ATLANTIS PRESS
Advances in Engineering Research, volume 166
3rd International Conference on Automation, Mechanical Control and Computational Engineering (AMCCE 2018)

Research on Enterprise Network Topology Anomaly Detection Techniques

Yanxia Li[a], Kaikun Dong[b] and Li Guo[c]

School of Computer Science and Technology,Harbin Institute of Technology at Weihai, Weihai 264200, China

[a]863751767@qq.com, [b]kaikun.dong@gmail.com, [c]2395551014@qq.com

Abstract: At present,the enterprise network management system presents the network connections between nodes in the form of network topology,so that the network topology can be visualized.However,the enterprise network itself is complex.With the increase of enterprise business,the number of network nodes increases,resulting in the complexity between node connections,therefore, this paper regards the changes of node connections in the network as exceptions and a network topology anomaly detection technique based on link redundancy preprocessing is proposed for enterprise intranet.The technique detects the abnormal situation in the network topology to locate the equipment failure and promptly discovers the violations of network access control behaviors and illegal intrusions to enhance network security.

Keywords: network topology graph, link redundancy preprocessing, topology anomaly detection.

1. Introduction

With the improvement of the importance of topology visualization,the integrity and accuracy of network topology are critical to network fault management and security management [1].In [2] the topology detection method based on DNS protocol can only detect network nodes with domain names,which has great limitations.In [3] Yuri Breitbart et al. has put forward a topology algorithm based on address forwarding table.Although the algorithm can accurately discover connections between devices, there is a high requirement on the integrity of the address forwarding table.In [4] the author uses data structure to store link informations for topology construction,however, the authenticity of data sources is not verified and there is a hidden danger that the topology detection result is deceived.This paper compares the link information with the original link by detecting the link information of each host in the authentication system. If any change is found,it detects whether the new link devices are abnormal, promptly alerts or updates the network topology in time, checking the authenticity of data sources by detecting the authorization index of the devices to prevent spoofing[5].

2. Network Topology Anomaly Detection Technology

2.1 Abnormal Classification in Enterprise Network Topology

This paper classifies the enterprise network topology anomalies into the following categories:

1) The device in the original topology is added,and the new device is connected under a certain device. Judge whether there is a case of illegal access.

2) The device in the original topology has not changed,but the upper-level or lower-level connected equipment of a certain device has changed.Judge whether the access is unauthorized.

3) The device in the original topology is reduced,and the device in the original link is no longer connected. Judge whether the equipment is faulty or shuts down.

2.2 Anomaly Detection Idea

Each host IP is captured from the authentication system and the link information is detected regularly.Then we compare the detected link information with the original link information.The source of the changed device is detected. According to different sources, different measures are taken.

Link redundancy preprocessing is required before the link information is compared.Provided that all path segments detected in the network are compared,it will inevitably cause redundancy detection and bring about a lot of time overheads.Therefore, this paper adopts the method of preprocessing link information to remove the repeat path and improve the efficiency of abnormal detection.

2.3 Anomaly Detection Problem Description and Model Definition

Definition 1. The unit link(Unit_Link) indicates that the node a is directly connected to the node b without passing any other nodes. The unit link is represented by (a, b).

Definition 2. Orthogonality, in computing technology, that indicates nondependence or decoupling. In this article, the term is used to indicate that there is no duplicate path between the two links.

Definition 3. AvoidList is an edge list which stores unit links and satisfy unit link orthogonality.

Definition 4. R_{ij} represents the jth hop node starting from the node i.$R_{ij} > 0$ indicates that there is the jth hop node,and $R_{ij} <= 0$ indicates that there is no jth hop node.

Definition 5. ResidualList is a node list which stores the remaining link information after link redundancy preprocessing.

2.4 Anomaly Detection Process

The anomaly detection process proposed in this paper is divided into three stages: link detection, link redundancy preprocessing and anomaly detection. The detection process is shown in Fig. 1.

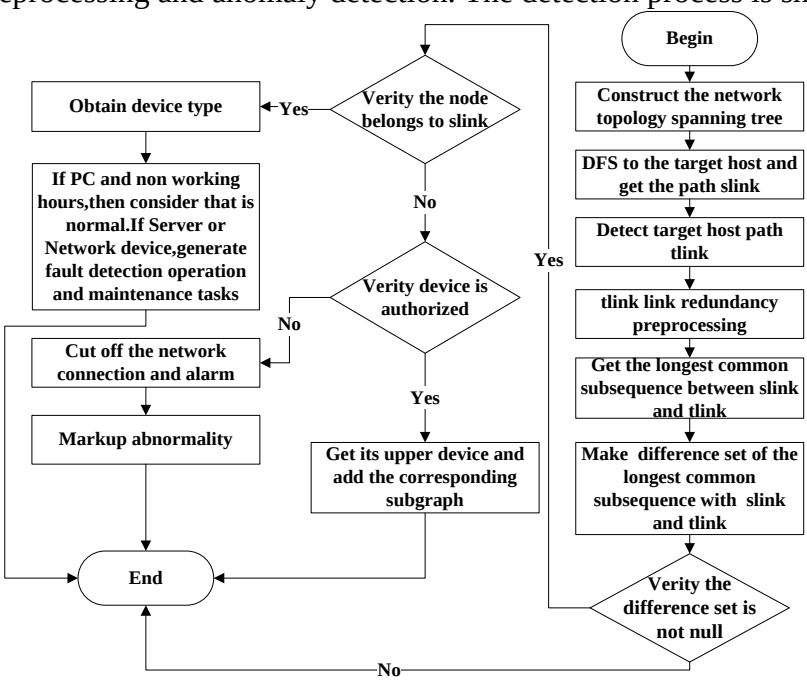

Fig. 1 Anomaly Detection Flowchart

2.5 Anomaly Detection Description

1) Link Detection

A network topology detection algorithm is constructed to detect all the target hosts in the network, and a path from the probe source to the target host is obtained. Each node passed through the path is represented by a node ID, and eventually obtain the link path stored in the dictionary.

The algorithm is described as follows:

Assuming that the link information detected is represented by dictionary links_dict,where the key of the dictionary is the ID of each target host, and the value of the dictionary is the node ID that is detected from source to the target host and is stored in the list.

Step1: Create a link information dictionary links_dict = {}, initialize the send socket TTL = 1.

Step2: Get the target host ID and set it to the key of the links_dict.

Step3: Send the ICMP message to the target host based on the TTL value.

Step4: The receiving socket receives the ICMP message until it times out. After passing one device, the TTL value is reduced by one, and the ICMP message continues to be sent down until the

TTL value is reduced to zero.Then the TTL hop of the path is obtained, and the device ID to the TTL hop is stored in the list. If the arrival device is the target host and the ICMP terminal inaccessible message is directly sent to the detection source, and the detection will be ended and turn to the Step6.

Step5:TTL increases progressively,go to Step3 and continue.

Step6: Set the list to links_dict's value.

2) Link Redundancy Preprocessing

The algorithm of link redundancy preprocessing(LRP) first decomposes the links obtained by detection into unit links. All the unit links contained in the path are filtered with AvoidList elements, and redundant links are discarded, and the other remaining links are added to the AvoidList.

The LRP algorithm is described as follows:

AvoidList is initially empty.The path source node index is $\mathbf{i}$.

For the initial path of AvoidList:

There is no redundancy, which is directly decomposed into unit links and added to the AvoidList.

For all R_{ij}>0,$\mathbf{f} = R_{ij}$,$\mathbf{g} = R_{i(j+1)}$,the edge (f,g) is added to AvoidList, where the initial value of j is 1,incremented by 1.Until R_{ij}<= 0,the algorithm ends.

For the path outside the initial path:

①For all R_{ij} >0, $\mathbf{f} = R_{ij}$, $\mathbf{g} = R_{i(j+1)}$,the edge (f,g) is added to the temporary list TmpList.If $\{(f,g) \mid (f,g) \in TmpList \text{ and } (f,g) \notin AvoidList\}$, the edge (f,g) is added to AvoidList and the nodes of the edge are added to ResidualList in order. If $(f,g) \in AvoidList$,discard (f,g) and clear TmpList.

②j=j+1,if R_{ij}<= 0, the algorithm ends and get the node list ResidualList ,otherwise turn ①.

3) Anomaly Detection

Compare the detected link information with the original link information to detect the anomaly.

The algorithm is described as follows:

Step1: By acquiring the node information and connection information of the original topology, construct the network topology spanning tree.

Step2: Get the path $Path_{old}$ from the detection source to the target host $\mathbf{i}$ by Depth-First Traver

Step3: Obtain the path from the detection source to the target host $\mathbf{i}$ by the link detection algorithm. After that, the link is preprocessed by the link redundancy preprocessing algorithm to obtain the ResidualList, which is marked as $Path_{new}$.

Step4: Take the first node of $Path_{new}$,and get the subpath $Path_{old}{}'$ consisting of all nodes from the node to the end node of $Path_{old}$.

Step5: Obtain the longest common subsequence by comparing $Path_{old}{}'$ with $Path_{new}$,and the nodes outside the longest common subsequence are the nodes that generate network topology changes.

Step6: The longest common subsequence is respectively differenced with $Path_{old}{}'$ and $Path_{new}$ to obtain the difference sets Old and New.

Step7: If Old is not empty, that is, the node with network topology change is the node in the original link,go to Step8. New is not empty, that is, the node is the newly detected node,go to Step9. If the difference set is empty, go to Step2 to continue the detection of the next target host.

Step8: Get the device type, if it is network device or server, generate equipment fault detection operation and maintenance task; if it is PC and the anomaly detection time is not at work time, then the device is considered to be off normaly, otherwise generate fault detection operation and maintenance task.

Step9: Find the newly detected node in authorized devices.If the device is authorized,get the upper device of this node,and add the node to the corresponding subgraph of the upper device.If the device is unauthorized,disconnect the device immediately and emit the alarm information containing the connections between nodes. and notify the administrator to deal with it in time.

3. Examples of Application

In this paper,we intercept some of the network topologies whose topological relationships have changed and show the topological variation anomalies discovered by using this technology by contrast. We can see that the comparison results are in good agreement with the expected results.

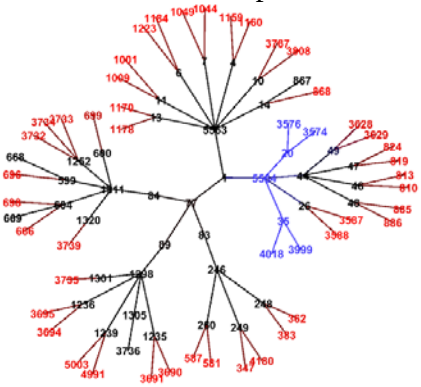

Fig. 2 Enterprise Network Topology 1

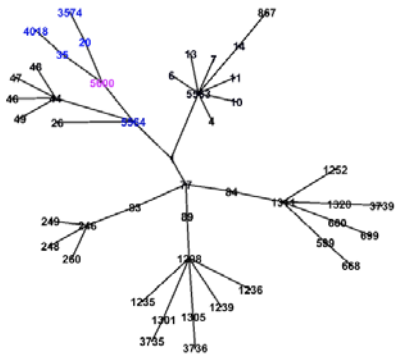

Fig. 3 Device Shutdown and Access Abnormity

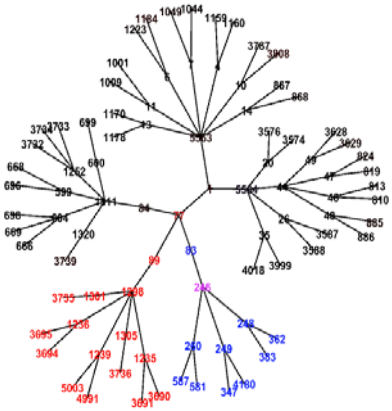

Fig. 4 Enterprise Network Topology 2

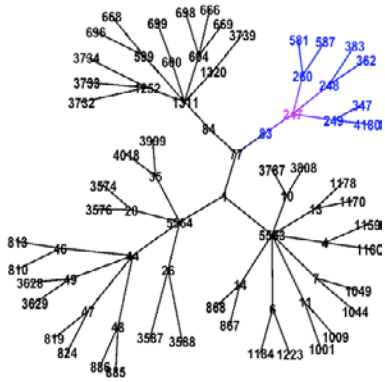

Fig. 5 Device Failure and Replacement Abnormity

In comparison with Fig. 2 and Fig. 3, it can be seen that detection shows that the number of PC is greatly reduced,and the device 5564 is connected to the new lower layer device 5600. Then the device 5600 is detected as the authorized equipment, and there is no illegal intrusion of the network. In comparison with Fig. 4 and Fig. 5, it is found that the device 89 is no longer connected to the network.In this case, the device fault detection operation and maintenance tasks are generated in time. The lower equipment of the equipment 83 is replaced,and then the system emits access path change alarm and blocks the network security events in time.

4. Conclusions

The research of network topology anomaly detection is of great significance. This paper detects the changes in topology connection to further enhance the security of enterprise networks. We verify that the anomaly detection method in this paper can effectively detect the topology abnormal connection and meet the real-time requirements of network topology.

References

[1] Yuxiao Wang. Research on Large Scale Network Topology Visualization[D].Beijing Institute of Technology,2016.
[2] Yifang Zhao, Dongmei Zhang.A Network Topology Discovery Algorithm Resistant to Routing Spoofing[J].Netinfo Security,2017(7):52-58.
[3] Y Breitbart, M Garofalakis, C Martin, et al.Topolopy discovery in heterogeneous IP networks[C].In Proc of INFOCOM 2000.Tel Aviv Israel,2000.
[4] Shuangjiao Fan. The Research of Topology Discovery and Attack Detection Technology Based

on OSPF Protocol[D]. Beijing University of Posts and Telecommunications,2015.
[5] Zhaopeng Jia,Binxing Fang,Chaoge Liu,Qixu Liu,Jianbao Lin. Survey on cyber deception[J].Journal on Communications,2017,38(12):128-143.