Anomaly Detection and Association Analysis of Traffic in Communication Network Based on Behavior Analysis

Jing Wenlong, Fang Limei, Wang Liujing

Zhejiang Tobacco industry co. LTD, Zhejiang, China, 31500

Keywords: Communication network; Detection; Behavior analysis

Abstract: Nowadays, with the rapid development of communication network technology, the structure of communication network is becoming more and more complex. In order to avoid users being attacked from the network, it is necessary to detect abnormal traffic behavior in the network and prevent possible network attacks in time. This paper expounds the definition of traffic anomaly detection and correlation analysis, studies the problem of traffic anomaly detection in communication network, and analyses the correlation of abnormal behavior.

1. Introduction

With the rapid development of information and communication technology, the structure of communication network is becoming more and more complex. The openness of communication network itself and the openness of its bearer protocol bring convenience to people, but also bring great hidden dangers to network security. In order to ensure the safe and efficient operation of the network, reduce the harm of various abnormal events to the normal business of the communication network, and construct a trusted communication network environment, it is necessary to analyze the operation of the communication network accurately, detect the abnormal traffic behavior of the communication network, and find out the hidden security risks in the operation of the network, so as to formulate corresponding network strategies to respond to the potential problems. Traffic anomaly detection and correlation analysis are the basis to ensure network security. Therefore, research on traffic anomaly detection and correlation analysis in communication network can better promote the development of network communication technology.

2. Flow anomaly detection and correlation analysis

2.1 Definition of traffic anomaly detection and correlation analysis

Network anomaly detection is based on the normal behavior of the objects and users or the normal use of resources to determine whether an anomaly occurs. It does not depend on whether the specific behavior appears to detect, and has strong versatility. Network association analysis combines the traffic characteristic parameters at different levels and different space-time locations. By analysing the relationship between the traffic characteristic parameters and the characteristic parameters, the root causes of abnormal network traffic behavior are found, and the causal relationship between the steps of network abnormal events is found. Redundant alarm information is mined to make up for the deficiency of traffic anomaly detection.

2.2 Flow anomaly detection and correlation analysis steps

The basic steps of network traffic anomaly detection include traffic data collection, feature parameter extraction, normal behavior model construction, anomaly detection and result output and model updating, as shown in Figure 1 below.

  DOI: 10.25236/isrme.2019.130

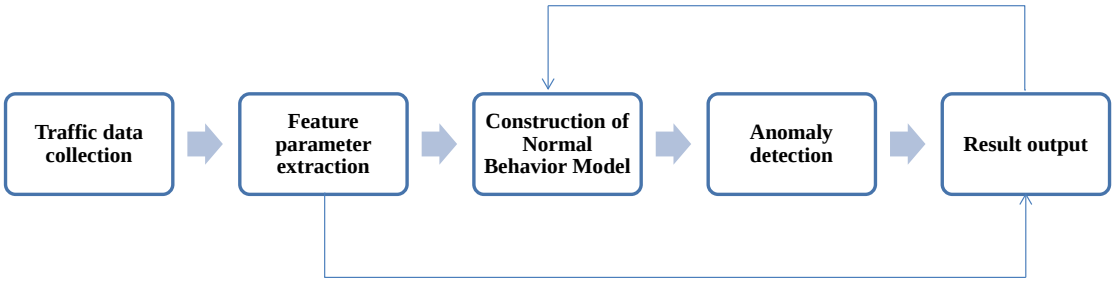

Figure1. Flow anomaly detection and correlation analysis steps

Association data mining in association analysis usually uses a variety of data mining or machine learning methods to analyze the relationship between network traffic behavior, traffic characteristic parameters, traffic behavior and its corresponding characteristic parameters, and to establish candidate sets of association rules.

3. Traffic anomaly detection in communication networks based on behavior analysis

Traditional traffic analysis methods generally have high false alarm rate and false alarm rate, and neglect detailed information. Traffic anomaly detection based on behavior analysis can overcome the above problems, which is of great significance to the safe and efficient operation of the network.

3.1 Anomaly detection based on time series graph

In the time sequence diagram, the abnormal behavior of communication network traffic will be expressed as abnormal subgraph pattern. By mining these subgraphs, anomaly detection can be carried out accurately. When anomaly detection is based on this system, it is necessary to construct logical topology time series diagram first. Secondly, mining frequent closed subgraphs in column graphs and selecting exposure patterns are needed to generate anomaly rules. Finally, the system can determine the time and space location of the abnormal occurrence according to the rules. Thus, it can accurately and completely describe the behavior characteristics of network anomaly detection.

3.2 Traffic anomaly detection based on behavior analysis

Different from other anomaly detection methods, traffic anomaly detection based on behavior analysis can discover anomalous behavior patterns by understanding, analyzing and modeling network traffic behavior characteristics, mining the potential relationship between behavior characteristics. Choosing efficient fine-grained network behavior characteristic parameters ensures the real-time performance of behavior analysis. Based on abnormal traffic behavior, a subspace method is used to decompose the high-dimensional traffic behavior characteristic parameter space into normal subspace and abnormal subspace, and anomalies are detected by the temporal correlation of time series representing normal behavior.

4. Distributed traffic anomaly detection in communication networks

With the increasing complexity of network structure, the detection of abnormal behavior of distributed traffic has become an important means of effective network management. Based on the real-time detection results, network administrators can realize a more comprehensive understanding of the whole network and make the best response to emergencies. Based on link traffic, the abnormal behavior of network distributed traffic is studied, and the abnormal behavior of network distributed traffic is detected.

4.1 Distributed traffic abnormal behavior detection based on traffic characteristic

Existing methods for detecting distributed traffic anomalies cannot distinguish between distributed traffic anomalies caused by the same cause and independent traffic anomalies. Distributed traffic anomaly detection in communication networks based on traffic characteristics

analysis. Using the traffic information obtained from PoP direct measurement to detect distributed traffic anomalies does not require OD flow data commonly used in network global anomaly detection, so it does not need to estimate the global traffic matrix, which greatly reduces the cost of communication between a large number of junctions. Based on the abnormal behavior detected, the network administrator can know the PoP corresponding to the specific behavior and take corresponding measures to respond to the specific behavior.

4.2 Abnormal behavior detection method based on traffic characteristic analysis

The traffic behavior characteristics related to the abnormal communication mode are extracted, and the correlation coefficients are calculated to measure the relationship between the detected PoP and the sequence of the change values of the characteristic entropy values of each traffic behavior between the adjacent PoP. Between the detected PoP and each PoP adjacent to it, the same number of correlation coefficients can be obtained with the traffic behavior characteristics compared. It is worth noting that when a distributed traffic anomaly occurs, which will cause similar changes in behavior related variables on multiple PoPs. Because of the huge background traffic, some behavioral variables do not change significantly. In this case, the maximum of all correlation coefficients between the detected PoP and each adjacent PoP is selected to reflect the impact of the abnormal communication mode on the network scope.

5. Association analysis of traffic abnormalities in communication networks based on behavior analysis

Abnormal traffic behavior recognition can be applied from the perspective of feature correlation analysis. In order to reveal the potential characterization of DoS/DDoS attacks in each sub-stream, the application of anomalous network traffic behavior recognition algorithm based on feature correlation analysis is used to calculate the abrupt proportion of the entropy value traffic behavior characteristics in each sub-stream. On sub-streams, the correlation of abnormal traffic behavior characteristics on sub-streams is validated, and the correlation between abnormal traffic behavior characteristics and abnormal network traffic behavior is validated, so as to identify DOS/DDoS attacks in the network. When correlation feature recognition is used to analyze abnormal traffic behavior, it is necessary to verify the correlation of abnormal traffic behavior characteristics on sub-streams and complete the verification work in candidate time. DoS/DDoS attacks and association rules of traffic behavior characteristics are used to identify DOS/DDoS attacks in communication networks and determine the correlation degree of abnormal traffic behavior characteristics on each sub-stream.

6. Conclusions

With the continuous development and wide application of information technology and communication technology, the data traffic carried by communication network is becoming larger and larger, and the network structure and application are becoming more and more complex. In order to ensure the safe and efficient operation of communication network, it is necessary to analyze and detect the network operation in real time and accurately. Traffic anomaly detection can effectively detect anomalous events in the network, and correlation analysis can reveal the root causes of anomalies, which is of great significance to improve the emergency response ability of communication network system. In the detection of abnormal traffic behavior in communication networks, time series graph analysis, traffic characteristic analysis and time-space sequence analysis can be used to make the detection results more accurate. In the correlation analysis of abnormal traffic behavior in communication network, it can also be carried out from two angles of feature correlation analysis and user behavior correlation analysis, so as to obtain the characteristics of traffic behavior, and then better identify the abnormal traffic behavior.

References

[1] Chen Zhong. Cloud communication anomaly detection method based on Collaborative neural network [J]. Journal of Liupanshui Normal University, 2014, 04 (24): 63-67.

[2] Feng Zhen. Relevance analysis of traffic anomalies in backbone communication networks [D]. Chengdu: University of Electronic Science and Technology, 2010, 53-65.

[3] Xu Yanmei. Statistical-based anomaly detection model for network traffic[J]. Computer Engineering, 2015, 31 (24): 123-125.