Multi-Dimensional Features Analysis in SDNs

George Meghabghab
Roane State Community College
Cyber Defense Program

Software Defined Network (SDN) is a programmable network that separates the network data plane from the control plane. However, lots of security threats and issues are concerned in software defined network. In order to reasonably complete the cyber-attack situation evaluation in the SDNs, a cyber-attack situation evaluating method based on multi-dimensional features analysis in SDNs is considered. Cyber-attack detection features and computation methods are deployed. Mininet is the experimental environment for the typical cyber-attacks to verify and analyze the multi-dimensional features. The experimental result shows that the proposed method can accurately reflect the cyber-attack situation in SDN environment.

Different Cyber Attacks in SDN

1. OpenFlow Flooding Attack(OFN)

OpenFlow protocol is used to communicate between controller and switch. Attacker can use the vulnerabilities of OpenFlow protocol to launch an attack in SDN. For example, denial of service attack and distributed denial of service attack are most common flooding attack in SDN. In general, we classify OpenFlow flooding attack (OFA) into two types. One type is that when the attacker uses a controlled host to send a great deal of fake packets (such as TCP, UDP or ICMP packages) to the switch, and these packages are not been labeled in flow table, at this moment the switch has to send all these unlabeled packages to the controller, then this situation will consume so much more computing resource that the controller cannot provide services for normal legal hosts. Another type is that the attacker uses the OpenFlow switch to send numerous packets whose actions field is the controller, because in this way the controller resource will be consumed in large quantities so that it has no enough resources to deal with the legitimate requests. Once the controller resources are maliciously consumed by a large number of illegal requests, and it will lead to the SDN environment impossible for legal services.

SPFN = numbers of different source ports/flow numbers

FC =Difference flow numbers/time interval

2. Network Scanning Attack (NSA)

The network scanning attack is the foundation for attackers to find a target they are interested in and implement a further attack. After network scanning, the picture of target network will be presented, such as the opened ports, the opened services, the behavior of users, the information about route tables, the name of workgroup, potential security vulnerabilities and so on. The attackers use network scanning attack to collect the information about target network in order to complete the next deep intrusion. Therefore, finding and detecting the potential network scanning attack is an indispensable part in the cyber-attack situation evaluation in SDN. Normally, port scanning is the most common scanning method, it contains vertical scanning, horizontal scanning, and block scanning, where block scanning is a combination of the first two.

%UCF =opc(att.dst _ addr = nor.dst _ addr)/opc(att.dst _ addr = nor.network _ addr)

3. ARP Attack (ARPA)

Address Resolution Protocol (ARP) is used to match an IP address into a corresponding MAC address. It is a request and response protocol whose messages are encapsulated by a link layer protocol. Usually, the ARP cache is used to increase the matching efficiency between IP and MAC, in order to improve the network communication speed. ARP uses a simple message format containing one address resolution request or response. The request frame contains the requester's MAC and IP address and the IP address of the responder from whom the requester hopes to get the response. The response frame contains the requester's MAC and IP address and responder's MAC and IP address.

In the process of attack, a source host will send much more number of ARP request frames than it receives the response frames. There will be a high probability of ARP attack when the RRRF is lower than a pre-assigned threshold value. We can obtain the request and response frames by counting the ARP packets by analyzing the fields in the packets. After Packet-In action got a packet, we use pkt_arp = pkt.get_protocol (arp.arp) to get the ARP packet. If pkt_arp.opcode == arp.ARP_REQUEST, it means this is a request frame, otherwise, pkt_arp.opcode == arp.ARP_REPLY indicates a response frame.

IP-MAC Mapping in ARP Cache (IMMC). In normal conditions, the IP-MAC pairs should be 1-1 mapping. In the process of attack, if a host sends the ARP frames results in a 1-N or N-1 mapping schema of IP-MAC pairs in the ARP cache, the network may be suffering from the ARP attack. We can obtain the history IP address and MAC address from the OpenFlow match fields, where arp_spa is source IP, arp_tpa is destination IP, arp_sha is source MAC, and arp_tha is destination MAC. In addition, we can obtain new IP and MAC using ryu.lib.packet.arp.

4. Switch Compromised Attack (SCA)

OpenFlow Switch is a very important part in SDN. It connects the controller and hosts, and receives the commands from a controller and delivers them to certain ports or forwards a packet from one host to another. The action of a packet can be changed using programming the switch by the developer and network manager. Switch compromised attack (SCA) is that the attacker controls the OpenFlow switch and modifies the flow table, then furthermore, launch attacks to the controller and host in SDN.

Flow change rate (FCR): In the process of attack, the attacker must modify the flow table to launch a further attack. If the flow table is modified frequently, then it is possible that the switch is compromised, and the attacker is eavesdropping. We calculate the flow change using comparing the flows in the flow table at different times.

Change of Destination IPs (CDI): In the process of attack, once the switch is compromised, the destination IP address is always directed to a certain host IP address. We can find the IP address in flow_stats.actions.

Change of Destination Ports (CDP): In the process of attack, once the switch is compromised, the destination output port is always directed to a certain host port. We can find the output port in flow_stats.actions.

In this work, the experiment simulation to establish the test scenario: Mininet was used to create a realistic virtual SDN environment, and simulated OpenFlow flooding attack, network scanning attack, ARP attack and switch compromised attack. In simulation environment, we used several important components and tools in SDN. They are OpenFlow switch, Ryu controller and Scapy program, and the brief introductions are as follows.

(1) Open vswitch aims to define how an SDN controller communicates with the SDN switches byusing OpenFlow protocol. It is a special component in software defined network, that supports universal OpenFlow protocol.

(2) Ryu controller is a component-based software defined networking framework written in Python, that supports fully OpenFlow versions. The well-defined APIs make it easy for the

developers to create a new network management and applications in software defined network.

(3) Scapy program is a packet manipulation program. We used Scapy to generate various packets during our experiment. The legitimate traffic generated by Scapy is a composition of different protocols including ICMP, TCP and ARP. The attacks simulated by Scapy including ARP flooding attack, ARP cache poisoning attack, TCP flooding attack and network scanning attack.

In the simulated network environment, there are two logistic networks, that respectively contain one Open vswitch and three hosts. The Ryu controller is the connection between two networks. Different attacks in network2 in order to generate a large number of attack data. All the four types of typical cyber attacks are simulated with Scapy in network1.

Process of Experiment

In this experiment, four typical attacks in SDN were simulated. The time interval for detection loop is set to 10 seconds. Two switches were programmed to obtain the flow tables in every 10 seconds during extracting features. Because of the limited storage space for flow tables, they were recorded and exported the information in the flow tables into a format file by the timestamp as well as by the duration time of each flow. In this simulation, continuously collected and recorded all the information in flow tables from time 0 to 1800. OpenFlow flooding attack (OFA) was simulated during time 200 to 400, network scanning attack (NSA) during 600 to 800, ARP attack (ARPA) during 1000 to 1200, switch compromised attack (SCA) during 1400 to 1600. During other time periods, experimental network was under normal situation, that means there were no simulated cyber attacks occurred. The following is the test steps in our experiment.

Compute respectively the values of all the cyber attack features during time 0 to 1800 using the computing and statistics methods developed above. In the process of computing and statistics, a sample of 135 feature values, that were equidistance sampling during time 0 to 1800. Table 1 shows the brief details about 135 sample feature values.

Time	PPF	CRSP	GF	NDP	RPH	%UCF	RRRF	FCR	CDI	CDP
1	97.27	0.34	2.00	5.00	1.00	26.89	98.73	0.00	0.56	0.50
20	90.07	0.50	2.00	5.00	1.00	16.99	98.45	0.18	0.82	0.72
40	95.33	0.50	2.00	3.00	2.00	18.34	98.17	0.06	0.78	0.96
60	91.04	0.32	1.00	556	0.00	98.96	98.6	0.16	0.70	0.76
80	93.74	0.22	3.00	4.00	0.00	13.2	54.28	0.14	0.88	0.56
100	94.32	0.64	3.00	2.00	5.00	16.71	99.18	0.48	0.62	0.30
120	90.92	0.94	3.00	4.00	4.00	9.41	99.88	0.66	0.12	0.20
135	93.33	0.82	2.00	590	0.00	95.35	99.03	0.00	0.88	0.56

Conclusion

In this work, an improved method to evaluate cyber attack situation in the software defined networks. The method is based on multi-dimensional features analysis that can be divided into cyber attack features extraction process and cyber attack features relationships analysis process. In the process of cyber attack features extraction, the computation and statistics methods about cyber attack features for the four typical cyber attacks, including OpenFlow flooding attack, network scanning attack, ARP attack and switch compromised attack was considered. All the original network information from the flow tables was collected and calculated all the values of features according to the computation and statistics methods situation in SDN.

In this experiment, the cyber attack feature computation and statistics methods were achieved in SDN environment by programming to detect the typical four cyber attacks and generated all values of cyber attack feature. Finally, we calculated the values of cyber attack features after considering relationships

between any two different features, and obtained the cyber attack situation by fusing all the values of cyber attack features and comparing with the cyber attack situation level table. The result showed that this method can accurately reflect the trend of cyber attack situation in software defined network