A Dynamic Network Anomaly Detection Method Based on Trend Analysis

Tong Sun, Yan Liu, Jing Chen
China State Key Laboratory of Mathematical Engineering and Advanced Computing
Zhengzhou 450002, China
e-mail: ms_liuyan@aliyun.com

***Abstract*—Detecting abnormal behavior during network evolution is an important and challenging data analysis task at present, it is named as dynamic network anomaly detection in this paper. The network abnormal behavior differs from that of normal behavior, the probability of occurrence stays relatively low but may cause serious damages once happened. This paper takes the topological structure of the network as the research object and identifies the network anomaly through the change of network structure. Based on Cox-stuart test, we put forward a new type of method to detect dynamic anomaly. This method refers to an alarm of monitoring the trend change of the network structure parameters. Finally, an experiment was carried out in the real dynamic network-Enron Email Network, which verified that the dynamic network anomaly detection method proposed in this paper can effectively detect the network anomaly behavior.**

Keywords-dynamic network; anomaly detection; trend detection

I. INTRODUCTION

With the development of information technology, social media including Twitter, email and Weibo have gradually matured. People communicate and send messages on the Internet generally. Therefore, a massive social network which will evolve over time has been structured in the fictitious cyberspace among people and constitutes a dynamic network [1]. Except for social network, route and forward network of computer field and molecular structure network of biological field also can expand into dynamic network in the time domain. Network members' abnormal behaviors may cause abnormal changes of network structure, which is referred as network anomalous evolvement. If network anomalous evolvement can be discovered in time, there's more opportunities for operators to deal with abnormal behaviors to reduce unnecessary loss, which is significant to comprehend network developing trends, prevent socially organized abnormal events and detect network attack behaviors.

Trend-detection aims at understanding the existence of increasing and decreasing tendency in data sequence, which can be applied to dynamic network to know whether there's a trend change in network or not. Network structure parameters won't have nonrandom changes when the network is stable. Therefore, if trend changes happen, network is developing towards some direction probably for some abnormal events. We try to identify network trend changes based on this thought to predict or detect abnormal events. Cox-stuart test could judge the overall trend of a data sequence but cannot identify the trend of the sub-data segment. The traditional Cox-stuart test is inappropriate because change trends of the real network is not unidirectional in most cases. Based on trend-detection theory of Cox-stuart test, this paper adjusted detection process and designed a new anomaly detection method applying variable-size sliding window mechanism. After first test data trend in the window, it will combine the outcomes based on some strategy to find all the data segment embracing trend changes. The abnormal behaviors exist the corresponding time slot possibly.

The paper is organized as follows. Section II introduces the related work of dynamic network anomaly detection. In Section III the analysis of the problem and related definitions are illustrated. Section IV reports the selection of network parameters and the dynamic network anomaly detection method proposed in this paper. Section V is the experimental part. Finally, section VI concludes the paper and puts forward the future prospect.

II. RELATED WORK

Dynamic network anomaly detection, as a branch of the field of dynamic network analysis, has a certain amount of related research work, most of them called anomaly detection or outlier detection. According to the main research object, dynamic network anomaly detection can be divided into two categories, one is for the behavior pattern of the network members , the other is for the network topology. According to the need to pre-construct the detection model, the anomaly detection method can also be divided into supervised, unsupervised and semi-supervised three modes [2]

In the study of anomaly detection of network member behavior patterns. Gupta *et al.* [3] used the method of machine learning to select the members of the normal evolution in the network as the training set to learn the characteristics of the normal evolution of the members, and then use these characteristics to detect abnormal members during the evolution. Wei *et al.* [4] used a regression analysis method to establish a regression model based on the historical activity of the network members to predict their future behavior. If the difference between the predicted value and the actual observation value exceeds the set threshold, the membership is judged to be abnormally evolved. Yasami *et al.* [5] modeled the evolutionary characteristics of network members using the Infinite Factor Hidden Markov Model (IFHMM), and the abnormal behavior is those with low probability of evolution. Erfani *et al.* [6] combined the depth

978-1-5090-6352-9/17/$31.00 ©2017 IEEE

belief network (DBNS) with one-class SVM to detect anomalies in networks. DBNs extract the underlying characteristics of network members to train one-class SVM classifiers. The resulting hyperplane can separate the normal members from the exception members.

In the study of anomaly detection of network topology, McCulloh *et al.* [7] proposed to use the method of cumulative sum control chart (CUSUM) in Statistical Process Control (SPC) to detect the structure parameters of the network in real time, and it could alarm the anomaly when the cumulative sum exceeds the set threshold. Anomalous time points can be traced back from the statistics of CUSUM. The method has been applied in the dynamic network analysis software ORA [8] developed by Carnegie Mellon University. ORA detects the network anomaly from the network parameters such as network density, intermediation and tightness. The disadvantage of the method is that the detected parameters must obey the normal distribution, which limits the application of the method to a certain extent. Rizk *et al.* [9] proposed a clustering-based anomaly detection algorithm. In large clusters, k-medoids clustering techniques are used to optimize the computational distance between points, which improves the efficiency of the algorithm.

The above two kinds of dynamic network anomaly detection method of different angles, each has its own advantages and disadvantages. In reality, the heterogeneity and dynamic of the members in the network are difficult to describe. Therefore, the model often has limitations on the evolution of the members in the network. It is also inefficient to model each member in a large-scale network analysis task. At present, the method of anomaly detection through the network topology is more stringent to the distribution of the network structure parameters, which leads to the poor effect of this method when applied to some actual dynamic networks.

III. Problem Analysis and Related Definitions

Using the form of graphs to represent the network can clearly describe the relationship between network entities [10]. For example, in the mail network, each node represents an e-mail address, one side between the two nodes on behalf of a message sent, while the weight of the two representatives of the frequencies of communication. In order to express the dynamics of the network, the network can be divided according to the time slice [11]. Each time slice corresponds to a network graph, and a dynamic network is represented by a set of network graphs.

Definition 1. Dynamic network: In this paper, it refers to the network with the network topology changes over time, which reflected as nodes and edges in the network graph appear or disappear over time. A dynamic network containing n time slices is represented as $G=\{G_1,G_2,...,G_t,G_{t+1},...,G_n\}$, where the t th time slice network is $G_t=(V_t,E_t)$. V_t is the set of vertices in the network, and E_t is the edge set representing the relationship between the vertices. $G_t=(V_t,E_t,W_t)$ when the network is a weighted network and W_t is the weights set.

Definition 2. Network anomaly: In this paper, it refers to the abnormal changes in the process of network evolution. For example, a significant mutation or a inconspicuous trend of change in the structure of the network.

In general, we believe that the network in the normal evolution process presents a relatively stable state, which we call network steady state [12].When the network is in steady state, the structural parameters of the network only have random fluctuation instead of significant mutation or trend changes. When mutations or trend changes occur, we believe that the network is abnormal in the evolution process, this "abnormal evolution" is called network anomalies.

Compared to the mutations of the network, the trend anomalies are more subtle, so this article mainly studies such anomalies. Network anomalies can be identified by the trend of network topology changes. For example, when the number of nodes in a network gradually increases, the network shows a trend of growth, which is a network anomaly. We need to find out all the time period, in which the number of nodes in the network has an increasing trend. In addition to the number of nodes, network tightness, center potential and other parameters of the trend changes are all network anomalies, need to be detected. Therefore, the key to dynamic network anomaly detection is to identify the trend of network structure parameters. Therefore, the anomaly detection algorithm needs to be able to detect the trend changes of various network structure parameters and does not depend on the trend structure. At the same time, it is necessary for the method to quickly detect the occurrence of a trend change and to be able to locate the start time and the end time of the trend change section, and try not to omit any trend change section.

IV. Dynamic Network Anomaly Detection Method

A. Selection of Network Structure Parameters

We use the network topology for abnormal evolution detection, different network structure parameters reflect the different structural features of the network. Because it is difficult to list all the network structure parameters, thus we choose five parameters from the aspect of network scale and the network connection to analyze the network evolution process, and the network is expressed as the undirected weighted graph. We examine the changes in the selected parameters over time, as a basis for detecting network anomalies.

Parameter 1: nodes count

Nodes count represents the number of members in the network.

Parameter 2: weights sum

Weights sum represents the total amount of communication between nodes in the network.

Parameter 3: average path length

The average path length reflects the difficulty of communication between any two nodes in the network.

Parameter 4: average clustering coefficient

This parameter reflects the clustering characteristics of the whole network.

Parameter 5: network centralization

This parameter is used to measure the network's central tendency. The closer the network centralization is to 1 indicates that the network tends to exhibit a star structure, which has a stronger concentration trend.

B. *A Dynamic Network Anomaly Detection Method Based on Cox-stuart Test Using Variable-Size Sliding Window Mechanism*

Cox-stuart test is a method of data trend detection, the theoretical basis is the symbol test. Since the Cox-stuart test method does not depend on the trend structure, it overcomes the limitations that the CUSUM needs to satisfy the normal distribution for the detection data. In the real dynamic network, the trend of network change is not necessarily a single direction of growth or reduction, in many cases will be the two alternately. In order to detect the trendy part in the non-unidirectional data sequence, we first use the variable-size sliding window mechanism to divide the data, and then detect the trend of the data sequence within the window. Finally, a certain strategy is used to combine the test results in the window to get all the data segment embracing trend changes, and these data segments are marked as abnormal evolution stage. Some of the parameters in this method can be adjusted to meet the actual detection requirements, the detection process all automatically. The main two parts of the detection process: variable-size sliding window trend detection and the results combination are described below.

1) Variable-size sliding window trend detection

Variable-size sliding window is a sliding window that can be changed in size, which is used to divide the sequence of data to be detected. Before the next slide operation, the window starts at the same position, and the window size gradually increases from the minimum to the maximum. Variable size windows can more accurately detect varying degrees of trend change.

Minimum window: The minimum size of the variable-size sliding window, recorded as $L_{\min}$.

Maximum window: The maximum size of the variable-size sliding window, recorded as $L_{\max}$.

Significance level: A hypothesis test used in trend detection, which refers to the probability or risk of rejecting the null hypothesis when it is correct. Indicated by α .

The trend of the data in the window is detected by Cox-stuart test. We define the null hypothesis H_0 means that the network without trend changes, alternative hypothesis H_1 indicates the network has a trend of change, the trend of change is divided into the trend of growth or decrease. Cox-stuart test divides the data sequence into the previous and subsequent parts, taking x_i and x_{i+c} in the previous and subsequent parts of the data sequence $x_1, x_2, ..., x_n$ and making the difference $(x_{i+c} - x_i)$, where $c = \begin{cases} n/2 & n \text{ is even} \\ (n+1)/2 & n \text{ is odd} \end{cases}$. When n is even, there are $n' = c$ pairs. When n is odd, there are $n' = c$-1 pairs. Let S^+ be the number of positive numbers after calculation, and S^- be the number of negative numbers. When H_0 is true, the variable $K = \min(S^+, S^-)$ obeys the binomial distribution $b(n', 0.5)$ of the parameter n' , 0.5, and n' is the number of pairs that do not contain a difference of zero. s^+ and s^- represent the value of the test statistic calculated from the sample, let $k = \min(s^+, s^-)$. Using the P-value method to carry out the hypothesis test, P-value calculation formula is $P(K \le k) = \frac{1}{2^{n'}} \sum_{i=0}^{k} \binom{n'}{i}$. The test method is shown in Table I.

TABLE I. COX-STUART TEST P-VALUE TEST METHOD

	Test statistic	P-value
H_0 : no increasing trend, H_1 : have a increasing trend	$K = S^+$	$P(K < k)$
H_0 : no decreasing trend, H_1 : have a decreasing trend	$K = S^-$	$P(K < k)$
H_0 : no trend, H_1 : have a increasing or decreasing trend	$K = \min(S^+, S^-)$	$2P(K < k)$

The significance level α is 0.05 or less, and when the calculated P-value is less than α , the null hypothesis H_0 is rejected, and the data sequence is considered to have a trend changes.

Before detecting the trend of data sequence in the window, we need to set the range of the window size. The minimum size of the window $L_{\min}$ is determined by the significance level α . When the data in the window is strictly incremented or decremented, the resulting P-value is the smallest. Let $L_{\min}$ be minimized while ensuring the minimum P value <= α . For example, let α = 0.05, then the minimum window size $L_{\min}$ is set to 10. When the window of the 10 data composition of the five pairs of difference results are all positive or negative, $P = \frac{1}{2^5} = 0.03125 < 0.05$, and any less than the size of the window can not meet the premise of $p_{\min} \le 0.05$. The maximum size of the window $L_{\max}$ is set according to the detection requirements. It is important to note that if the window size is too large, the trend of some data segments in the middle may be missed.

The initial size of the variable-size sliding window is set to the minimum window, and the Cox-stuart test is executed on the data in the window. If the resulting P-value is less than α , the data in the window is marked as a having a trend

change. Add a time slice to the window, continue to execute Cox-stuart test, if the P-value is less than α , do the trend mark. At the same time add a new detection window, the initial position of the window moves forward a time slice. When a new time slice arrives, it is added to all existing detection windows and a new detection window is created. The cox-stuart test is executed for the data sequence in each window. When the window is increased to the maximum size, the detection window has been detected and then discarded. This operation is continually executed until all time slices have been calculated. The detection process is shown in Fig. 1.

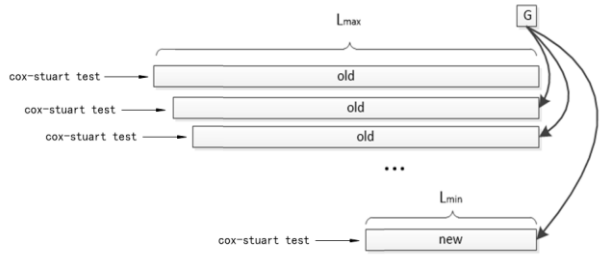

Figure 1. Variable-size sliding window detection process.

2) Results combination and determine the alarm time point

Trend starting point: The trend starting point is the start time point of the trend change. If the data in the current detection window is detected with a trend change, the starting position of the window is the trend starting point.

Trend discovery time point: The trend discovery time point is the current time point when the trend change is detected. If the data in the current detection window is detected with a trend change, the end position of the window is the trend discovery time point.

The work of this step is to combine all the trend change segments detected in the previous step with overlapped parts into one, and determine the earliest trend discovery time point of the combined segment. These earliest trend discovery time points are the alarm time points, which is the final output of the algorithm. Two segments with overlapping parts are combined as the following method: Assume that it is detected that both segment L_i (the starting time is t_{i1} , and the finishing time is t_{i2}) and L_j (the starting time is t_{j1} , and the finishing time is t_{j2}) are increasing trend and they have overlapping part, the starting time of segment after being combined is $\min(t_{i1}, t_{j1})$, and the finishing time is $\max(t_{i2}, t_{j2})$, and find the earliest trend discovery time point of the segment that is combined. When conducting combined operation, increasing trend and decreasing trend should be calculated separately, and combined result may exist that some segments are labeled as being increased and decreased, which is reasonable.

The dynamic network anomaly detection algorithm pseudocode is shown in algorithm 1.

Algorithm 1: Dynamic network anomaly detection algorithm

Input: A dynamic network $G = \{G_1, G_2, ..., G_n\}$, significance level α , network parameters X .

Output: All trend parts and the alarm time point for each trend part.

Preprocessing stage

Initialize: window size $L_{\min}$, $L_{\max}$, $W_1 = \{G_1, ...G_{L_{\min}}\}$.

Detention stage

1. while $i \le n$
2. add a new network G_i to all existing windows W
3. if size of $W > L_{\max}$
4. discard the window W
5. create a new window W (window start position moves forward a time slice, window size $= L_{\min}$)
6. for all existing window W , apply cox-stuart test
7. if P-value $\le \alpha$
8. mark the trends of W and all trend discovery time point
9. $i \leftarrow i+1$
10. for all segments marked with trend changes
11. if the two segments have overlapping parts
12. merge them into one and mark the alarm time point

The algorithm is intended to find more time periods where the corresponding network parameters have a trend change. The computational cost of the algorithm is mainly for the calculation of the network parameters of each time slice and the trend detection of each window. In a dynamic network with N time slices, suppose $N >>$ (far greater than) $L_{\max}$. Let K_i be the computational complexity of the i -th network parameter, which is related to the network size. C_{avg} is the average computational complexity of the Cox-stuart test in each window, the time complexity of the algorithm can be expressed as $K_i N + C_{avg}(L_{\max} - L_{\min})N$. It can be seen that the larger the network size, the more time slices are divided, the higher the computational complexity of the algorithm.

V. EXPERIMENTS

A. Experimental Data

This article uses the Enron e-mail data set to build a mail network for dynamic network anomaly detection. Enron's mail data set is Enron's (formerly one of the world's largest integrated gas and power companies, and is the number one natural gas and power wholesaler in North America) 150 senior executives of the e-mail. It has been publicly available

by the US Federal Energy Regulatory Commission and is currently available online [13].

Data preprocessing: Extracts the address and the sending time of the sender and receiver in the mail record, used to build the mail network. The time slice size is one week, with a week as a time slice unit mainly taking into account the cyclical nature of the mail sending behavior, that is, working days mail more rest days less. A mail network snapshot consists of a week of mail traffic records. The starting position of the current time slice moves forward for 1 day to form the next time slice network, and the two consecutive time slices have a 6-day coincidence. The test data ranges from July 1, 2001 to December 31, 2001, and the resulting time slice network contains 178 time slices.

B. Experimental Designs

In order to verify the validity of this method, we marked some important events and their occurrence time of Enron in the second half of 2001 [14]. We define these events as "abnormal events", as shown in Table II, and define the time of occurrence of abnormal events 7 days before and after as the effective detection interval. Then we detect the trend of the five network structure parameters mentioned in the fourth chapter in the process of network evolution, and then get a series of trend change period corresponding to each parameter and get the trend starting time point and the alarm time point. We hope that the alarm time point of the abnormal event in the effective detection interval, so as to be able to effectively prevent or detect abnormal events. The alarm time point of the anomaly detection has the following three cases: (1) 1 to 7 days before the abnormal event, we thought that the abnormal event was predicted successfully. (2) 0 to 7 days after the exception occurred, we thought that the abnormal event was detected successfully. (3) Not in the effective detection range, we believe that the detection of abnormal failure. [15] The ideal anomaly detection algorithm should not miss the real error events and minimize the error alarm. Therefore, we use the abnormal event coverage, alarm accuracy and anomaly detection ability of three indicators to evaluate the performance of the algorithm.

Abnormal event coverage is defined as

$$P_C = \frac{\text{Abnormal events identified by the algorithm}}{\text{All abnormal events}} \tag{1}$$

Alarm accuracy is defined as

$$P_T = \frac{\text{Correct number of alarms}}{\text{Total number of alarms}} \tag{2}$$

Anomaly detection ability is defined as

$$D_C = P_C \times P_T \tag{3}$$

The events that occur near the trend start point, such as a company's decision, are likely to be the cause of the abnormal change of the network. Find these events and combine them with the environment to do analysis, we can get more useful information. But because of the lack of credible evidence, so this paper is no longer looking for these events, no longer on whether it is the cause of abnormal network changes for further analysis.

TABLE II. ENRON'S IMPORTANT EVENTS.

Time, Time slice	Event
2001/8/14，39	Skilling announced his resignation as CEO after half a year. Skilling served as president and chief operating officer for a long time and then promoted to chief executive officer.
2001/10/16，102	Enron announced that they had restated their financial statements for the years 1997 to 2000 to correct accounting irregularities.
2001/10/22，108	The Securities and Exchange Commission conducted a survey of potential conflicts of interest between Enron and its directors and their special partnerships.
2001/11/8，125	Enron restated its financial for the prior four years to consolidate partnership arrangements retroactively. Earnings from 1997 to 2000 declined by $591 million, and debt for 2000 increased by $658 million.
2001/11/9，126	Enron entered merger agreement with Dynegy.
2001/11/28，145	Dynegy pulled out of the proposed merger.
2001/12/2，149	Enron filed for bankruptcy in New York and simultaneously sued Dynegy for breach of contract.

C. Experimental Results

The minimum detection window $L_{\min}$ in this experiment is set to 10, the maximum detection window $L_{\min}$ is set to 30, the significance level α is 0.05. We record all the alarm time for the above five network structure parameters to be checked, and keep the alarm records (in time slices) from 2001/8/1 to 2001/12/2, that is the 26th time to the 149 time slice, as shown in Table III. The summary results are all alarm time points for the five network structure parameters. Fig. 2 shows the results of the trend of each network

structure parameter. In each graph, the polyline is the case where the parameter changes over time, and the intersection of the straight line perpendicular to the time axis and the time axis is the alarm time point.

TABLE III. NETWORK ABNORMAL ALARM TIME POINT.

Parameter / α	Parameter1	Parameter 2	Parameter 3	Parameter 4	Parameter 5	Sum results
0.05	41 122	41 96 122 149	39	62 97 105	40 121	39 40 41 62 96 97 105 121 122 149

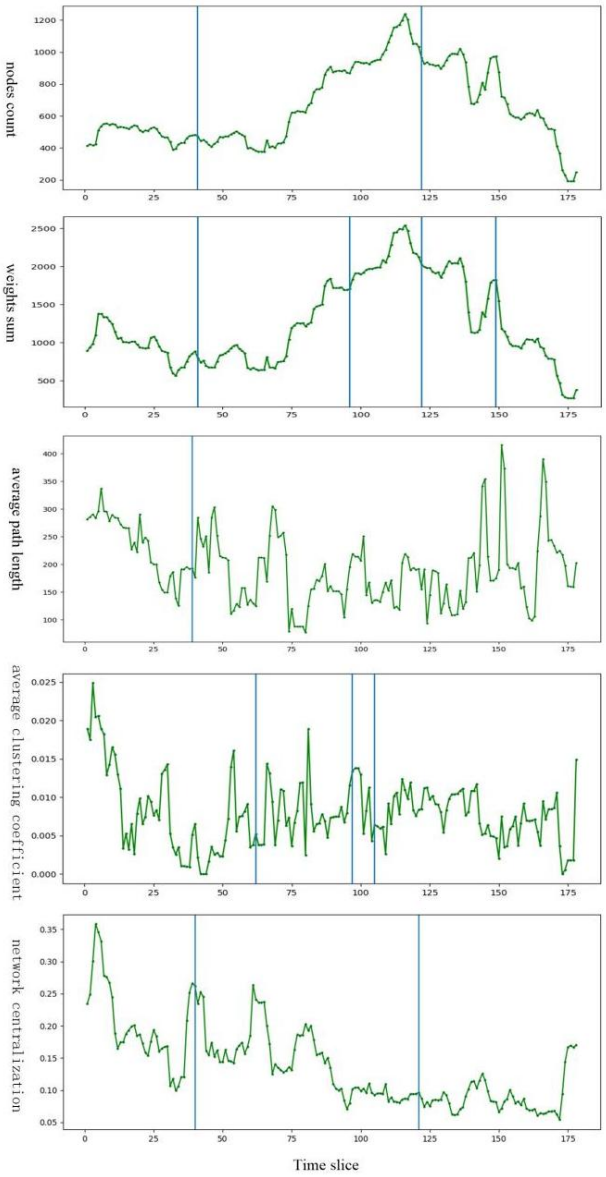

Figure 2. Trend detection results.

We examined the first abnormal event (39th time slice), before Skilling announced that he would resign from the CEO post in six months, the parameters 1, 2, 3 had a trend of change and issued an abnormal alarm at 39 and 41 time slice. It can be seen that Enron's development has become unstable before Skilling makes the decision, and this anomaly is captured by our algorithm in time. Before the second abnormal event (102th time slice), parameters 2, 4, respectively, in the 96,97 time slice issued an abnormal alarm. Indicating that the company has been unstable before Enron's decision to re-examine the finance. In Fig. 3, the dot on the horizontal axis indicates the point of occurrence of the abnormal event, and the intersection of the horizontal axis and the straight line perpendicular to the horizontal axis is the alarm time point. It can be seen more intuitively that the alarm time point is basically concentrated near the abnormal event, indicating that the method can make effective prevention and detection of abnormal events.

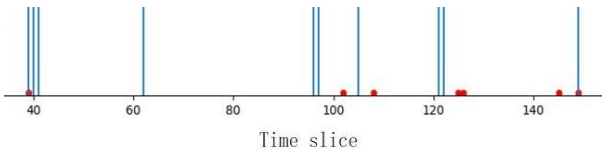

Figure 3. Abnormal event occurrence time point and alarm time point.

Unsuccessfully predicted events, events that were not successfully predicted or detected. Predict network anomalies, predict and detect network anomalies, their corresponding P_C and P_T are shown in Table IV.

TABLE IV. NETWORK ANOMALY TEST RESULTS.

Unsuccessfully predicted events	P_C	P_T
39, 145, 149	0.571	0.500
Unsuccessfully predicted or detected events	P_C	P_T
Null	1.000	0.900

The above-mentioned detection range contains 124 time slices, and there are 39 time slices in the correct prediction range of abnormal events, and there are 64 time slices in the correct prediction or detection range. In the case of random, the expected value of the alarm accuracy P_T for predicting the abnormality is $E(P_T) = \frac{39}{124} = 0.315$, and the expected

value of the alarm accuracy P_T for predicting or detecting the abnormality is $E(P_T) = \frac{64}{124} = 0.516$. The summary results have a total of 10 alarm time points, and we use the random sampling method to sample 10 time slices in 26 to 149 time slice as the alarm time points to estimate the abnormal event coverage P_C in random case. After 1000 replicates, the mean P_C of the predicted abnormality was 0.387, and the mean of P_C for predicting or detecting abnormalities was 0.682. The results of our algorithm and the random results are shown in Table V.

TABLE V. COMPARISON OF RESULTS.

	prediction			prediction or detection		
	P_C	P_T	D_C	P_C	P_T	D_C
Our algorithm	0.571	0.500	0.286	1.000	0.900	0.900
Random result	0.387	0.315	0.122	0.682	0.516	0.352
Percentage improved	48%	59%	134%	47%	74%	156%

The results show that the three indicators P_C , P_T and D_C are significantly improved in both the prediction as well as the prediction or detection of the anomaly, and the alarm time point has practical significance. The experiment shows that it is feasible to carry out network anomaly detection by using the change of network structure.

VI. CONCLUSION

This paper presents a dynamic network anomaly detection method based on trend analysis. A total of five commonly used network structure parameters were selected for trend change detection, as far as possible to identify more changes in the network. Considering the trend of network mostly not unidirectional, the original Cox-stuart trend detection algorithm has been improved by us, adding a variable sliding window strategy, which can detect the trend of the sub-data segment in the overall data.

Finally, we use the dynamic mail network constructed by Enron e-mail data set to prove that the network anomaly detection algorithm proposed in this paper can effectively predict and identify the abnormal behavior in the network. The next step is to test the effectiveness of this method on more real dynamic networks and to improve our approach to high-dimensional datasets in order to be able to detect network anomalous behavior in multi-attribute, multi-relationship and high-dimensional complex networks [16].

ACKNOWLEDGMENT

The authors thank Junyong Luo and Meijuan Yin for their suggestions and assistance in the course of this research. This research was supported by the National Natural Science Foundation of China (Grant No. 61309007, U1636219) and the National Key R&D Program of China (Grant No. 2016YFB0801303, 2016QY01W0105).

REFERENCES

[1] Carley KM. Dynamic Network Analysis: Alphascript Publishing; 2003.

[2] Zhang Y, Meratnia N, Havinga PJM. A taxonomy framework for unsupervised outlier detection techniques for multi-type data sets[J].PIK - Praxis der Informationsverarbeitung und Kommunikation.2017

[3] Gupta M, Gao J, Sun Y, Han J, editors. Integrating community matching and outlier detection for mining evolutionary community outliers.2012.

[4] Wei W, Carley K M. Measuring Temporal Patterns in Dynamic Social Networks[J]. Acm Transactions on Knowledge Discovery from Data, 2015, 10(1):1-27.

[5] Yasami Y, Safaei F. A statistical infinite feature cascade-based approach to anomaly detection for dynamic social networks[M]. Elsevier Science Publishers B. V. 2017.

[6] Erfani S M, Rajasegarar S, Karunasekera S, et al. High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning[J]. Pattern Recognition, 2016, 58(C):121-134.

[7] Mcculloh I A, Carley K M. Social Network Change Detection[J]. 2016.

[8] Carley K M. ORA: A Toolkit for Dynamic Network Analysis and Visualization[M]. Springer New York, 2014.

[9] Rizk H, Elgokhy S, Sarhan A. A hybrid outlier detection algorithm based on partitioning clustering and density measures[C]// Tenth International Conference on Computer Engineering & Systems. IEEE, 2016:175-181.

[10] Hagberg A, Schult D, Swart P. Exploring network structure, dynamics, and function[C]// Scipy. 2008:11--15.

[11] Akoglu L, Tong H, Koutra D. Graph based anomaly detection and description: a survey[J]. Data Mining & Knowledge Discovery, 2014, 29(3):626-688.

[12] Velizcuba A, Aguilar B, Hinkelmann F, et al. Steady state analysis of Boolean molecular network models via model reduction and computational algebra[J]. Bmc Bioinformatics, 2014, 15(1):1-8.

[13] Priebe C E, Conroy J M, Marchette D J, et al. Scan Statistics on Enron Graphs[J]. Computational & Mathematical Organization Theory, 2005, 11(3):229-247.

[14] Healy P M, Palepu K G. The Fall of Enron[J]. Journal of Economic Perspectives, 2003, 17(2):3-26.

[15] Zheng P, Qi Y, Zhou Y, et al. An Automatic Framework for Detecting and Characterizing Performance Degradation of Software Systems[J]. IEEE Transactions on Reliability, 2014, 63(4):927-943.

[16] Yu L, Li Y, Jia J. Research on outlier detection for high dimensional data stream[C]// International Conference on Artificial Intelligence and Engineering Applications. 2016.