorithm.

Acknowledgement

In this paper, the research was sponsored by Provincial key platforms and major scientific research projects of Guangdong universities (No.2021ZDZX3004)

References

[1] Ren Jiawei. Research on Risk Hierarchy Analysis Model of computer network information security. Journal of Bonding, vol. 43, pp. 49-51,September 2020.

[2] Zhang Xin, Dong Liming. Quantitative simulation of network node information security based on attack and defense game model. Computer Simulation, vol. 037, pp. 18-21,98,June 2020.

[3] Lian Wenjuan, Zhao Duoduo, Fan Xiubin. CFL SSL protocol based on CFL_BLP model. Computer Engineering, vol. 47, pp. 120-124,June 2021.

[4] Tong Changwei. Computer network security and its preventive measures. Economics, vol. 3, pp. 25-32,February 2020.

[5] Yan Rui-ammonium, ZHANG Li-chen. Intrusion detection based on Focal Loss and convolutional Neural network. Computer and Modernization, vol. 7, pp. 55-61,January 2021.

[6] Liu Yuzhou, Fang Xianwen. Validation algorithm of effective variation domain of attack and defense model based on game strategy. Application Research of Computer, vol. 39, pp. 69-75,July 2022.

[7] Zhang Ning, Fan Haitao. Information security early warning model based on Bayesian network. Microcomputer Applications, vol. 44, pp. 38-44,June 2022.