AN EFFECTIVE WAY TO DETECT COMPUTER NETWORK ANOMALIES

Sa'dullayev Avaz Akmal o'g'li
Teacher of the "Computer systems" department of the
Karshi University of Economics and Pedagogy
E-mail: avazbek_sadullayev_1997@mail.ru

ABSTRACR

With increased threat on the network, the detection of network anomalies is becoming more complicated. This thesis looked at anomaly detection by modeling a computer network as a temporary network.

Keywords: Anomaly detection, network level detection, app level detection, mobile security, Android security.

In general, according to the cardinalities of Nature, Environment, behavior and correlation, the anomalies of the Computational Network can be divided into 3 categories: point anomalies, natural anomalies, integrated anomalies.

The technology for detecting current anomalies can be divided into 4 categories, namely classification methods, statistical methods, clustering methods and information theory method.

Among them, the development of statistical theory and computer network science has greatly helped to detect network anomalies. An algorithm for analyzing localized key components has been used to continuously monitor the properties of the network area. A fault detection algorithm based on Xos vectors has been proposed and applied to a multilayer web network system represented by Time series graphs. The computer network was modeled as a dual graph and then a dual graph was projected as a directed weighted graph. Unlike these methods, in this thesis, an active subnet was isolated from the network. We divide it by the specified time frame. We divide into networks with directed weighted graphs in the time sequence. Then we carry out the decomposition of the properties separately for each network segment. In the first part of the work, the identification of active sub-networks is obtained from the network. In the second part, the process of detecting anomalies is carried out. At the end of the work, the results are considered.

IDENTIFICATION OF ACTIVE SUBSETS

At work, we model the time-lapse communication record in two parts, including Source IP and Destination IP. The “Source IP” part represents all nodes sending a connection message in the time section, and the “Destination IP” part represents all nodes at the time the message is received. Some nodes in “Source IP” only send connection messages, some nodes in “Destination IP” receive messages, while nodes present in “Source IP” and “Destination IP” not only send but receive messages. Therefore, we can use the “Source IP” or “Destination IP” communication state to indicate the communication state of the entire network. This causes some of the contact information to be lost. But significantly reduces the computational complexity.

RESULTS OF DETECTION OF ANOMALIES

In the experiment, we used W = 7 as an examination of the experiment. On this basis, we mark different moments after the division. If there is a case where there are entries within a marked as an anomaly, this case is defined as an anomaly. Both the Source IP address and Destination IP address of this entry, currently designated as an anomaly, are defined as anomalies at the same time.

Figure 1 shows the value of deviations at different times in the given window. In the figure, the time marked “+” is the time when the anomalous record is set in the data set.

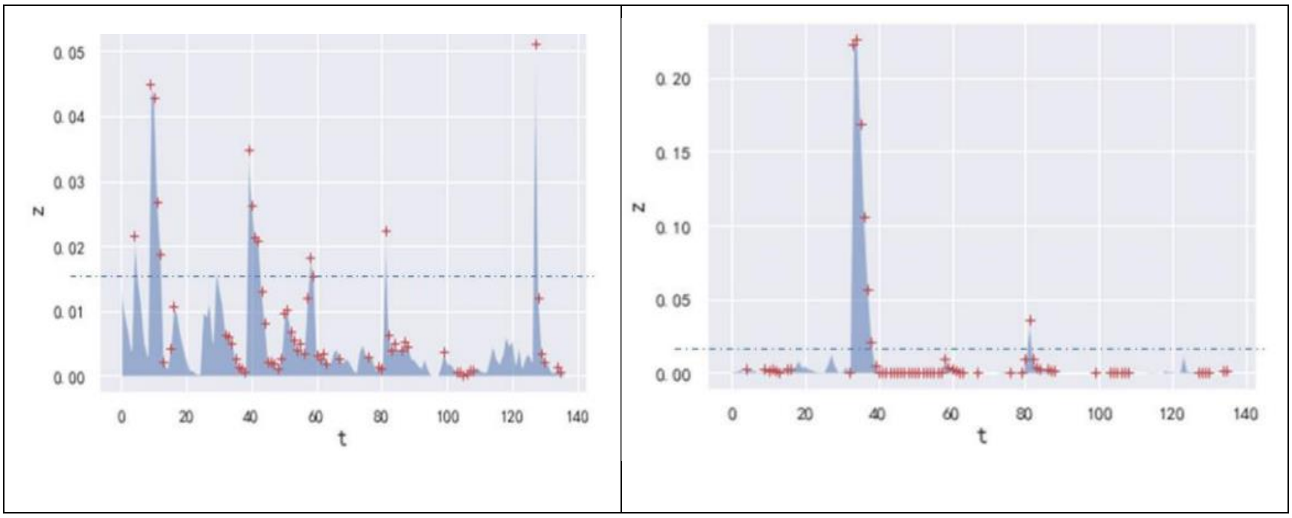

Figure 1. Change of information exits

As can be seen from the picture, after giving a certain limit, it is possible to assess whether an anomaly occurs at the moment, depending on whether it exceeds the limit. Table 1 shows anomaly detection results with dual projection results under the priority of accuracy.

Table 1. Anomaly detection results

Anomaly types Signal number accuracy recall ratio	Anomaly types Signal number accuracy recall ratio	Anomaly types Signal number accuracy recall ratio	Anomaly types Signal number accuracy recall ratio	Anomaly types Signal number accuracy recall ratio
Off-level joint projection unspecified anomalies, internal access, HTTP service denial,	Off-level joint projection unspecified anomalies, internal access, HTTP service denial,	Off-level joint projection unspecified anomalies, internal access, HTTP service denial,	Off-level joint projection unspecified anomalies, internal access, HTTP service denial,	Off-level joint projection unspecified anomalies, internal access, HTTP service denial,
Distributed denial from IRC botnet service, brute force Cracking of SSH 12 1 0.188	Distributed denial from IRC botnet service, brute force Cracking of SSH 12 1 0.188	Distributed denial from IRC botnet service, brute force Cracking of SSH 12 1 0.188	Distributed denial from IRC botnet service, brute force Cracking of SSH 12 1 0.188	Distributed denial from IRC botnet service, brute force Cracking of SSH 12 1 0.188
Level joint projection internal access, distributed rejection from IRC botnet Service 7 1 0.109	Level joint projection internal access, distributed rejection from IRC botnet Service 7 1 0.109	Level joint projection internal access, distributed rejection from IRC botnet Service 7 1 0.109	Level joint projection internal access, distributed rejection from IRC botnet Service 7 1 0.109	Level joint projection internal access, distributed rejection from IRC botnet Service 7 1 0.109

REFERENCES:

1. Chandola, V., Banerjee, A., and Kumar, V. (2009) Anomaly detection: A survey. ACM Computing Surveys (CSUR), 41, 15:158.

2. Ahmed M, Mahmood A N, Hu J. A Survey of Network Anomaly Detection Techniques[J]. Journal of Network and Computer Applications, 2015, 60:19-31.

[3] Yu W, Aggarwal CC, Ma S, Wang H. On anomalous hotspot discovery in graph streams. In: Proceedings of the 13th IEEE International Conference on Data Mining (ICDM), Dallas, TX, 2013.

4. Ide, T. and Kashima, H., Eigenspace-Based Anomaly Detection in Computer Systems, ACM SIGKDD 2004, pp.440-449.

5. Eslami M, Zheng G, Eramian H, et al. Anomaly detection on bipartite graphs for cyber situational awareness and threat detection[C]// 2017 IEEE International Conference on Big Data (Big Data). IEEE, 2017.
6.SCXIDS2012)[OL].https://www.unb.ca/cic/datasets/ids.html Canadian Institute for Cybersecurity.