Detection of Abnormal Weak Correlated Data in Network Communication Based on Feature Analysis

Shufen Liu, Xuejun Ma, Zhixiang Hou

College of Computer Science and Technology, Jilin University, China
liusf@jlu.edu.cn, jlmxj08@163.com, 736688480@qq.com

Abstract

With the continuous development and expansion of electronic technology, network communication began to appear abnormal communication, and abnormal network communication generated by weak correlation data is difficult to be eliminated. In order to solve the above problems, this paper proposes a detection method of abnormal weak correlation data in network communication based on feature analysis. The proposed method updates the basic detection principle of the traditional method and adds the steps to set abnormal weak correlation data feature types by using association rule to get more difference features between normal and abnormal data. The method tests abnormal flow data by using Netflow system, unifies data format, and extracts abnormal weak correlation data feature in abnormal flow according to coarse grain size representation. The information entropy is used to define the standard information entropy of abnormal weak correlation data. The weak correlation data is detected in fractal dimension for different time periods, and anomaly detection results are obtained. Experimental results show that the proposed method can effectively improve the adaptive ability of network communication.

Key words: Network communication, Weak correlation data, Feature analysis, Association rules, Information entropy, Anomaly detection

1 Introduction

Electronic technology plays an increasingly important role in contemporary people's lives and production, and network technology has been taken seriously. The development of massive data network communications, developing with network technology at the same time, is facing enormous challenges in today's development background, such as network intrusion, zombie data, worms, communication denial of service [1], which affects network user-related interests and is likely to cause network paralysis [2]. When there are large-scale abnormal weak correlation data in network communication, general detection technology cannot issue alarms in a timely manner [3], which is because although weak correlation data network flow changes are easy to be found [4], data characteristics correlation is small, and is very easy to be missed or false detected [5]. To this end, domestic and foreign research units have begun to proceed with abnormal weak correlation data detection technology research to improve the adaptive capacity of network communications.

[6] proposed an abnormal weak correlation data detection method based on support vector regression. The proposed method uses support vector regression estimation model to avoid individual large regression error, and consider the linearity characteristics of regression linearity as a whole. The purpose of abnormal weak correlation data detection is realized by identifying the associated data in the measured data, comparing residuals between the estimated estimates and the measured values. However, the method has the problem of complex process and time-consuming detection. [7] put forward an anomalous weak correlation data detection way based on fast decomposition orthogonal transformation state estimation algorithm, which detects and discriminates the anomalous weak correlation data based on fast decomposition orthogonal transformation state estimation algorithm by successfully applying hypothesis checking identification and measuring compensation. Anomalous weak correlation data set is established based on the transformation of augmented measurement Jacobian matrix, and orthogonal transformation state estimation algorithm is introduced to realize the purpose of abnormal weak correlation data detection. But the method has poor detection ability. [8] proposed a detecting method of abnormal weak correlation data based on variable width histogram, which aggregates abnormal weak correlation data in the network communication into a width histogram for the detection of abnormal weak correlation data, and avoids unnecessary data transmission, but the method has a problem of large detection error. [9] divided network characteristics into several grades with different similarity degree, and weak correlation data is extracted by advanced mathematical statistics principle. However, when facing user illegal operation, burst data congestion and

[*] Corresponding Author: Xuejun Ma; E-mail: jlmxj08@163.com

DOI: 10.3966/160792642018121907011

network intrusion, the test results appear unstable.

In view of the above problems, this paper proposes a detection method of abnormal weak correlation data based on feature analysis in network communication. Firstly, the causes and detection principles of the related problems are illustrated, and network communication anomaly weak correlation data detection method based on feature analysis is designed. The detailed description of weak correlation data in network communication is carried out, and experimental comparison is made. Experiment results show that the proposed method can effectively improve the adaptive ability of network communication.

2 Problem Description

2.1 Basic Detection Principle of Abnormal Weak Correlation Data

The proposed method of abnormal weak correlation data detection in network communication based on feature analysis is based on the scientific and technological achievements of the previous researchers, and abnormal weak correlation data is detected by normal means, and then the weak links are updated to improve detection performance. The basic detection principle is divided into five steps, namely, abnormal flow extraction, weak correlation data feature extraction, normal data exclusion, abnormal weak correlation data detection, and test result output [10], as shown in Figure 1.

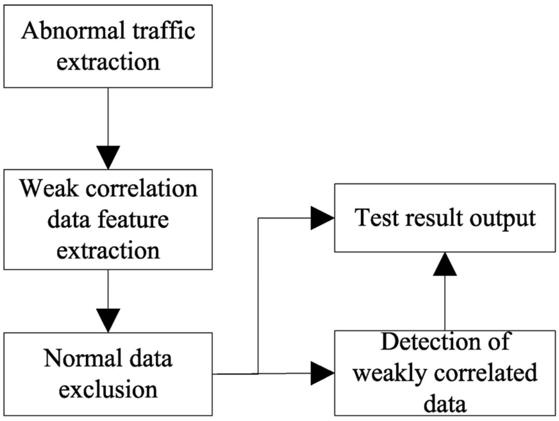

Abnormal traffic extraction
Weak correlation data feature extraction
Normal data exclusion
Test result output
Detection of weakly correlated data

Figure 1. Basic detection principle of abnormal weak correlation data

2.1.1 Abnormal Flow Extraction

Devices perform exception flow extraction are usually distributed over network communication terminal, and each terminal has the same status. They upload abnormal flow to the host independently [11]. Usually there are many network communication terminals which generate abnormal flow, so a number of host agents is set up for terminal flow classification in their respective jurisdictions and then uploads to the host at the same time, as shown in Figure 2. It is worth mentioning that because network communication is heterogeneous, host agents' network structures are different. After abnormal flow extraction, feature format must be unified.

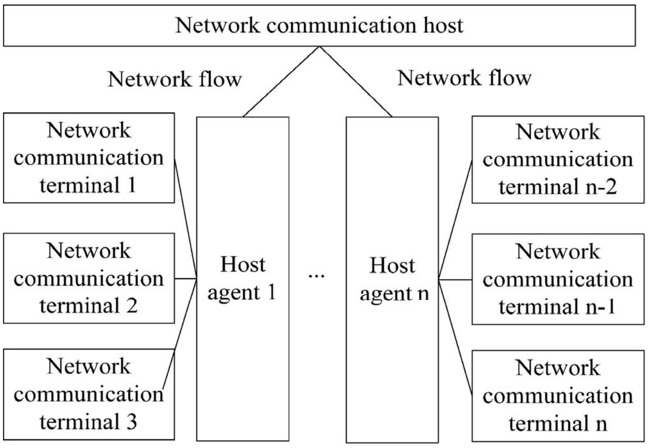

Network communication host
Network flow
Network flow
Network communication terminal 1
Network communication terminal 2
Network communication terminal 3
Host agent 1
...
Host agent n
Network communication terminal n-2
Network communication terminal n-1
Network communication terminal n

Figure 2. Abnormal flow extraction principles

2.1.2 Weak Correlation Data Feature Extraction

The treatment process of this process is very different in different detection methods, so they are not enumerated.

2.1.3 Normal Data Exclusion

Normal and abnormal are two corresponding theories. Weak correlation data contains normal data and abnormal data, and the characteristics between them are very different. Literature analysis can be used to set the characteristic types. Detection method will take the initiative to establish abnormal weak correlation data measurement criteria in weak correlation data feature extraction [12]. From the opposite direction of thinking, it can exclude normal data. The excluded normal data is aggregated in the buffer and output together with the test result. If the accuracy of the test results is not enough, the data in the buffer can be transferred to correct.

2.1.4 Abnormal Weak Correlation Data Detection

According to abnormal weak correlation data feature, we can detect the abnormal situation in weak correlated data, and compare with the normal data to see if there is any consistency between the two and analyze the difference between the two. Compare the test result.

2.1.5 Test Results Output

The result of the test is got from network communication management center [13]. The communication manager will analyze the detection result deeply, and then adjust the abnormal situation of network communication, which can provide the basis for the optimization of weak correlation data detection method.

2.2 Detection Method for Abnormal Weak Correlation Data Based on Feature Analysis

The processing steps of the proposed method, abnormal weak correlation data in network communication based on feature analysis, is shown in Figure 3. Its update of the basic detection principle is the depth of analysis on weak correlation data characteristics. This step is added due to the fact that there are many types of abnormal data in weak correlation data, and there is a strong correlation between normal and abnormal data characteristics [14]. Therefore, we use association rules to better express the characteristics of the association between weak correlation data and abnormal network communication. Association rule is a form like $X \to Y$, in which X and Y are called antecedent or left-hand-side(LHS) and consequent or right-hand-side(RHS).

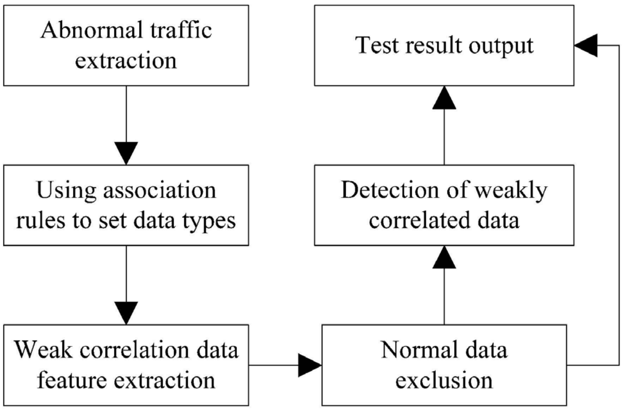

Abnormal traffic extraction
Using association rules to set data types
Weak correlation data feature extraction
Normal data exclusion
Detection of weakly correlated data
Test result output

Figure 3. The processing steps of the proposed method

Association rule is a similarity-based processing scheme in feature analysis. It is also a machine learning method. It will establish association rules for the characteristic parameters of weak correlated data in network communication, and reflect the similarity degree of network flow, data structure and data type [15]. According to the data analysis based on association rules, we can find out the reason and location of abnormal weak correlation data in network communication, and then eliminate the useless data characteristics, and get difference characteristics between normal and abnormal data.

Association rule is adopted to correct weak correlation data feature to optimize real-time and communication cost of traditional detection method and avoid the neglect of internal data characteristics when feature type is set up directly by literature analysis method [16], so that the abnormal weak correlation data can be easily extracted. In addition to the network flow, the research object of association rule also includes node service content and routing protocol in network communication. It emphasizes unite statistical characteristics of weak correlated data, and mines the implicit information between data features. It plays the role of real time network intrusion prevention, and makes a warning to user's illegal operation immediately. The proposed method has so many optimization functions because abnormal weak correlation data detection in network communication based on feature analysis is sensitive to abnormal behavior of network communication and is of high precision in classification of high dimensional data characteristics compared with the detection steps without updating, and it can explain why there are abnormal behavior of network communication. It can tap the characteristics structure to flexibly cope with the dynamic changes in feature parameters, effectively solve network communication malpractice, and coordinate the relationship between user needs and business volume.

3 Weak Correlation Data Detection Details in Network Communication

3.1 Abnormal Flow Extraction

The medium that network communication anomaly weak correlation data detection method based on feature analysis uses in extracting the abnormal flow in network communication is Netflow system. The system contains data exchange protocol, which can collect data coordinates orientation, express the real-time status of network flow, and is international common measurement and analysis agreement [17]. Network communication host agent will use Netflow system to test the validity of abnormal flow data uploaded by the terminal. Netflow system processing block diagram is shown in Figure 4.

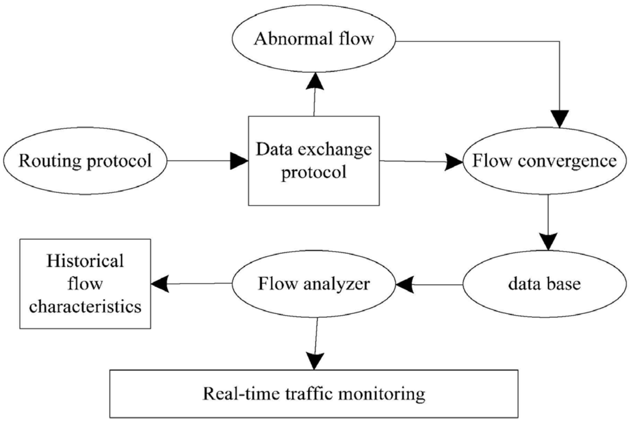


Figure 4. Netflow system processing block diagram

It can be seen from Figure 4 that Netflow system is mainly composed of flow aggregation, database and flow analysis. Network communication host agent gets abnormal flow. Data exchange protocol will deal with abnormal flow with the network's routing protocol, and consolidate them to the database by traffic aggregation port. The abnormal flow stored in the database will not be deleted, and the weak correlation data is also accumulated. Flow analysis port will monitor the real-time flow based on the historical flow characteristics provided by association rules (the first analysis is based on literature analysis method [18]). If there is no abnormality, Netflow system generates a Netflow packet to the host.

Netflow packets have two roles: one is abnormal flow classification summary, the second is unified exception data format. Table 1 describes the data format used for Netflow packets.

Table 1. Data format used by Netflow packets

Start byte	Representation
0	Data source orientation
4	Communication port position
9	Next hop routing orientation
13	Simple network management protocol slogan
16	Total data stream
22	Beginning and end time of data flow
25	Communication port number
30	Identification, service and other information
33	Communication secret key

3.2 Weak Correlation Data Feature Extraction Method Based on Coarse Granularity

In network communication, abnormal network flow caused by abnormal weak correlation data mainly includes distributed denial of service, illegal port scanning, illegal network scanning, worm, instantaneous congestion and Alpha attack [19]. These abnormal weak correlation data characteristics are in Table 2.

Table 2. Characteristic introduction to abnormal weak correlation data

Kinds	Characteristics
Distributed denial of service	A number of communication origins uploads massive data streams to the same communication node, with a single upload time of no more than 20 minutes and has the possibility of including an illegal communication destination.
Illegal port scanning	Target communication has a high degree of aggregation and the ports are evenly distributed
Illegal network scanning	High degree of aggregation in target communication port number with high degree of dispersion
Worm	Target communication directions have a certain similarity under the premise that communication port number is fixed.
Instantaneous congestion	The same number of communication terminals in congestion area, or ports with similar terminal communication port number simultaneously issues a communication request.
Alpha attacks	A number of communication starting point upload large-capacity data packets to the same communication node, and a single upload time is not higher than 10min.

In order to avoid the fail in rapid analysis of weak related data due to excessive network flow, the proposed method adopts coarse grain size method to extract the feature of abnormal weak correlation data. Coarse grain size is a method that only studies object type and does not explain the particular behavior of the object. The anomalous weak correlation data feature type is regarded as granularity, and granularity is divided into coarse grain size and fine grain size [20]. Because network communication anomaly weak correlation data detection method based on feature analysis has established association rules for abnormal flow, only coarse grain size can be used to study feature types to improve precision detection and save detection time.

Abnormal weak correlation data adopts coarse grain size to express their own differences with other data, and abnormal weak correlation data characteristics will monotonically increase with coarse grain size gets greater, that is, data differences increase. Array language is used in calculating coarse grain size that compares the size of data feature only and does not perform accurate calculations. Set the size of coarse grain size of bodies to be compared with each other x and y, and belong to the jurisdiction of different host agents R_1 and R_2, and if $xR_1 \Rightarrow yR_2$, the coarse grain size of x is larger than that of y [21]. Array coarse grain size according to this principle, some of the weakly correlated data features that are of small coarse grain size will be extracted. The normal data in abnormal flow according to Table 2 and association rules will be deleted.

3.3 Anomaly Weak Correlation Data Detection Based on Information Entropy

Information entropy is used to describe probability and information redundancy in feature analysis, and it is a form of coarse grain size expression originated in thermodynamics. American mathematician Claude Alwood Shannon once argued that "The uncertainty of information is similar to the disorder of particles in thermodynamics [22]", proving the feasibility of information entropy in weak correlated data in network communication. Therefore, the proposed network communication anomaly weak correlation data detection method based on feature analysis uses information entropy to describe the disorder of correlated data. The expression of information entropy is shown in equation (1):

$$H(S) = -\sum_{i=1}^{n} P_i \log_2(P_i) \tag{1}$$

In the formula, S is the total capacity of network communication packet, n is the total number of packets, P_i indicates the probability of the existence of abnormal data, i is characteristic order. $H(\mathrm{S})$ is essentially the average capacity of network communication packets.

If the network communication packets in different time periods are disordered, weak association data of the packets will form a random task packet [23]. In the definition of information entropy, the characteristics of abnormal weak correlation data are expressed in coarse granularity, and the characteristic X entropy of abnormal weak correlation data in network communication is calculated according to different time periods. The expression is as follows:

$$H(X) = -\sum_{i=1}^{N} P_i \log_2(P_i) \tag{2}$$

In the formula, N is the total feature, $\sum_{i=1}^{N} P_i = 1$.

The expression of (2) is the distribution rules of abnormal weak correlation data in data packet. The smaller $H(X)$ and the distribution of abnormal weak correlation data are more intensive. The anomalous weak correlated data region is refined, and communication anomaly detection is carried out directly on weak correlated data region with weak distribution. Considering the existence of multiple dimensions in network communication data, it is necessary to place the data of different dimensions in different vector machines, and detect weak correlation data in different time periods in divided dimensions in order to improve detection efficiency. The detection diagram is shown in Figure 5.

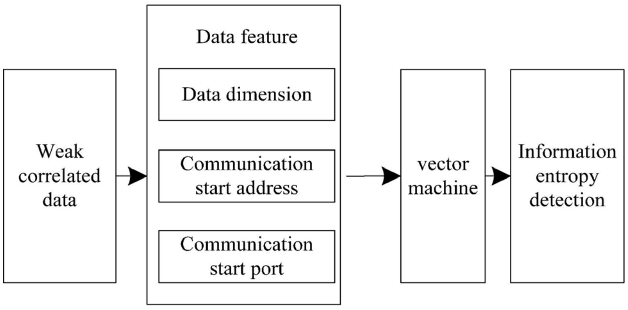


Figure 5. Schematic diagram of anomalous weak correlation data detection based on information entropy

Regardless of any dimension, the actual information entropy of the abnormal weak correlation data has a large difference with the standard information entropy [24], and difference threshold is set according to the actual situation of network communication. Here, the threshold is set to O, which is equal to the variance value between feature sort i and feature arrangement after dimension classification. Set the standard information entropy as H_i, then:

$$H_i = \begin{cases} aO + (1-a)O, \mathrm{t} > 2 \\ O \qquad\qquad\quad ,\mathrm{t} \le 2 \end{cases} \tag{3}$$

In this case, a is weak correlation data characteristic of network communication abnormality detection that is currently being performed, t is time period. $\mathrm{t} > 2$ represents the homeopathic calculation from the second time period. $\mathrm{t} \le 2$ represents the first time period. In summary, although the use of information entropy method can optimize network communication abnormal weak correlation data detection, but it still needs experiment proof.

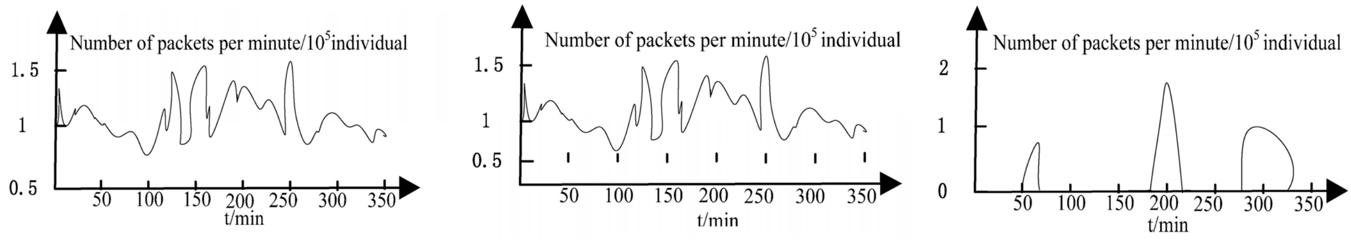
4 Experiment

4.1 Test Set Preparation

In network communication adaptive ability test of network communication anomaly weak correlation data detection method based on feature analysis, virtual test set and real data set are selected in a university campus network. The virtual data set inputs abnormal weak correlated data that is likely to be encountered to network flow based on specific weight. The extraction time of the network flow is from 9:00 am to 3:00 pm on October 30, 2016, and abnormal flow is selected from CAIDA data, which contains some of the more influential network flow anomalies.

There are abnormal weak correlated data characteristics in virtual data set, which includes worms, distributed denial of service, and Alpha attacks. Worms hide their features by cyclical intrusion, thereby reducing network communication efficiency by invading once every fifteen minutes; distributed denial of service takes effect after the first 10 minutes, the last ten minutes and the middle 20 minutes of the intrusion network flow. Worms, distributed denial of service and Alpha attacks account for 10%, 30% and 5% of total network flow. Figure 6 shows that (a) is network total flow, which shows a smooth floating trend; (b) is virtual data aggregate flow, and is basically consistent to the total network flow waveform; (c) is the total network flow of abnormal weak correlated data, invaded by worm (0min~150min), distributed denial of service (150min~250min) and Alpha attack (250min~350min).

The real data set extracts the network flow in the network flow on October 30 and 31, 2016, as shown in Figure 7. There are four abnormal flow problems caused by weak correlation data in network flow on the 30th, and there are three places on 31st. Table 3 shows the statistics of the two test sets.



(a) Network total flow (b) Virtual data aggregate flow (c) The total network flow

Figure 6. Virtual data set flow curve

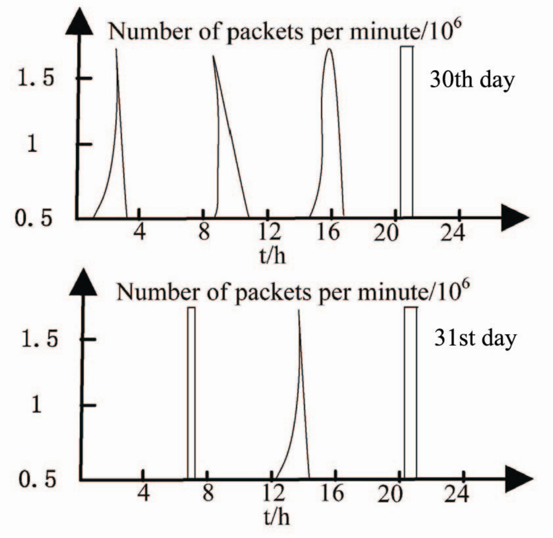


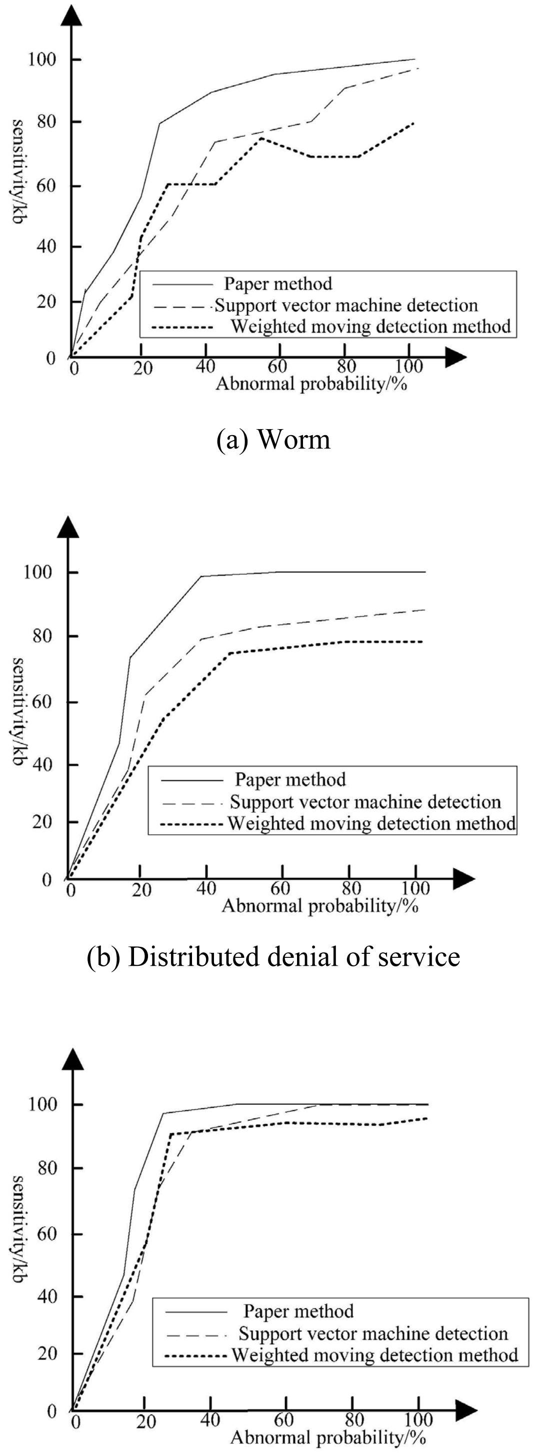
Figure 7. Abnormal flow curves in real data set

Table 3. Test set attribute statistics table

Attribute	Virtual Data Set			Real Data Set
	Worm	Distributed denial of service	Alpha attacks	
Number of packets / number	18435684	78994632	5126785	124685443
Packet capacity/GB	0.751	3.19	2.47	10.21
Intrusion speed/Mbps	99	88	102	123
Number of false communication ports / number	913344	9453	2344680	942351

4.2 Adaptive Test of Network Communication

ROC curve is used to describe the adaptive capability of network communication in this paper. ROC curve is receiver operating characteristic curve, which can express the accuracy and misjudgment rate, and intuitively obtains the sensitivity of the method to be measured, that is, the adaptive ability. In order to improve the reliability of the experimental results, the other two methods of abnormal weak correlation data detection are compared with the proposed method. One of the methods is the weighted moving detection method. It can automatically adjusts itself according to situation of data flow by training the window to update timely. In view of these advantages, it can be used as a method of abnormal weak correlated data detection to ensure the continuous data flows to be focused in classification processing of abnormal detection. The experimental results of the same type are plotted in the same ROC curve, as shown in Figure 8 and Figure 9.

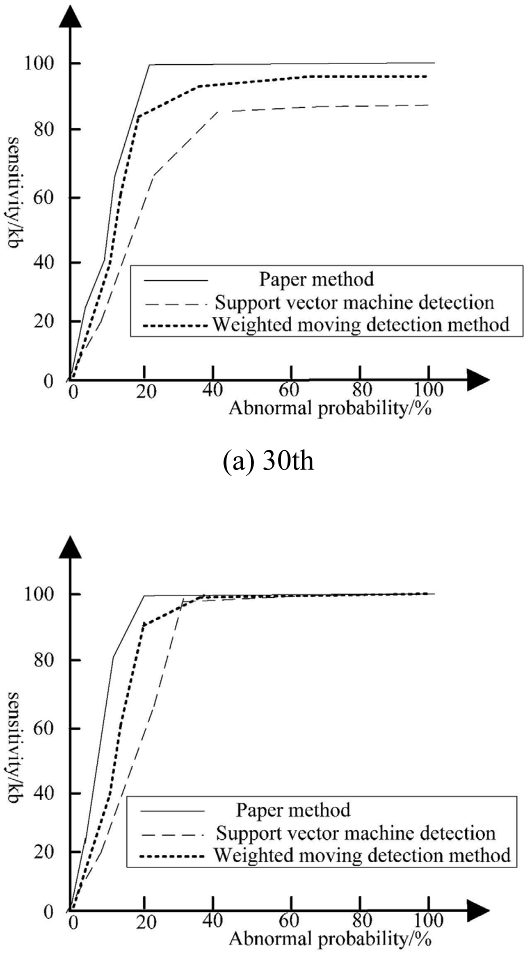


(a) Worm

(b) Distributed denial of service

(c) Alfa attack

Figure 8. Virtual data set ROC curve



(a) 30th

(b) 31st

Figure 9. Real data set ROC curve

As shown in Figure 8, because worm is the original intrusion of virtual data set, so the network communication enhancement adaptive ability of the three methods for abnormal weak correlation data detection in early detection is not very strong, however, the proposed method's network communication adaptive ability still excels than support vector machine detection and weighted mobile control detection method. In later detection, only this method has achieved 100% adaptive capacity. In Figure 8(b), because the intrusion flow of distributed denial of service is very large, the self-adaptability of the pre-detection network communication cannot reach 100% quickly, but ROC curve float ability is far less than that of Figure 8(a). The proposed method has the strongest self-improvement ability in network communication. In Figure 8(c), the intrusion flow of Alfa attack is small and at the late stage of the invasion, so the detection effect of the three methods is improved. The proposed method can still make network communication get the best adaptive ability.

It can be seen from Figure 9 that the less is abnormal network communication caused by weak correlation data, the less the three methods' adaptive ability improvement, which is a limit chain reaction. In the three methods, the proposed method has the strongest ability to improve the adaptive ability of network communication.

5 Conclusion

In this paper, the method of network communication anomaly weak correlation data detection based on feature analysis is studied, and the adaptive ability of network communication is improved effectively. Through experimental analysis, several finds are concluded:

(1) The network communication enhancement adaptive ability of the three methods for abnormal weak correlation data detection in early detection is not very strong, however, the proposed method's network communication adaptive ability still excels than support vector machine detection and weighted mobile control detection method. In later detection, only this method has achieved 100% adaptive capacity;

(2) On 30th, the proposed method's real data set ROC curve quickly reached a balance, compared with the other two methods, and it has been better than the other two methods;

(3) On 31st, although its sensitivity has a certain degree of rise with the use of support vector detection and weighted motion detection method, the use of the proposed method's sensitivity has been better than that of support vector testing and weighted motion detection method.

Although the proposed optimization method can improve the detection efficiency of abnormal weak correlation data in network communication, the detection process is more complicated. In the subsequent optimization work, we can focus on the extraction of abnormal weak correlation data, shorten the extraction time, and optimize the detection efficiency of abnormal weak correlation data.

References

[1] J. González-Nuevo, A. Lapi, M. Negrello, L. Danese, G. De Zotti, S. Amber, M. Baes, J. Bland-Hawthorn, N. Bourbe, S. Brough, R. S. Bussmann, Z.-Y. Cai, A. Cooray, S. P. Driver, L. Dunne, S. Dye, S. Eales, E. Ibar, R. Ivison, J. Liske, J. Loveday, S. Maddox, M. J. Michałowski, A. S. G. Robotham, D. Scott, M. W. L. Smith, E. Valiante, J.-Q. Xia, Herschel (a similar to.)-ATLAS/GAMA: SDSS Cross-correlation Induced by Weak Lensing, *Monthly Notices of the Royal Astronomical Society*, Vol. 442, No. 3, pp. 2680-2690, August, 2014.

[2] S. Tosi, S. Casolari, M. Colajanni, Detecting Correlation between Server Resources for System Management, *Journal of Computer & System Sciences*, Vol. 80, No. 4, pp. 821-836, June, 2014.

[3] P. Berezinski, B. Jasiul, M. Szpyrka, An Entropy-Based Network Anomaly Detection Method, *Entropy*, Vol. 17, No. 4, pp. 2367-2408, April, 2015.

[4] Z. Zhang, F. Song, P. Zhang, H.-C. Chao, Y. Zhao, A New Online Field Feature Selection Algorithm based on Streaming Data, *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-13, August, 2018. https://doi.org/10.1007/s12652-018-0959-0

[5] S. D. S. Da Silva, S. R. de Brito, N. L. Vijaykumar, C. A. J. da Rocha, M. de A. Monteiro, J. C. W. A. Costa, C. R. L. Francês, Social Network Analysis and Mining to Monitor and Identify Problems with Large-Scale Information and Communication Technology Interventions, *Plos One*, Vol. 11, No. 1, pp. e0146220, January, 2016.

[6] Y. Jiang, K. J. Kim, J. D. Gibson, R. A. Iltis, Channel Estimation and Data Detection for MIMO-OFDM Systems, *2003 GLOBECOM '03. IEEE Global Telecommunications Conference*, Vol. 2, San Francisco, CA, 2003, pp. 581-585.

[7] D. Koulakiotis, A. H. Aghvami, Data Detection Techniques for DS/CDMA Mobile Systems: A Review, *IEEE Personal Communications*, Vol. 7, No. 3, pp. 24-34, June, 2000.

[8] A. Klein, Data Detection Algorithms Specially Designed for the Downlink of CDMA Mobile Radio Systems, *1997 IEEE 47th Vehicular Technology Conference. Technology in Motion*, Vol. 1, Phoenix, AZ, 1997, pp. 203-207.

[9] C. Cozzo, B. L. Hughes, Joint Channel Estimation and Data Detection in Space-time Communications, *IEEE Transactions on Communications*, Vol. 51, No. 8, pp. 1266-1270, August, 2003.

[10] E. S. A. Dahshan, H. M. Mohsen, K. Revett, A.-B. M. Salem, Computer-aided Diagnosis of Human Brain Tumor through MRI: A Survey and A New Algorithm, *Expert Systems with Applications*, Vol. 41, No. 11, pp. 5526-5545, September, 2014.

[11] A. Glowacz, A. Glowacz, P. Korohoda, Recognition of Monochrome Thermal Images of Synchronous Motor with the Application of Binarization and Nearest Mean Classifier, *Archives of Metallurgy & Materials*, Vol. 59, No. 1, pp. 31-34, March, 2014.

[12] A. Karim, R. B. Salleh, M. Shiraz, S. A. A. Shah, I. Awan, N. B. Anuar, Botnet Detection Techniques: Review, Future Trends, and Issues, *Frontiers of Information Technology & Electronic Engineering*, Vol. 15, No. 11, pp. 943-983, November, 2014.

[13] H. Lin, W. Tov, L. Qiu, Emotional Disclosure on Social Networking Sites: The Role of Network Structure and Psychological Needs, *Computers in Human Behavior*, Vol. 41, No. 41, pp. 342-350, December, 2014.

[14] C. Bretti, R. M. Cigala, C. D. Stefano, G. Lando, S. Sammartano, Thermodynamics for Proton Binding of Pyridine in Different Ionic Media at Different Temperatures, *Journal of Chemical & Engineering Data*, Vol. 59, No. 1, pp. 143-156, January, 2014.

[15] Z. Ghassemlooy, S. Arnon, M. Uysal, Z. Xu, J. Cheng, Emerging Optical Wireless Communications-Advances and Challenges, *IEEE Journal on Selected Areas in Communications*, Vol. 33, No. 9, pp. 1738-1749, September, 2015.

[16] A. Zoran, R. Shilkrot, S. Nanyakkara, J. Paradiso, The Hybrid Artisans: A Case Study in Smart Tools, *ACM Transactions on Computer-Human Interaction (TOCHI)*, Vol. 21, No. 3, pp. 1-29, June, 2014.

[17] B. Tilahun, F. Fritz, Comprehensive Evaluation of Electronic Medical Record System Use and User Satisfaction at Five Low-Resource Setting Hospitals in Ethiopia, *Journal of Medical Internet Research*, Vol. 3, No. 2, pp. e22, April-June, 2015.

[18] D. A. Basuil, D. K. Datta, Effects of Industry- and Region-Specific Acquisition Experience on Value Creation in Cross-Border Acquisitions: The Moderating Role of Cultural Similarity, *Journal of Management Studies*, Vol. 52, No. 6, pp. 766-795, September, 2015.

[19] R. J. Santos, J. Bernardino, M. Vieira, Approaches and Challenges in Database Intrusion Detection, *ACM Sigmod Record*, Vol. 43, No. 3, pp. 36-47, September, 2014.

[20] V. Rashtchi, M. Nourazar, A Multiprocessor Nios II Implementation of Duffing Oscillator Array For Weak Signal Detection, *Journal of Circuits Systems & Computers*, Vol. 23, No. 4, pp. 3-21, April, 2014.

[21] A. M. Ortiz, T. Olivares, F. Royo, N. Crespi, L. Orozco-Barbosa, Smart Cross-layer Protocol Integration for Efficient Wireless Communications, *International Journal of Ad Hoc and Ubiquitous Computing*, Vol. 20, No. 3, pp. 148-158, December, 2015.

[22] B. Ju, T. Jin, Incorporating Nonparametric Statistics into Delphi Studies in Library and Information Science, *Information Research an International Electronic Journal*, Vol. 18, No. 3, pp. 1-11, September, 2013.

[23] V. Paraušić, D. Cvijanović, B. Mihailović, K. Veljković, Correlation between the State of Cluster Development and National Competitiveness in the Global Competitiveness Report of the World Economic Forum 2012-2013, *Economic Research-Ekonomska Istraživanja*, Vol. 27, No. 1, pp. 662-672, November, 2014.

[24] O. Dibie, T. Sumner, Using Weak Ties to Understand the Resource Usage and Sharing Patterns of a Professional Learning Community, *Social Network Analysis and Mining*, Vol. 6, No. 1, pp. 27-37, December, 2016.

Biographies

Shufen Liu is a professor in College of Computer Science and Technology of Jilin University. She has been conducting research for many years on computer network and security technology, computer supported cooperative work, computer simulation technology, software programming method based on model-driven, etc.

Xuejun Ma is a Ph.D. candidate in College of Computer Science and Technology of Jilin University. Her research area covers software engineering, computer network and cooperative computing.

Zhixiang HOU is a Ph.D. and full professor of Changsha University of Science and technology. He research area covers intelligent control and optimization, computer network.