ISBN 978-981-14-1684-2
Proceedings of 2019 the 9th International Workshop on Computer Science and Engineering
(WCSE 2019 SUMMER)
Hong Kong, 15-17 June, 2019, pp. 599-604
doi: 10.18178/wcse.2019.06.088

Analysis of Illegal Terminal Bypass Blocking in Power Industry Marketing Scene Based on Network Topology and Result Estimation

Ruxia Yang [1+], Wei Chen [1], Xianzhou Gao [1] and Congcong Shi[1]

[1] Global Energy Interconnection Research Institute, State Grid Key Laboratory of Information & Network Security, Nanjing, China

Abstract. Because of the characteristics of wide-ranging points, diverse access modes and complex network topology in power industry marketing site, precise blocking must be achieved when abnormal terminals are blocked to ensure that blocking action only affects specific illegal access terminals. This requires precise selection of blocking points, and wrong selection of blocking points may have a significant impact on the normal business of the network. In order to solve this problem, this paper adopts the construction of the power industry marketing field terminal access network topology map, pre-calculates the blocking revenue and blocking cost of each blocking node in the attack graph, and then selects the blocking with the least benefit of the blocking cost. The node implements accurate and effective illegal terminal access path blocking by bypassing the access port, network redirection and other bypass blocking technologies. This method can achieve accurate control and precise blocking of illegal terminals, and is more suitable for the complex environment of the power industry business hall.

Keywords: Power industry marketing site, Network topology, Illegal terminal blocking

1. Introduction

As the largest power grid marketing field terminal of State Grid Co., Ltd., due to its wide variety, large scale, and complex and open physical environment, under the condition of relatively weak security protection measures, it is easy to become an illegal person to carry out cyber attacks. At present, the company's security access measures still have shortcomings. It is difficult to cover all marketing service terminals. It can only solve the problem of access to office computer terminals and mobile operating terminals that can be modified. At the same time, the access control measures are insufficient and there is a risk of being bypassed. It is urgent to deeply study the unified access technology for marketing field terminals applicable to various types and different software and hardware platforms, to achieve unified management and control of various marketing field terminals accessing the company network, and to improve the security protection level of the power grid.

Due to the multi-faceted, multi-access, and complex network topology of the power industry, it is necessary to achieve accurate blocking when blocking abnormal terminals, ensuring that the blocking action only affects specific illegal access terminals. This requires precise selection of blocking points, and the wrong blocking point selection may have a significant impact on the normal business of the network. By constructing the power industry marketing field terminal (such as marketing mobile operation terminal, charging POS machine, ATM automatic payment machine, video terminal, printer, fax machine and other common office peripheral terminal) to access the network topology map, pre-calculate each attack map Blocking the blocking gain and blocking cost of the node, and then selecting the blocking node with the lowest cost of blocking the maximum benefit, and achieving the accurate and effective illegal terminal

[+] Corresponding author. Tel.: + 86 13655178548; fax: +86 025-83095588.
E-mail address: yangruxia@geiri.sgcc.com.cn.

access path resistance by closing the access port, network redirection and other bypass blocking technologies. Broken.

When the identity of the access terminal is illegal, this paper uses network topology analysis and effect estimation to block it. The flow chart is shown in Figure 1. It is divided into three stages: network topology discovery, blocking response decision, and bypass blocking control. The network topology discovery phase analyzes and generates abnormal source behavior through online monitoring of abnormal behavior of the terminal. The topology path between the abnormal terminal and the monitoring point; blocking the corresponding decision stage according to the topology path generated in the previous stage, and estimating the effect from the blocking cost and the blocking benefit, and obtaining the optimal blocking strategy and generating a corresponding response decision; on this basis, the control node generates a corresponding blocking policy, and performs protocol blocking by means of bypass on the pre-selected node.

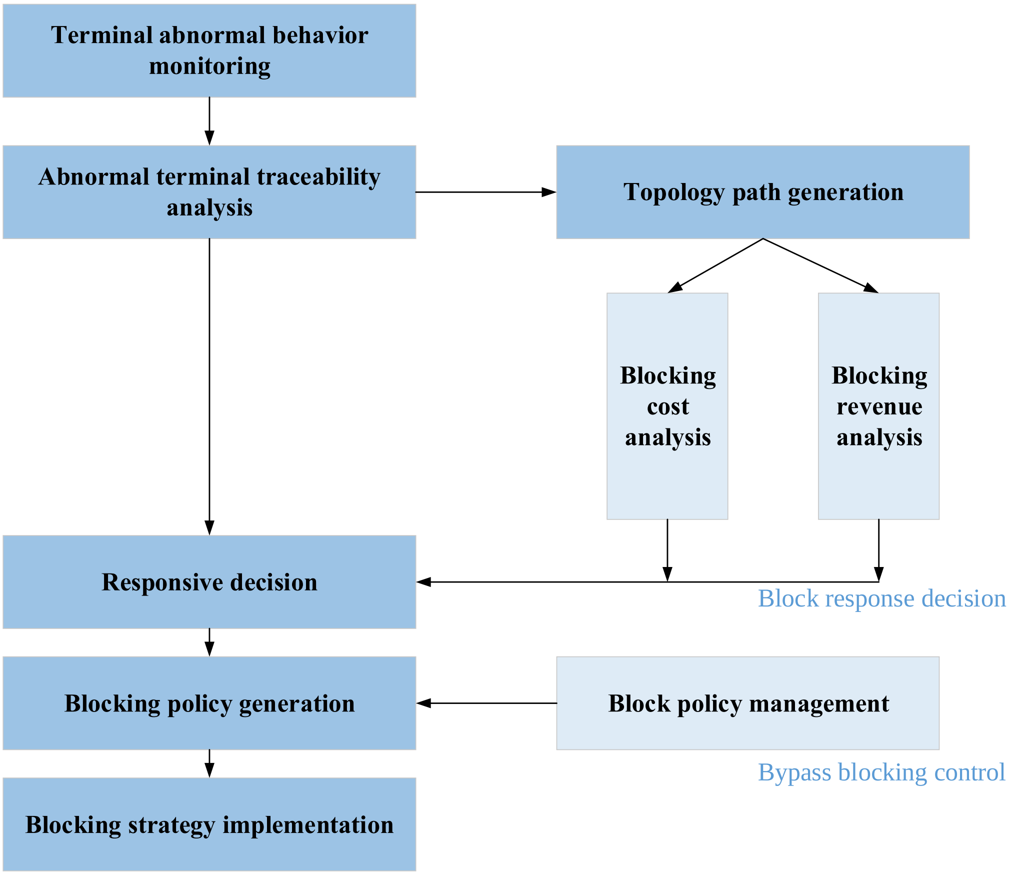
Terminal abnormal behavior monitoring
Abnormal terminal traceability analysis
Topology path generation
Blocking cost analysis
Blocking revenue analysis
Responsive decision
Block response decision
Blocking policy generation
Block policy management
Bypass blocking control
Blocking strategy implementation

Fig. 1: The process of illegal terminal bypass blocking based on network topology analysis

2. Network Topology Discovery

The network layer is the third layer of the ISO-defined OSI standard model, between the transport layer and the data link layer. The purpose of the network layer is to achieve transparent data transmission between the two end systems, specific functions including addressing and routing, connection establishment, maintenance and termination.

Network topology discovery refers to discovering network elements and determining interconnections between network elements, including interconnected devices (such as routers, bridges, switches, etc.), hosts, and subnets[1].

Topology discovery is an important part of configuration and fault management and an important part of network management. The network topology map generated by the topology discovery can help the network administrator understand the topology of the network, quickly locate the fault location, determine the scope of the fault, and become the common starting point for discovering the network element and calling other management function modules[2]. Topology discovery is also an important part of measuring the success or failure of a commercial network management system, and plays a very important role in the development of the entire network management system.

There are many methods for topology discovery at the network layer. The following are commonly used: network layer topology discovery algorithm based on ICMP protocol, network layer topology discovery algorithm based on SNMP protocol, network layer topology discovery algorithm based on ARP protocol, and OSPF protocol based Network layer topology discovery algorithm.

2.1. Network layer topology discovery algorithm based on ICMP protocol

The topology discovery principle based on the ICMP protocol is the network range to be detected, that is, the IP address space. Then select a series of probe destination addresses, which should be distributed to each subnet of the destination network as much as possible; use Ping to sequentially detect each IP address in a given address range to obtain a list of active host IP addresses; for all active IPs The address performs the Traceroute operation in sequence, records the result of the Traceroute operation, obtains the routing information of the device arriving at the IP address, sends a DNS packet to all active IP addresses to determine the domain name of all active devices, and then sends an ICMP mask to the IP address in the list. Request the packet to get the subnet mask of the device, and add each IP to the corresponding subnet; distinguish the network according to the router interface address and network mask, get the corresponding network address, and then establish the router and router according to the result of the Traceroute operation. The connection, as well as the connection information of the router and subnet, to obtain the topology information of the entire network.

2.2. Network layer topology discovery algorithm based on SNMP protocol

The principle of network topology discovery based on the SNMP protocol is to automatically maintain the MIB library in the network device, and store system information such as system information, routing information, and interface information. The SNMP MIB can remotely obtain device information from the network and obtain information from the information. The connection relationship of the network. The SNMP protocol works through the manager-proxy mode. The management station sends the SNMP protocol primitive to the proxy. The proxy server sends a response to the management station to send back the MIB information[3]. Through the analysis of the information, information about the network structure can be obtained. By reading the MIB information in the network obtained from the MIB, the network nodes having the network routing function in the network can be gradually found down, and finally the entire network topology is obtained[4]. The advantages of this topology discovery algorithm are: the discovery process and the algorithm are simple, the target is clear, the discovery efficiency is high, and the system overhead is small. For routers with restricted permissions, although topology discovery is limited, because the routing information can be obtained from the routing table, it can discover its first-level router and get a relatively complete topology relationship[5]. The disadvantages are as follows: The network device must support the SNMP protocol and must have access to the network device. Network devices without routing on the network, including switches and host devices, cannot be discovered. For routers that use static route configuration protocols, the discovery effect will be greatly limited. This method is applicable to topology discovery of a large backbone network and obtains the overall topology of the network.

2.3. Network layer topology discovery algorithm based on ARP protocol

The ARP-based topology discovery principle is based on the ARP table of any router or switch. It can discover all the network devices in the Ethernet LAN connected to the Ethernet port, and then determine the routers and switches in the network, and continue to use the AI strong table. Discovery is performed to obtain the topology relationship of the entire Ethernet network. This method is suitable for local area network discovery and finds high efficiency, but it is not suitable for network over-large, and can not find network connections and devices that do not support ARP.

2.4. Network layer topology discovery algorithm based on OSPF protocol

The principle of OSPF-based topology discovery is to reproduce the topology structure by periodically exporting the router configuration file or periodically exporting the OSPF link state database[3]; or using the listener to listen to all IP data packets to analyze the topology changes. Since OSPF maintains a basic network link state database for each router, it is more desirable to obtain OSPF packets directly, extract network topology information based on this database, and obtain updated LSAs in real time to synchronize networks. Topology information. The algorithm is also fast, efficient and accurate[6].

3. Block Response Decision

The blocking response decision stage needs to automatically generate a decision according to the abnormal behavior analysis of the terminal, and submit the blocking decision to the blocking control node to start blocking. Different types of decision-making, the blocking scheme will also change greatly. The blocking of abnormal behavior of the terminal not only needs to consider the blocking effect, but also needs to consider the normal operation of the legitimate service. Therefore, factors such as network topology characteristics and terminal type need to be considered. , comprehensively consider blocking costs and blocking revenue, and generate the best blocking decision.

In the terminal abnormal behavior scenario, the network topology discovery can effectively discover the topology path between the abnormal terminal node and the monitoring point. The path passes through multiple router switch nodes. Therefore, it is necessary to select the optimal set in the path to complete the blocking[7].

The selection of the blocking node is based on an estimate of the blocking node's defense effect. The defense effect of blocking nodes can be divided into two aspects: blocking cost and blocking revenue. The blocking cost is used to measure the performance overhead and false positive cost of a set of blocking nodes; the blocking benefit can be measured against two harmful aspects of the distributed denial of service attack: First, the protection effect on the victim resources, the second is the protection effect on link resources. The blocking cost includes blocking performance overhead and blocking false positives. Blocking performance overhead refers to the negative impact that blocking on the network can have on the business itself. Blocking false positives refers to the difficulty of distinguishing between attack traffic and normal traffic. Undifferentiated network filtering filters out normal traffic of the terminal. Since in the network, the routing protocol tends to use the shortest path as the packet transmission path, the shortest path related to the abnormal terminal is counted. By comparing how much the shortest path is blocked by a group of filtering nodes, the filtering node can be measured. Impact on normal communication of abnormal terminals. Blocking revenue includes attack flow blocking rate and link protection rate. Blocking the attack flow blocking rate can be used to assess the protection of the victim's host resources by the blocking scheme. The blocking rate refers to the number of blocked attack streams as a percentage of the total number of destinations. The higher the blocking rate, the better the infiltration mitigation effect.

The selection of blocking nodes adopts a greedy strategy selection strategy. The core idea of this strategy is to recursively select the current cost-effective blocking node: calculate the blocking revenue and blocking cost of each blocking node in the path, and select the cost performance. The highest blocking node, adjusts the path, blocks the attack path, recalculates the cost performance of the blocking node in the residual graph, and continues to select the node with the highest cost performance. In this algorithm, the blocking gain value is calculated by weighting the blocking rate and the link protection rate, and the blocking cost value is calculated by weighting the performance overhead and the false alarm overhead. The response decision module determines the cost budget based on the comprehensive influence of the intrusion event. When the sum of the blocking costs generated by the selected node exceeds the cost budget, it means that the node selection work ends, and the remaining cost budget can be used to fine tune the blocking node set. And then get the final blocking solution[8].

4. Bypass Blocking Control

This document dynamically configures analog port control for VLANs through SNMP to implement bypass blocking of illegal terminals. With the implementation of port VLAN dynamic configuration, 802.IQ is used to dynamically, real-time, and on-demand switching between the connected VLAN and the isolated VLAN, and with the corresponding decision, according to the blocking policy, the VLAN of the terminal is dynamically implemented. Configured to provide port-based access control similar to 802.1X. Therefore, dynamic configuration of VLANs based on SNMP is the core idea of bypass blocking control technology.

In the VLAN-aware bridge that supports the SNMP protocol, the VLAN-related items are set in the Private branch of the vendor's MIB to allow VLAN management and configuration using the SNMP protocol. In the bridge, the SNMP agent collects data on the device, and the management call includes many parts. The Agent usually classifies these functions, and the functions of a certain part are mapped to an Interface in the MIB. Each interface has some attributes to indicate the status of the device. For example, for certain status information of a port (such as whether the switch of the port is connected to other devices, etc.), the collection of statistical data (such as the inflow and outflow of the port, the broadcast of the port, the multicast packet, etc.) corresponds to After interface.102 is completed, the management station can obtain information or implement management by reading or modifying the interface-related attributes in the switch MIB. The collection of the various states of the VLAN and the configuration management functions of the agent in the VLAN-aware bridge are also performed corresponding to the relevant interface.

There are two ways to implement port VLAN in the VLAN-aware bridge: tagged frame and PVID. In a VLAN-aware bridge, after a VLAN is newly defined by the vendor's own management software, the agent will generally add a VLAN interface to the MIB, corresponding to the VLAN (and corresponding to the PVID implementation of this VLAN). Ageit generally assigns a local VLAN number to this VLAN interface for easy management. At the same time, an interface (tagging interface) of the 802.IQ EcnapsuliatonaTg type is added to the MIB, corresponding to the implementation function of the tagged frame of the VLAN, and then the tagging interface and the VLAN interface are associated in the ifStackTable in the ifMIB branch of the MIB. When a port is added to a VLAN, the interface representing the port and the interface representing the VLAN are associated in the MIB. If a port is added to the VLAN by PVID, the interface representing the port and the interface corresponding to the VLAN are in the MIB. If the port is added to the ifStack table in the ifMIB branch, if the interface is added to a VLAN by using a tagged frame, the interface corresponding to the request port and the interface (tagging interface) of the 802.IQ Ecnapsulation Tag type corresponding to the VLAN will be in the MIB. The ifStackTable is associated in the ifMIB branch. Conversely, if the management station makes the above changes in the MIB of the switch through the SNMP protocol, the agent will create, define, or add the ports involved in the specified VLAN to the device.

5. Conclusion

This paper mainly proposes the illegal terminal bypass blocking in the power industry business hall based on network topology and result estimation, which realizes the accurate blocking of illegal terminals in the power industry business hall, and has strong applicability in the power industry.

First, complete the topology discovery. Topology discovery is an important part of network management. The network topology map can help administrators understand the network topology and quickly locate the fault. There are many network topology discovery methods, such as network layer topology discovery algorithm based on DNS protocol, network layer topology discovery algorithm based on ICMP protocol, network layer topology discovery algorithm based on SNMP protocol and network layer topology discovery algorithm based on OSPF protocol. Wait.

Then, perform topology analysis and result estimation. Through the topology map generated by topology discovery, analyze and estimate the positive and negative impacts caused by blocking from a certain port. Positive impacts such as: how much to eliminate, mitigate or suppress this abnormal terminal access event; negative impacts such as: the cost and impact of port blocking.

Finally, the specific blocking position is determined by topology analysis and estimation, and port blocking is performed.

6. Acknowledgements

This paper is supported by the science and technology project of State Grid Corporation of China: "Research on Key Technologies of Marketing Site Terminal Security Access" (Grand No. SGGR0000XTJS1800079).

7. References

[1] J. Shen, G. Gu, J. Luo. Research and Development of Network Management [J]. Journal of Computer Research and Development, 2002, 39(10):1153-1167.

[2] Siamwalla R, Sharma R, Keshav S. Discovering internet topology [J]. Unpublished manuscript, 1998.

[3] X. Wang, C. Chen. An improved topology discovery algorithm based on SNMP and OSPF [J]. Scientific and Technological Innovation Information, 2018, (9).

[4] S. Xue. Discuss the Design Method of Topology Discovery System based on SNMP [J]. Advanced Materials Research, 2011, 267:594-598.

[5] IETF RFC2271 -1998. An architecture for describing SNMP management rameworks[S].

[6] Y. Wang, N. Pan, X. Tao. Network Topology Discovery Algorithm based on OSPF Link State Advertisement [J]. International Conference on Intelligent Computing & Integrated Systems, 2010, 32(5):136-139.

[7] Z. Wang, Y. Zhang, D. Zhang, H. Wang. Improved network topology discovery algorithm [J]. Railway Computer Application, 2017, 26(5).

[8] W. Fu, J. Zhang, Y. Chen. Network topology discovery algorithm against routing spoofing attack in Internet of things [J]. Journal of Jilin University (Engineering and Technology Edition), vol.48, NO.4.