Research on Random Virtual IP Address Redistribution Technology Based on OpenFlow

Hai wang*, Yi wang, Bingbing luo and Baoying zhang
ZhangJiaKou Electric Power CO., LTD. 075000, China
*Corresponding author’s e-mail: 254576969@qq.com

Abstract. In view of the shortcomings of traditional network defense measures and the dynamic defense needs of existing network security, a random virtual IP address redistribution technology based on OpenFlow protocol is proposed, which realizes the conversion between real IP address space and random virtual IP address space. The technology can increase the randomness of IP addresses in two dimensions of time and space, and increase the difficulty of network sniffing and network attacks. It provides new solutions and ideas for the implementation of dynamic defense at the network level.

1. Introduction
A variety of network devices and program software constitute the modern computer network, but there are a lot of known and unknown vulnerabilities in these devices and software. At present, most of the network security solutions take the following two defense measures to deal with the network threat: on the one hand, by adding firewalls and security gateways on the basis of the existing network architecture, implementing access control and data encryption to build a multi-level defense system to improve the security of the network and applications; on the other hand, through penetration testing, the weakness, technical defect and vulnerability of network system and application software are analyzed actively. When problems are found, the security policy or program is updated by patching.

However, in recent years, a series of network security incidents and the serious consequences brought by them have sounded the alarm for the traditional defense ideas and measures, and the network security presents the situation of easy attack and difficult defense. The main reasons for this situation are as follows[1]:

(1) Convenience of attack
Computer technology not only enriches the Internet, but also provides convenience for malicious attackers in the network to carry out attacks. For example, attackers have the advantages of time and information. Attackers can test and scan network system vulnerabilities for a long time, and even carry out apt attacks.

(2) Passivity of Defense
First of all, when using traditional defense measures to build a multi-level defense system, it still relies on the deterministic network structure and network configuration in the network system. Once the static and isomorphic information is collected by the attacker, the attacker can carry out targeted intrusion against the characteristics of the network, and attack the network system or even the defense system.

The rise of dynamic defense provides a new and effective research idea to solve the problem of asymmetric disadvantage of both sides in network security. Dynamic defense is not a specific
technology, but an idea. It aims to deploy and run uncertain, random and dynamic networks and systems, making it difficult for attackers to find targets. This paper proposes a dynamic defense method, the core of which is to realize random virtual IP address reallocation by using OpenFlow. Through the random conversion of network address space, on the one hand, to build dynamic network configuration, to increase the randomness of network system, so as to increase the detection difficulty of attackers to network system; on the other hand, by randomly assigning virtual IPs and legitimate users to distinguish attackers in the network.

2. Working principle of SDN and OpenFlow

2.1. SDN
SDN (Software Defined Network) is a new network architecture with revolutionary significance[2]. Its core idea is to separate the control plane and data forwarding plane of the network, realize the programmable control of the underlying forwarding device through the centralized controller, and realize the flexible on-demand deployment of network resources. As shown in Figure 1, SDN is divided into application layer, control layer and forwarding layer, which is different from the traditional OSI seven layer network structure.

![Figure 1. SDN network architecture](image)

(1) Application layer
The application layer contains all kinds of network applications developed based on SDN network to meet the needs of users. When users develop and use these network applications, they do not need to care about the operation mode of the bottom layer of SDN network.

(2) Control layer
The control layer is composed of various DNS controllers (such as: floodlight, opendaylight, ons, etc.), which is the control center of the whole SDN network. Its core function is to realize the path exchange calculation and boundary service routing calculation within the network, and at the same time to send data forwarding instructions to the forwarding layer. The control layer mainly interacts with the forwarding layer and the application layer through the South and North interfaces.

(3) Forwarding layer
The forwarding layer is a basic forwarding network mainly composed of switches and communication links, which is responsible for the forwarding of user data. In the process of forwarding, it depends on the forwarding table items generated by the control layer. The device in the forwarding layer does not make any decision, but only performs the task of data message forwarding. The forwarding layer interacts with the control layer through the control interface. On the one hand, it reports the information and status of network resources upward, on the other hand, it receives the forwarding information sent by the control layer.
2.2. OpenFlow
OpenFlow is a standard implementation form of SDN network architecture, which is widely recognized by the industry. In the OpenFlow network architecture, the forwarding layer uses a large number of interconnected OpenFlow switches as the network infrastructure[3]. These OpenFlow switches (hereinafter referred to as switches) use the OpenFlow protocol (South standard interface protocol in the OpenFlow network architecture) to establish the connection and interaction with the controller in the control layer through the security channel. The controller is responsible for managing the entire OpenFlow / SDN network.

(1) The principle of OpenFlow packet forwarding
In the traditional network architecture, packets are forwarded according to the forwarding table in the switch or the routing table in the router. In OpenFlow, the forwarding table and routing table in traditional network are unified, and the concept of flow table is added. The of switch in the forwarding layer can forward packets at high speed by querying the flow table information.

(2) Definition of packet forwarding
Protocols and packet forwarding rules running in OpenFlow network are uniformly completed by controllers in control layer, so users or network operation and maintenance managers can edit and define rules in the controller according to their own needs, and then uniformly distribute them to OpenFlow switch by the controller, so that the whole SDN / OpenFlow network can forward according to these personalized rules The corresponding data package.

3. Random virtual IP reallocation model based on OpenFlow
The definability of packet forwarding rules in SDN / openflow network provides the basis for the realization of virtual IP reallocation technology. Based on this, this paper proposes a network dynamic defense model of random virtual IP reallocation based on openflow. The model adds topology management module, virtual IP generation module and virtual IP reallocation module to the controller in the control layer. The specific model structure is shown in Figure 2.

3.1. Topology management module
The module is mainly responsible for network topology management and network equipment certification. On the one hand, it authenticates the switches and network equipment accessing the network; on the other hand, it registers or logs out the new switches and network equipment accessing and exiting the network while maintaining the network link, and updates the network link information.

This module sends LLDP (Link Layer Discovery Protocol) packets to all switches in openflow network, and processes LLDP packets uploaded by switches at the same time[4,5]. After receiving LLDP data, the OF switch will send the packet to all its ports. When the OF switch receives these lldp packets, it will sends link information between the two switches to the controller by the pack_ in messages. When the controller collects enough link information, it can build the network topology
based on this information. The module updates the information of the OF switch in real time and feeds back the link status of the network in time.

In this module, the information of OF switch is updated and the link state of network is fed back. At the same time, the IP address space of the whole network is divided into two parts for management. One part is that the real IP address of the actually linked device and of switch is recorded as , and , where, represents the real IP address of the ith device, n represents the number of devices accessing the OpenFlow network. The other part is the idle IP address, which is obtained by removing RIP from all IP addresses, which are conforming to IPv6 format. It is used to generate the virtual map of the real IP address, which is recorded as , and , where, represents the j-th idle IP.

3.2. Random generation module of virtual IP

This module first needs the topology management module to provide the link connection of the whole OpenFlow network, including the actual IP pool and the idle IP pool in the OpenFlow network. Then, according to the actual number of devices in the access network, it randomly selects sufficient and different idle IP addresses from the idle ip set, and the selected IP forms a virtual IP address pool, so as to randomly Generate a virtual IP address. In this paper, a random generation algorithm of virtual IP is designed, and its implementation process is shown in algorithm1.

Algorithm 1 Random generation algorithm of virtual IP

| Input:                                |
|---------------------------------------|
| Number of IP addresses of real devices: n |
| Set of free IP addresses: VIP = \{vip1, vip2, ... vipj ... vipm\} |

| Output:                              |
|--------------------------------------|
| Randomly generated virtual IP set: VIP' = \{vip'_1, vip'_2, ... vip'_j ... vip'_n\} |

1. for each i in [1,n] do
2.   j=Random(1,m)
3.   while VIP\[j\] in VIP' do
4.    //Find the randomly generated IP address according to the randomly generated index value J, and judge whether the IP address is repeated
5.      j=Random(1,m)
6.      end while
7.      AddIP(VIP', VIP\[j\])
8.   // add randomly generated virtual IP addresses that meet the requirements into the virtual IP generation set VIP'
9. end for

3.3. Virtual IP redistribution module

Generally speaking, attackers must master the topology of the target network and the IP address of the target host before launching attacks. In the traditional network, these information are fixed and directly exposed in the communication link, which is easy to be detected by the attacker. Therefore, using dynamic virtual IP to confuse attackers and make them fail has gradually become a new way of network defense and one of the main research directions of dynamic defense.

The main function of the virtual IP reallocation module proposed in this paper is to implement the mapping from real IP to random virtual IP, transform the real IP address space and virtual IP address space, and realize dynamic defense through the dynamic transformation of the real and false IP address in the two dimensions of time and space. The ultimate purpose is to confuse the attacker and make the attack fail. The process of random virtual IP reallocation is shown in the figure 3.
It is assumed that host1 and host2 are two terminals in OpenFlow network that implement dynamic defense to communicate. When implementing random virtual IP reallocation, the virtual IP reallocation module first maps the real IP exchanged by host1 and host2 on the link to the randomly generated virtual IP through editing the flow table and creating the real virtual IP mapping table. Finally, host2 at the receiving end maps the last hop through the IP mapping relationship. The virtual IP address of host2 is converted to the actual IP address of host2 to realize the communication between terminals. If a new virtual IP pool is randomly generated in each communication process, and the mapping from real IP to virtual IP is carried out at the same time, the attacker will get different virtual network topology after sniffing the OpenFlow network every time, and it is difficult to grasp the necessary information to launch the attack, so as to reduce the threat to the entire OpenFlow network and access devices.

4. Conclusion

In this paper, we propose a dynamic defense technology based on random virtual IP reallocation implemented by openflow, which provides a solution for the implementation of dynamic defense at the network level. In this paper, a random virtual IP address reassignment model is designed, and the modules such as topology management, random virtual IP generation and random virtual IP assignment are studied and designed in detail. At the same time, the random virtual IP generation algorithm is studied and designed. The model and algorithm proposed in this paper improve the difficulty of the attacker's sniffing and prediction of IP address, increase the difficulty of attack, and effectively prevent all kinds of attacks that need to know the network topology in advance, which is of great significance to the research of dynamic defense.

References

[1] Zhou yuyang, Chen guang, Guo jingsheng, et al.(2018 ) A review of research on dynamic transfer of attack surface in mobile target defense . Journal of software. pp. 2799-2820.
[2] Yuan wei, Qi yudong, Chen qinghua.( 2015) SDN technology and application research review . China command and control conference.
[3] Zhao lianxiang.(2016) Discussion on the principle of open flow under SDN Architecture. Telecommunication technology.pp. 67-70
[4] Chen X , Chen Y , Sangaiah A K , et al.(2017) MonLink: Piggyback Status Monitoring over LLDP in Software-Defined Energy Internet. Energies.
[5] Ehab Al-Shaer, Qi Duan, Jafar Haadi Jafarian.(2013) Random Host Mutation for Moving Target Defense. International Conference on Security & Privacy in Communication Systems.
[6] Shin S, Yegneswaran V, Porras P, et al.(2013) AVANTGUARD: Scalable and vigilant switch flow management in software-defined networks. Proc of ACM CCS’13. New York:ACM. pp. 413-424.