Journal of Computers Vol. 30 No. 5, 2019, pp. 185-204
doi:10.3966/199115992019103005014

A Cyber Attack Situation Evaluating Method Based on Multi-Dimensional Features Analysis in SDNs

Zhijie Fan[1,2*], Qian Xu[1], Wenye Zhu[1], Chengxiang Tan[1]

[1] Electronics and Information Engineering School, Tongji University, Shanghai 201804, China

[2] The Third Research Institute of Ministry of Public Security, Shanghai 201204, China
aaronzfan@126.com, goldey@126.com, mei-414@163.com, tancx1990@sina.com

Received 22 January 2018; Revised 25 May 2018; Accepted 4 July 2018

Abstract. 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 this work, in order to reasonably complete the cyber attack situation evaluation in the SDNs, we proposed a cyber attack situation evaluating method based on multi-dimensional features analysis in SDNs. We systematically considered cyber attack detection features and improved their computation methods about four typical cyber attacks in SDN. And furthermore, we emphatically considered the interrelations and restrictive correlations between any two different cyber attack features using Fuzzy Cognitive Maps (FCM). Then we completed the quantization method of cyber attack situation evaluation in the SDN simulation environment. Finally, we used Mininet to establish our experiment environment, in which we simulated four typical cyber attacks to verify and analyze our method in the experiment. The experimental result shows that our proposed method can accurately reflect the cyber attack situation in SDN environment.

Keywords: attack detection, attack situation, cyber attack, cyber security, fuzzy cognitive maps, software defined network

1 Introduction

Software defined network (SDN) technology is a novel approach to cloud computing that facilitates network management and enables programmatically efficient network configuration in order to improve network performance and monitoring [1]. It is a programmable network, that can provide network virtualization service. It separates the network data plane from the control plane and provides a mean for a network manager to program in order to control network packet processing [2]. Therefore, recently SDN become a hot research point and has been widely used in different fields.

There have been many researches about independent analysis and detection of different kinds of cyber attacks in SDN. However, there are few researches about cyber attack situation evaluation in SDN environment, and they also need to be improved the accuracy. In this paper, in order to more accurately obtain an integrated cyber attack situation in SDNs, we proposed a cyber attack situation evaluating method based on multi-dimensional features analysis in software defined networks, where the four typical cyber attacks (OpenFlow flooding attack, network scanning attack, ARP attack and switch compromised attack) are discussed. We used the typical cyber attack detection features definitions in [3], and improved their computation methods, In the process of evaluating, we emphatically considered the interrelations and restrictive correlations between any two different features. We modeled the interrelations and restrictive correlations using Fuzzy Cognitive Maps (FCM) model in order to reasonably complete the cyber attack situation evaluation in SDN.

In the experiment section, we used the experiment simulation to establish the test scenario. We used Mininet [4] to create a realistic virtual SDN environment, where we used several important components

[*] Corresponding Author

and tools in SDN (such as OpenFlow switch, Ryu controller and Scapy program). We simulated four typical cyber attacks to verify and analyze our method in experiment environment, and the experiment results showed that our method can accurately reflect the cyber attack situation in SDN environment.

The rests of the paper are organized as follows. In Section 2, we briefly introduce the background knowledge on SDN architecture and OpenFlow protocol. Section 3 overviews the related work about cyber attack and cyber security in SDN. Section 4 introduces the foundation about the survey method of cyber attack situation we proposed. Section 5 presents our proposed detailed survey method. Section 6 shows the cyber attack situation simulations that describe experimental analysis. Finally, concluding remarks are made in Section 7.

2 Background

2.1 SDN Architecture

Software Defined Networking (SDN) is an architecture purporting to be dynamic, manageable, cost-effective, and adaptable, seeking to be suitable for the high-bandwidth, dynamic nature of today's applications. It decouples network control and forward functions, enabling network control to become directly programmable and the underlying infrastructure to be abstracted from applications and network services [5].

According to the definition in white paper of Open Networking Foundation (ONF), SDN architecture consists of five parts, they are three structure layers and two communication interfaces. The five parts respectively are application layer, controller layer, data layer, northbound interfaces and southbound interfaces. The brief SDN architecture that contains five parts and the internal relations between them is as shown in Fig. 1.

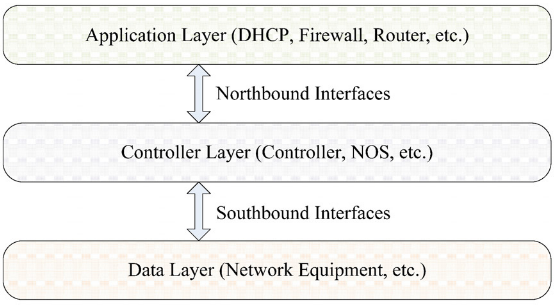
Application Layer (DHCP, Firewall, Router, etc.)
Northbound Interfaces
Controller Layer (Controller, NOS, etc.)
Southbound Interfaces
Data Layer (Network Equipment, etc.)

Fig. 1. Brief SDN architecture

The application layer contains various different network applications and one application logic and one or more northbound interface drivers. It is responsible for managing and controlling data forwarding and policy processing. It also controls the application interfaces in order to complete network rapid configuration, improve network utilization, support various security policies and support quality of service requirements.SDN applications can themselves expose other layers of abstracted network control, thus it can offer one or more higher-level northbound interfaces through respective northbound interface agents.

The controller layer is also named network operating system. It is responsible for translating the requirements from the application layer down to the data layer and providing the applications with an abstract view of the network, that includes statistics and events. The controller layer as a logically centralized entity, it precludes implementation details in order to separate heterogeneous characteristics and complete virtualization or slicing of network resources in the underlying network.

The data layer is also named infrastructure layer. It is responsible for storing and delivering the forwarding traffic. It is composed of various different switching nodes, such as OpenFlow switchers and routers. It is communication tunnel that purposed to complete the corresponding operating according to the orders from controller layer. It can also be defined as multiple physical network elements, that is a physical combination of communications resources, managed as a unit. This definition means it can complete the physical mapping, management of shared physical resources, virtualization and slicing of the data, interoperability with non-SDN networking.

The northbound interfaces are between applications layer and controller layer, and typically provide abstract network views and enable direct expression of network behavior and requirements. The southbound interfaces are between controller layer and data layer, and it provides at least programmatic control of all forwarding operations, capabilities advertisement, statistics reporting, and event notification.

2.2 OpenFlow Protocol

The OpenFlow protocol [6] is accepted by Open Networking Foundation (ONF) to be a standardized protocol in SDN southbound and northbound interfaces. It aims to define how an SDN controller communicates with the SDN switches. Flow table proposed in OpenFlow protocol is the foundation of querying and forwarding a package. The structure of flow table in OpenFlow protocol consists of six parts: match fields, priority, counters, instructions, timeouts and cookies. When a data packet arrives, the packet header will be compared with the match fields. if there is a match, the switch will update the counters and execute the actions, otherwise, the packet will be sent to the controller through the secure channel. The match fields contain source and destination address of Ethernet, source and destination IP address, source and destination TCP/UDP port and so on. The priority defines the order of matching flow items. Counters count the relevant information such as packet count and byte count. Instructions define the actions like forward, drop or modify. Timeouts define the longest time a flow exists and the longest time a flow exists in a flow table if no packet matches the flow.

The OpenFlow switch is a special kind of SDN switch which supports the OpenFlow protocol. Each switch processes the packages according to the flow table, and the controller can modify the flow table to change the actions of a packet.

3 Related Works

Recent years, there are lots of types of cyber security researches in the field of software defined network, that can be classified into several parts: data plane security, control plane security, control channel security and application plane security. Because of particular characteristics of software defined network, types of traditional attacks can easily occur in SDN environment, such as flooding attack, ARP attack, network scanning attack, compromised attack and so on. The following is the literature review, that is described and organized according to different detection methods of the typical cyber attacks in SDN environment.

Flooding attack. It can lead to the massive paralysis of the network and the denial of service, it was classified into several types in the traditional network, such as ICMP flooding attack, TCP SYN flooding attack, UDP flooding attack, TCP LAND flooding attack, Ping flooding attack and so on. In SDN environment, OpenFlow switch is a key component that uses the OpenFlow protocol to complete data transmission between the controller and infrastructure. There are many researches about flooding attack in SDN environment. The UDP flooding attack was considered in SDN environment, and a lightweight countermeasure was proposed that used traffic monitoring to detect the flooding attack [7]. The novel mechanism using the self-organizing map application was proposed, it aims to solve the performance bottleneck and overload problems for the upper layers in a large-sized SDN in case of flooding attacks. It integrated a distributed self-organizing map system to OpenFlow Switches to detect the OpenFlow flooding attack [8]. The authors proposed a mechanism that combines normal traffic learning, external blacklist information, and elastic capacity invocation in order to provide effective load control, filtering and service elasticity during a flooding attack in SDN. They implemented the mechanism and analyzed the performance on a physical SDN environment using a comprehensive set of real-life normal traffic traces [9]. The optimized protection method named OpenFlowSIA in SDN from OpenFlow flooding attacks was proposed, it was based on support vector machine. The method applied effectively the algorithm they proposed and coherent policies to protect the network from resource exhaustion caused by OpenFlow flooding attacks, particularly for the controller and OpenFlow switches [10].

ARP attack. It means that the attackers use fake IP address and MAC address to generate a large number of ARP messages in order to interrupt network service by using man-in-the-middle attack. There are many researches about ARP attack in SDN environment. The authors described how to handle ARP traffic in SDN environment. It may also be generated if network devices are not configured properly. This bulk of traffic created by ARP packets causes an unnecessary overhead on the network. This issue has been tackled by properly configuring controller ARP table and installing flow entries in the SDN switch properly [11]. The Bayesian theorem was used to calculate the probability of a host being an attacker, the algorithm was proposed to detect the ARP attack in SDN environment based on Bayesian theory [12]. Some vulnerabilities were exploited to implement a suite of attacks, especially man-in-the-middle attack and ARP attack was discussed. The authors successfully accessed to control bypassing port scan, and launched an ARP attack in a floodlight controlled SDN environment [13]. The automatic ARP attack detection and mitigation mechanism was proposed in SDN environment, that can prevent ARP attack. The solution added a separate module in the network where ARP packets are received to obtain ARP traffic, that was analyzed for a possible attack in the SDN environment [14].

Network scanning attack. It means that the attackers use several equipments and tools to complete the information gathering for target network before launching an attack action. There are many researches about network scanning attack in SDN environment. The method based moving target defense was proposed in order to improve the advancement and effectiveness of defensive mode. It can prevent scanning attack by changing network configuration and status dynamically [15]. The end-point mutation technique was proposed, that is one of the key techniques. It can prevent connection requests not within service period by using address transition of packet header and update of net-flow table based on DHCP update [16]. The authors confused scanning attack by virtual hopping, that deploys a hypervisor node in each subnet to ensure mutation consistency. The virtual end-point mapping mechanism was based on OpenFlow protocol. It converts real IP addresses to virtual IP addresses so as to implementing end-point hopping [17]. The mutation mechanism named ST-RHM was proposed. It can resist cooperative scanning attack effectively by using temporal spatial mixed mutation method based in SDN environment [18].

Compromised attack. OpenFlow switch is the core important component in SDN, once an SDN switch is compromised by an attacker, the assumption fails and the attacker will bring serious problems to the SDN network. There are many researches about compromised attack in SDN environment. Improved authentication mechanism was proposed for protecting the SDN architecture. In this research, they deployed the PKI authentication structure on hierarchical SDN controllers and SDN switches. This work provided network resilience when some controllers and switches are known as being compromised [19]. The authors analyzed the damages when a switch is compromised, such as modify the flow table, hijack the control channel to reconfigure a different controller, eavesdrop the control plane communication, spoof the topology and denial of service attack [20]. Furthermore, the attack models of switch compromised attack were discussed and two algorithms were designed to detect a compromised switch. The authors deployed security information and event management technology in SDN. The technology can provide real-time analysis of security alerts for network managers [21].

However, all the above researches on cyber attack detection deeply considered only several specific types of attacks in SDN. There are relatively few researches about cyber attack situation evaluation in SDN. In this paper, we proposed a cyber attack situation evaluating method based on multi-dimensional features analysis in SDN. During the evaluation process, we emphatically considered the method of four typical cyber attack features extraction and the interrelations and restrictive correlations between any two different features.

4 Foundation about Cyber Attack Situation Evaluation in SDN

4.1 Basic Concepts

In order to better and clearly describe the survey method of cyber attack situation, the related terminologies are defined as follows.

Definition 1. A Cyber Attack Situation denoted by E is defined as the current cyber attack status and future development trend in the target SDN.

Definition 2. f is a function of $E_e(i)$, where $E_e(i)$ is a set of cyber attack situation elements that is defined as the basic data elements.

Cyber attack situation elements are used for calculating cyber attack situation. In our work, the element means the different cyber attack features. After extracting all the situation elements, we can get the overall cyber attack situation by calculating the element status, i.e., $E=f(E_e(i))$.

Definition 3. T is a Cyber Attack Situation Index System that T is used to describe and quantify the cyber attack situation.

Definition 4. $D_L=\{D_{Lh}, D_{Lc}\}$ is a local data which is the cyber attack related data in target SDN, where D_{Lh} and D_{Lc} are a set of history data, current data, respectively.

Definition 5. $D_{Lf}(i)=f(D_{Lh}(i), D_{Lc}(i))$ is defined as a cyber attack situation evaluating process based on multi-dimensional feature data, where $D_{Lh}(i)$ and $D_{Lc}(i)$ are history and current data of the *i*-th situation element, respectively.

Definition 6. $D_r(i)=g(D_{Lf}(i))$ is defined as a cyber attack situation evaluating process based on the interrelations and restrictive correlations between features, *g* is used for the evaluation method.

The computing of cyber attack elements $E_e(i)$ is expressed as $E_e(i)=f(D_{Lh}(i), D_{Lc}(i), D_r(i), T)$ in this work. As shown in Fig. 2, the cyber attack situation evaluating process can be divided into multi-dimensional feature extraction and feature relationship analysis. First, we collect all the security information from the flow tables in SDN. Then we independently complete the feature extraction according to every feature definitions. Next, we find the interrelations and restrictive correlations between any two different features. Finally, we complete the cyber attack situation evaluation according to our proposed method and calculate the integrated cyber attack situation in SDN.

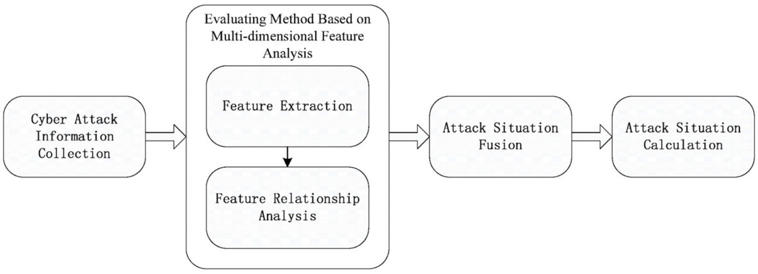
Evaluating Method Based on Multi-dimensional Feature Analysis
Feature Extraction
Feature Relationship Analysis
Cyber Attack Information Collection
Attack Situation Fusion
Attack Situation Calculation

Fig. 2. Cyber attack situation evaluating process

4.2 Hierarchical Multi-Dimensional Quantificational Index System in SDN

The analytic hierarchical process (AHP) was developed by Thomas L. Saaty in the 1970s, and it used the structured technique to organize and analyze complex system and make decisions. In [22], AHP was firstly used in the field of the cyber security situation, it was used to propose a hierarchical quantificational index system about cyber security situation. In our work, AHP is used to be a basic method of describing cyber attack situation.

The cyber attack situation index set is divided into three index layers. The first layer is used to describe the integrated cyber attack situation (ICAS) index in SDN network. The second layer is composed of four indexes, they are OpenFlow flooding attack (OFA), network scanning attack (NSA), ARP attack (ARPA) and switch compromised attack (SCA). All of these indexes in the second layer decide the index in the first layer. The indexes in the third layer include 13 features that are respectively correspond to the four different cyber attack types in the second layer. The index system and the hierarchical relationship between different layers is as shown in Table 1.

Table 1. Cyber attack situation index system in SDN

Indexes in 1-st layer	Indexes in 2-nd layer	Indexes in 3-rd layer	No.
Integrated Cyber Attack Situation (ICAS)	OpenFlow Flooding Attack (OFA)	Average Number of Packets per Flow (ANPF)	1
		Average Number of Bytes per Flow (ANBF)	2
		Percentage of Pair-Flow (PPF)	3
		Change Rate of Source Ports (CRSP)	4
		Growth of Flows (GF)	5
	Network Scanning Attack (NSA)	Number of Destination Ports (NDP)	6
		Ratio of Ports to Hosts (RPH)	7
		Proportion of Unsuccessful Connected Flow (PUCF)	8
	ARP Attack (ARPA)	Ratio of Response and Request Frames (RRRF)	9
		IP-MAC Mapping in ARP Cache (IMMC)	10
	Switch Compromised Attack (SCA)	Flow Change Rate (FCR)	11
		Change of Destination IP (CDI)	12
		Change of Destination Ports (CDP)	13

In our work, we collect the variety of network information from SDN, such as the flow tables at different times, and analyze the information according to the features in the third layer to obtain a 13-tuple data set per time sequence. Furthermore, we use AHP method to structure all the indexes in different layers to provide a foundation to complete the cyber attack situation evaluation in SDN. The definitions of all typical four cyber attack features in the third layer are introduced in next section.

4.3 Features Extraction in Anomaly Detection

In our work, typical four cyber attacks are considered, they are OpenFlow flooding attack, network scanning attack, ARP attack and switch compromised attack. The feature extraction is the first key step for calculating cyber attack situation in SDN. We used and improved the features definitions and the computing methods that are introduced in [3]. Next, our features definitions and computing methods in this paper are as below.

4.3.1 OpenFlow Flooding Attack (OFA)

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.

In this work, we use the typical obvious five features proposed in [23] to find the potential OpenFlow flooding attack. When the SDN is under attack, the amount of flow increases sharply in a short period of time. We make a decision to use the following five values as the features for the OpenFlow flooding attack.

Average Number of Packets per Flow (ANPF). In the process of OpenFlow flooding attack, attackers always use a small number of packets or bytes in most flow items to increase the efficiency of attack. For every flow, we can obtain the *packet_count* from *flow_stats* in the OpenFlow switch. The middle value of the sorted packets is used as an average value in case that some flow items have a large number of packets to increase the average value. In this work, we use equation (1) to calculate the middle average value of ANPF, where *F(i)* is the sequence of packets of each flow in ascending order, and *n* is the number of flows.

$$mid(ANPF)=\begin{cases} F((n+1)/2) & n\ is\ odd \\ \dfrac{(F(n/2)+F((n+1)/2))}{2} & others \end{cases} \quad (1)$$

Average Number of Bytes per Flow (ANBF). In the process of OpenFlow flooding attack, we also can obtain the *byte_count* from *flow_stats* in the OpenFlow switch for every flow. We calculate the middle average value of ANBF as same as the process of equation (1), Where *F(i)* is an ascending sequence of the number of bytes of each flow, and *n* is the number of flows.

Percentage of Pair-Flows (PPF). We suppose that there are two flows, they are flow1 and flow2. If these two flows can satisfy the following two conditions, then the flows are called pair-flow. Otherwise, if these two flows do not fit any one condition, they are the single-flows.

(1) Protocol: Two flows (flow1 and flow2) contain the same communication protocol in SDN.

(2) IP address: The destination IP of flow1 is the same as the source IP of flow2, and the source IP of flow1 is the same as the destination IP of flow2.

In the attack process, an attacker can use a fake IP address to launch an attack, that will lead to increase of single-flows. When the percentage of pair-flows is too lower or higher, the raise of possibility shows that the SDN is under attack. We can obtain the number of flows from *flow_stats* in OpenFlow switch.

Change Rate of Source Ports (CRSP). In the process of the attack, because the packages are generated from one port, the source ports will change less frequently than the normal situation. We can obtain the number of port from *actions* field in *flow_stats*. The CRSP can be calculated using the below equation.

$$CRSP = \frac{numbers\ of\ different\ source\ ports}{flow\ numbers} \tag{2}$$

Growth of Flows (GF). In the process of the attack, a lot of packages will be generated rapidly, we can record every packet flow in the flow table, and will work out the rapid growth of the number of flows. The GF can be calculated by the below equation.

$$GF = \frac{flow\ numbers\ difference}{time\ interval} \tag{3}$$

4.3.2 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 [24]. 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. In our work, we consider three items as the key features about network scanning attack in SDN. The details of the features are as below.

Number of Destination Ports (NDP). In the process of vertical scanning, the packets are usually sent from one certain IP address to other different ports. Therefore, there are lots of flow items, that contain the same IP address with different ports in the flow table. In the normal time, there are only several open active ports. Therefore, the change rate about the port number and flow amount will increase rapidly when the network is under scanning attack. It also means most of the destination ports are not available when under the attack. In our work, we use the number of the destination ports as a feature of concern. Because of the generality of this feature, the attackers can easily escape the detection by lower down the sending rate of packets. More other different features should also be taken into our consideration.

Ratio of Ports to Hosts (RPH). In the process of horizontal scanning, several certain ports on different hosts are scanned. In our work, we record the certain ports on different target hosts that have a certain access, and we calculate the maximum number of common ports among these port sets to measure this canning attack. We first set a pre-assigned threshold value for the network system in normally. When the ratio between the maximum number and host number is larger than the pre-assigned value, there will be a possible scanning certain ports on different target hosts from a compromised host by the attacker.

Proportion of Unsuccessful Connected Flow (PUCF). In the process of NSA, because of existing the large amount of flows, that are sent to search the available ports in SDN. But most these flows can establish the connection unsuccessfully. Therefore, the PUCF is used to be an effective feature in our work. It can be calculated by the following equation.

$$PUCF = \frac{opc(obj.dst\_addr = ref.dst\_addr)}{opc(obj.dst\_addr = ref.network\_addr)} \tag{4}$$

where *ref* means the normal flows and *obj* means the flows under attack. Considering different package protocols *obj.protocol* and various package number *obj.pkg_count (opc)* to establish a complete connection. In the numerator of above equation (4), the count value is based on two conditions. One is *obj.protocol=TCP* and *obj.pkg_count＜ 3*. Another is *obj.protocol=UDP* and *obj.pkg_count＜ 2*. The equation (4) can be easily changed or extended.

4.3.3 ARP Attack (ARPA)

Address Resolution Protocol (ARP) is used to match an IP address into a corresponding MAC address [12]. It is a request and response protocol whose messages are encapsulated by a link layer protocol. In the cache, there is an IP-MAC pair. 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. Therefore, this simple communication mechanism is easily used to launch an ARP attack.

ARP attack can be classified into two types. One type is the ARP flooding attack, it can be lead to network congestion using faking IP and MAC to generate lots of ARP packets. Another type is the ARP cache poisoning attack [25], it can be lead to network interruption and man-in-the-middle (MITM) attack using continuously faking ARP response packets to change the IP-MAC pairs in the ARP cache. In our work, we consider the two key features related to ARP attack in the ARP communicating process and attack mode.

Ratio of Response and Request Frames (RRRF). 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*.

4.3.4 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. We take the man-in-the-middle attack (MITT) in [26] for an example, the attacker can add a new destination IP address, duplicate the packets and forward to the attacker's host for eavesdropping, or modify the flow table to a new one, eavesdrop the packet and send a fake packet to the destination host to launch a MIIT. In our work, we consider the following three features to describe the switch compromised attack.

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 or launching a MITT. 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*.

4.4 Relationship Extraction among Different Features

There are a lot of researches about different kinds of cyber attack detection in SDN, but there are relatively few researches about cyber attack situation evaluation in SDN. Furthermore, after extracting the features in the target SDN network environment, most of detection methods independently calculate the values of different features at different time, and then complete the detection according to the different values of features. However, most of traditional detection methods always lack analysis of interrelations and restrictive correlations among different features, that usually exist in reality. In this article, we use Fuzzy Cognitive Maps (FCM) to quantitatively describe the interrelations and restrictive correlations between different cyber attack features in SDN.

Fuzzy Cognitive Maps (FCM) is firstly proposed by Kosko [27], who combines the cognitive map with fuzzy set theory. FCM model consists of nodes, directed arcs and weights of directed edges. It is a weighted directed graph that can describe a causal relationship. The node in FCM is called concept node that can describe the abstract things, concrete things, activities, system properties and system statuses according to actual demand. The weighted directed edges in FCM structure are used to describe the causal relationship between any two concept nodes. Directed edges can be viewed as single layer neural network with feedbacks and the object-oriented concept. The knowledge is inside of concept nodes and weighted directed edges. FCM model uses weighted directed relationships to simulate fuzzy reasoning, in which the interrelationships are used to stimulate dynamic behavior of the system.

FCM can stimulate the operation states of the system. The evolution process of FCM model includes forward and backward evolution. The forward evolution is mainly used for decision support and prediction, and backward evolution mainly is used for reason trace. In this article, we used the forward evolution to complete the cyber attack situation evaluation. After building the FCM model and obtaining the initial status values of all concept nodes, the status values of all concept nodes at any time can be calculated according to forward evolution by the following formula.

$$A_i(t+1) = f\left(A_i(t) + \sum_{j=1, j\neq i}^{n} A_j(t) \times w_i \right) \tag{5}$$

Suppose that $C=\{ c_1, c_2, \cdots, c_i, \cdots, c_n \}$ is a set of all concept nodes, $n=|C|$, and C_i is the value of the i-th concept node, recorded as A_i after mapping to range [0, 1], and it means the status value of concept node. $A_i(t)$ means the status value of i-th concept node at time t, and $A_i(t+1)$ means the status value of i-th concept node at time $t+1$. w_{ji} is the incidence matrix of concept nodes, also named as adjacent matrix. f is a function, the two or three valued step function and S-curve function are commonly used in practice.

An FCM model structure processing consists of several steps: selecting suitable concept nodes, connecting the causal relationship between any two concept nodes, and determining the impact degree of causal relationship. In this work, we choose all the attack features as the concept nodes in FCM, and the causal relationship and adjacent matrix can be decided respectively by typical machine learning technology [28].

5 Cyber Attack Situation Evaluation in SDN

In this section, we propose a cyber attack situation evaluating method based on multi-dimensional features analysis in SDN. In our work, we consider four typical attacks in SDN, that were decided by several dependent features. In section 4.2, we proposed and referenced the computing and statistics methods about every feature we considered. In this paper, we emphatically consider the interrelations and restrictive correlations between any two different features. Therefore, we use Fuzzy Cognitive Maps (FCM) to describe the relationship between different features. The following is the steps about the cyber attack situation evaluation in our work.

(1) Structure the FCM model. We choose all the 13 cyber attack features in Section 4.3 as the concept nodes in our work.

(2) Determine the adjacent matrix of FCM model using the weight learning method proposed in [28]. How to obtain the adjacent matrix of FCM, that satisfies the requirement in equation (5). We can equivalently convert this problem into the corresponding problem of obtaining the adjacent matrix of FCM according to the following equation:

$$\sum_{t=1}^{T}\left(d_j^t-\sum_{i=0}^{N}A_i^t w_{ij}\right)^2=0, \tag{6}$$

where A_i^t is the value of i-th feature at time t, and

$$d_j^t=-\lambda\ln\left(\left(A_j^{(t+1)}\right)^{-1}-1\right)-A_j^t. \tag{7}$$

We use least squares method to obtain the value of w_j as following:

$$w_j=\left(AA^{'}\right)^{-1}AD_j, \tag{8}$$

where $A=\left(A_i^t\right)_{(n+1)T}$, $D_j=\left(d_j^1,d_j^2,\cdots,d_j^i,\cdots,d_j^T\right)'$ and $w_j=\left(w_{0j},w_{1j},\cdots,w_{ij},\cdots,w_{nj}\right)'$.

Equation (8) is a linear equation. We can obtain every w_j by per time computation in equation (8). It means the weights that caused the concept node c_j can be obtained by one time computation. Furthermore, the values of w_{ij} can be obtained by n time computation in equation (8).

(3) Complete independently computing and statistics about the cyber attack situation values of 13 typical cyber attack features at time t according to the methods we proposed in Section 4.2.

(4) Consider the interrelations and restrictive correlations between every two attack features. We compute the cyber attack situation values of 13 typical cyber attack features at time t according to the following equation:

$$e_i(t)=f\left(g(e_i(t-1))+\sum_{i=1,j\neq i}^{n}g(e_i(t))w_{j,i}+\delta_i\right), \tag{9}$$

where $e_i(t)$ denotes the value of i-th feature at time t, and $e_i(t\text{-}1)$ means the value of i-th feature at time $t\text{-}1$. w_{ji} is the adjacent matrix of FCM. f is an S-curve function:

$$f(x)=\frac{1}{1+e^{-cx}},$$

where c is constant 4 in our work. In equation (9), δ_i is a corrective parameter of i-th feature, that is assigned by the average difference of negative feedback between real values and experiment test values for every features according to the historical data mining. $g(x)$ is a normalization function:

$$g(x)=\begin{cases}10 & x>value_{Max}\\ \dfrac{(x-value_{Min})\times 10}{value_{Max}-value_{Min}} & x\in[value_{Min},value_{Max}]\\ 0 & x<value_{Min}\end{cases}.$$

(5) Compute respectively the cyber attack situation values of four types of typical cyber attack based on AHP method, that means we compute the probability of occurrence about four types of typical cyber attack as the situation values. Each situation value of the type of typical cyber attack is calculated by the following equation:

$$Ev_i(t)=g\left(fea_1w_1+\cdots+fea_iw_i+\cdots+fea_nw_n\right), \tag{10}$$

where $Ev_i(t)$ means the situation values of i-th types of typical cyber attack. fea_i is the situation values of features, and w_i is the corresponding weight values of features. $g(x)$ is a normalization function.

(6) Obtain the integrated cyber attack situation values based on cyber attack situation values of four types of typical cyber attack and AHP method according to the following equation:

$$E(t)=\begin{cases}10 & \exists Ev_i(t)\geq\theta\\ g(10-\sum_{i=1}^{n}Ev_i(t)w_i) & if\ Ev_i(t)<5\\ g(\sum_{i=1}^{n}Ev_i(t)w_i) & if\ Ev_i(t)\geq 5\end{cases}, \tag{11}$$

where *E(t)* is integrated cyber attack situation value. $Ev_i(t)$ means the situation values of *i*-th types of typical cyber attack, and w_i is the corresponding weight values. *g(x)* is a normalization function. θ is a threshold that obtained by expert experience and history data mining.

(7) Evaluate quantitatively cyber attack situation in SDN network referring to the cyber security state level table defined in [29]. In our work, we divide the cyber attack situation level into excellent, fine, middle, poor and danger with every level corresponding to a range, [0, 2.0), [2.0, 4.0), [4.0, 7.5), [7.5, 9.0) and [9.0, 10.0], respectively, and with the corresponding weight values are 0.06, 0.11, 0.21, 0.26 and 0.36, respectively.

6 Experimental Analysis

6.1 Introduction to Experimental Environment

In our work, we used the experiment simulation to establish the test scenario. We used Mininet [4] to create a realistic virtual SDN environment, and simulated OpenFlow flooding attack, network scanning attack, ARP attack and switch compromised attack by referring to [30]. 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 [31] aims to define how an SDN controller communicates with the SDN switches by using OpenFlow protocol. It is a special component in software defined network, that supports universal OpenFlow protocol that is introduced in section 2.2.

(2) Ryu controller [32] 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 [33] 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 our experiment, we used a physical machine with Intel I5 with 2.5GHz and 8GB memory to be the physical infrastructure, and used Mininet to establish a simulated experiment environment based on the infrastructure. The brief network structure and topology is as shown in Fig. 3.

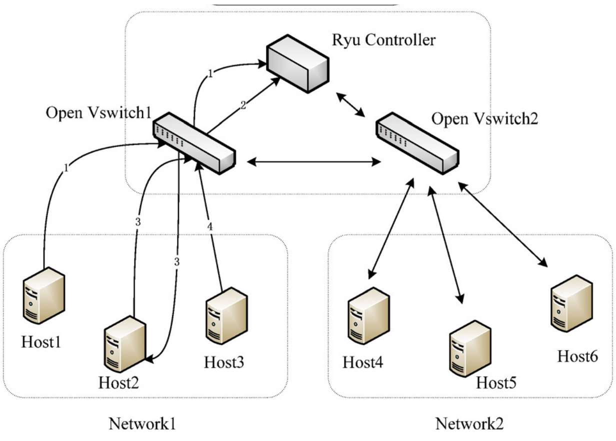

Fig. 3. Brief network structure and topology in experiment

In our 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. We first simulated different attacks in network2 in order to generate a large number of attack data, that is to be as the history data to be used to train our FCM model structured in network1 in next step. All the four types of typical cyber attacks are simulated with Scapy in network1. The attack traffics are labeled as lines with numbers in Fig. 3. Traffic 1 and 2 represent flooding attack to the controller while traffic 1 is launched from Host1 and traffic 2 is from vswitch1. Traffic 3 is the ARP cache poisoning and flooding attack launched by host2. Traffic 4 denotes the flows which are forwarded to host3 when the switch is compromised. Host4 launches the network scanning attacks.

6.2 Process of Experiment

In our experiment, we simulated respectively four typical attacks in SDN. We set the time interval for detection loop to 10 seconds. We programmed the two switches to obtain the flow tables in every 10 seconds during extracting features. Because of the limited storage space for flow tables, we record and export the information in the flow tables into a format file by the timestamp as well as by the duration time of each flow. In our experiment, we continuously collected and recorded all the information in flow tables from time 0 to 1800. We simulated OpenFlow flooding attack (OFA) 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, our experimental network was under normal situation, that means there were no simulated cyber attacks occurred. The following is the test steps in our experiment.

(1) Structure FCM model, where we chose all the 13 cyber attack features in section 4.2 as the concept nodes, and we determined the adjacent matrix of FCM model using the weight learning method proposed in [28]. The FCM structure chart is as follows in Fig. 4.

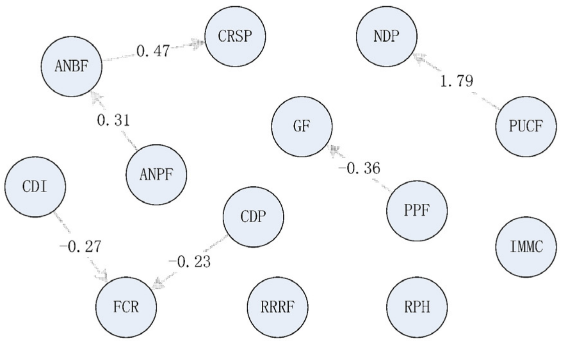

Fig. 4. FCM model structure of features

(2) Compute respectively the values of all the 13 cyber attack features during time 0 to 1800 using the computing and statistics methods in section 4.3. In the process of computing and statistics, we used a sample of 135 feature values, that were equidistance sampling during time 0 to 1800. Table 2 shows the brief details about 135 sample feature values.

Table 2. Brief original feature values at different time

Time	ANPF	ANBF	PPF	CRSP	GF	NDP	RPH	PUCF	RRRF	IMMC	FCR	CDI	CDP
1	41.00	2202	97.27	0.34	2.00	5.00	1.00	26.89	98.73	1.00	0.00	0.56	0.50
20	88.00	1279	90.07	0.50	2.00	5.00	1.00	16.99	98.45	1.00	0.18	0.82	0.72
40	96.00	895	95.33	0.50	2.00	3.00	2.00	18.34	98.17	1.00	0.06	0.78	0.96
60	63.00	1718	91.04	0.32	1.00	556	0.00	98.96	98.6	1.00	0.16	0.70	0.76
80	107.00	1889	93.74	0.22	3.00	4.00	0.00	13.2	54.28	1.10	0.14	0.88	0.56
100	91.00	1521	94.32	0.64	3.00	2.00	5.00	16.71	99.18	1.00	0.48	0.62	0.30
120	23.00	1723	90.92	0.94	3.00	4.00	4.00	9.41	99.88	1.00	0.66	0.12	0.20
135	43.00	908	93.33	0.82	2.00	590	0.00	95.35	99.03	1.00	0.00	0.88	0.56

(3) Calculate out respectively the values of all 13 cyber attack features according to 135 sample feature values using equation (9) based on FCM model during time 0 to 1800. Table 3 shows the brief details in 135 feature values after considering the interrelations and restrictive correlations between any two different features modeled by structured FCM model in previous step, where $w_{(ANBF,\ CRSP)}=0.47$, $w_{(ANPF,\ ANBF)}=0.31$, $w_{(CDI,\ FCR)}=-0.27$, $w_{(CDP,\ FCR)}=-0.23$, $w_{(CUPF,\ NDP)}=1.79$ and $w_{(PPF,\ GF)}=-0.36$. And all the feature values about four typical cyber attacks during their respective attack process are as shown from Fig. 5 to Fig. 9.

Table 3. Brief final feature values at different time

Time	ANPF	ANBF	PPF	CRSP	GF	NDP	RPH	PUCF	RRRF	IMMC	FCR	CDI	CDP
1	2.93	6.90	9.75	3.04	0.34	0.04	2.00	2.33	9.75	4.29	0.00	5.83	5.21
20	6.29	4.01	9.03	4.78	0.34	0.04	2.00	1.27	9.69	4.29	2.00	8.54	7.50
40	6.86	2.80	9.55	4.78	0.34	0.02	4.00	1.42	9.64	4.29	0.67	8.13	10.00
60	4.50	5.38	9.12	2.82	0.00	5.82	0.00	9.99	9.72	4.29	1.78	7.29	7.92
80	7.64	5.92	9.39	1.73	0.69	0.03	0.00	0.87	0.98	7.14	1.56	9.17	5.83
100	6.50	4.77	9.45	6.30	0.69	0.01	10.00	1.24	9.84	4.29	5.33	6.46	3.13
120	1.64	5.40	9.11	9.56	0.69	0.03	8.00	0.47	9.98	4.29	7.33	1.25	2.08
135	3.07	2.85	9.35	8.26	0.34	6.17	0.00	9.61	9.81	4.29	0.00	9.17	5.83

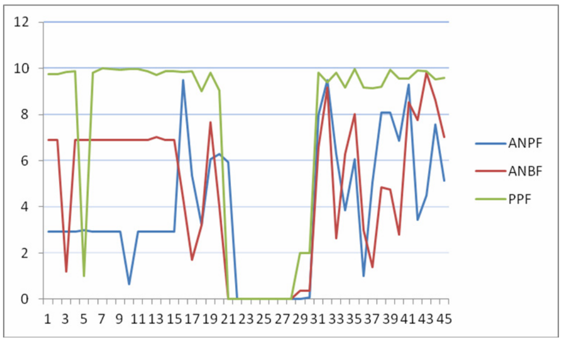

Fig. 5. Trend of ANPF, ANBF and PPF

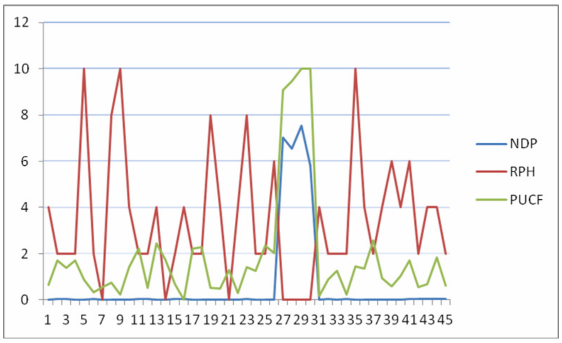

Fig. 6. Trend of NDP, RPH and PUCF

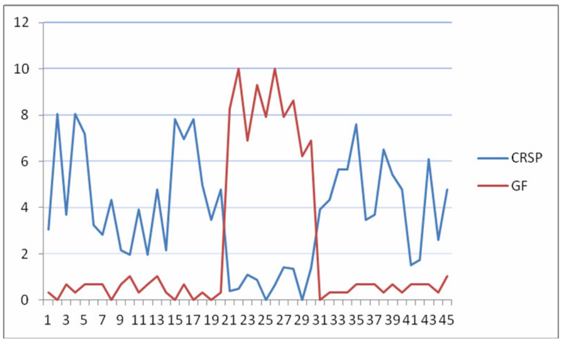

Fig. 7. Trend of CRSP and GF

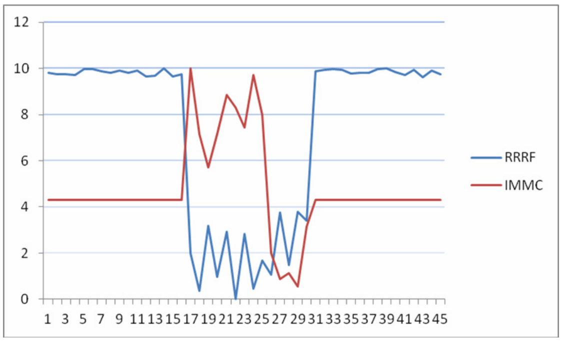

Fig. 8. Trend of RRRF and IMMC

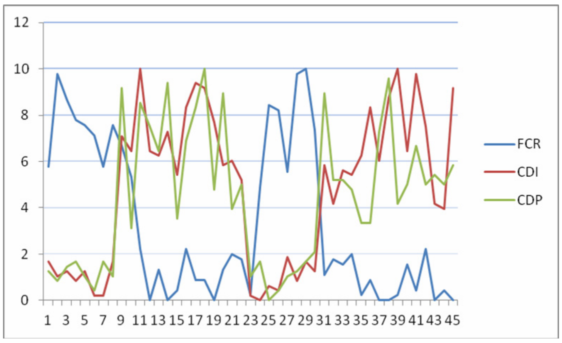

Fig. 9. Trend of FCR, CDI and CDP

(4) Use equation (10) to calculate out the cyber attack situation values of four types of typical cyber attack (OFA,NSA, ARPA and SCA), that means we compute the probability of occurrence about four types of typical cyber attack during different attack periods, and each weight set of the 13 cyber attack features in third layer index are $w_1=\{0.29, 0.16, 0.30, 0.14, 0.11\}$, $w_2=\{0.51, 0.17, 0.34\}$, $w_3=\{0.77, 0.23\}$, $w_4=\{0.28, 0.49, 0.23\}$. The details are in Table 4 and as shown from Fig. 10 to Fig. 13.

Table 4. Brief situation values at different time

time	OFA	NSA	ARPA	SCA	ICAS
1	5.60	2.25	9.80	4.46	1.62
20	6.16	1.70	9.75	7.72	1.17
40	6.11	2.81	9.71	8.08	2.42
60	5.18	8.23	9.77	7.24	5.78
80	6.50	0.44	4.98	7.03	4.48
100	7.38	5.85	9.87	6.27	4.82
120	6.89	4.41	9.98	4.28	1.28
135	5.94	8.21	9.85	6.31	5.68

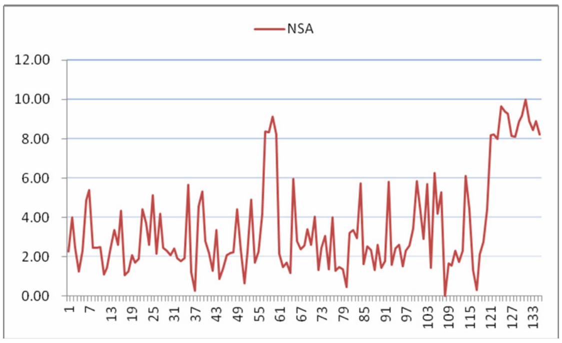

Fig. 10. Trend of NSA

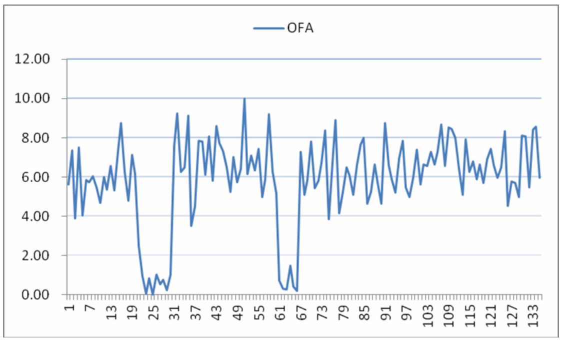

Fig. 11. Trend of OFA

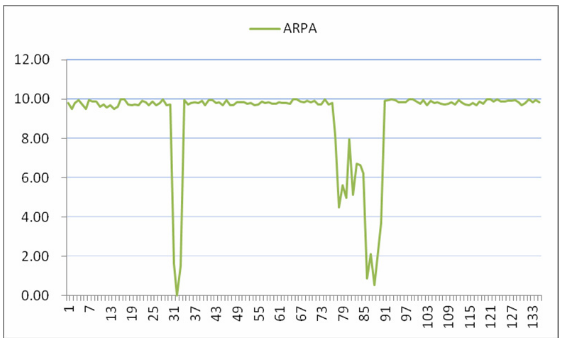

Fig. 12. Trend of APRA

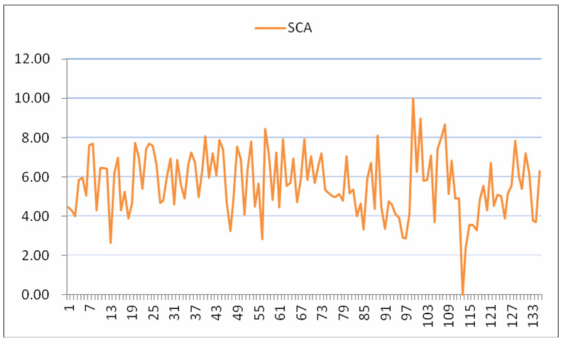

Fig. 13. Trend of SCA

(5) Use equation (10) to calculate out the integrated cyber attack situation (ICAS) values in our experimental simulation environment, that means we compute the probability of occurrence about different cyber attacks during time 0 to 1800, and each weight set of four cyber attacks in second layer index are *w={0.26, 0.12, 0.39, 0.23}*. The details are in Table 4 and from Fig. 10 to Fig. 13.

(6) Evaluate quantitatively the integrated cyber attack situation in our SDN network environment during the time 0 to 1800 referring to the cyber security state level table defined in [29]. In our experiment, we divide the cyber attack situation level into excellent, fine, middle, poor and danger with every level corresponding to a range. They are [0, 2.0), [2.0, 4.0), [4.0, 7.5), [7.5, 9.0) and [9.0, 10.0], respectively. The details are as shown in Fig. 14.

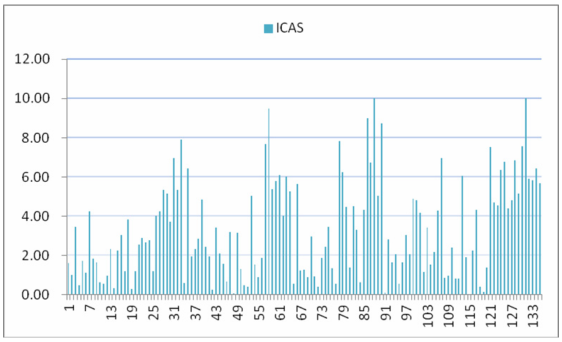

Fig. 14. Trend of ICAS

As from the Fig. 14, we can find that there is a poor cyber attack situation level in the sample 31 with the corresponding about time 400, where the OpenFlow flooding attack occurred. In addition, there is danger cyber attack situation level in the sample 57, 86 and 129 with the corresponding about time 750, 1160 and 1600, where the network scanning attack, ARP attack and switch compromised attack occurred respectively. In our experiment, the results show our method can accurately reflect the cyber attack situation in software defined network.

6.3 Related Works Comparison

In the field of cyber attack situation evaluation in SDNs, there are several related methods was proposed. In [34], the authors proposed an effective security assessment mechanism based on attack graphs and analytic hierarchy process for software defined networking-based mobile networks. They analyzed the new characteristics of SDN-MNs and introduced a dynamic nature and complexity into mobile networks. In [35], the authors proposed a method based on traffic data and the corresponding topology, it gave security software defined network by combining with business process model of cloud computing, and optimized network security algorithm. In [36], the authors proposed a measurement method which allows collecting network traffic flow parameters. The method is based on self-organized maps of artificial neural network, it was used to detect DDoS attack in SDNs. In [3], we proposed a security situation awareness approach for SDN. The method is based on multiple observations hidden Markov model. However, its accuracy need to be improved. Therefore, in this paper, we proposed a cyber attack situation evaluating method based on multi-dimensional features analysis in SDN. During the evaluation process, we emphatically considered the method of four typical cyber attack features extraction and the interrelations and restrictive correlations between any two different features. The related works comparison is in Table 5.

Table 5. Related works comparison

Different Methods	Key Theories and Techniques	Advantage	Defect	Application Scene
Method in [34]	Based on attack graphs and analytic hierarchy process	Applied in real 5G mobile network	Unbalanced scale of judgment	5G mobile network in real environment
Method in [35]	Based on traffic data combined with business process model and OpenFlow protocol	Applied in real cloud computing	Single network traffic data sources	Cloud computing in real environment
Method in [36]	Based on self-organized maps of artificial neural network	Effective accuracy for DDoS detection	Only DDoS detection	Universal model in experimental environment
Method in [3]	Based on multiple observations hidden Markov model	Multiple observations and multiple attacks detection	Accuracy need to be improved	Universal model in experimental environment
Method in paper	Based on multi-dimensional features analysis and fuzzy cognitive maps	Multiple-dimensional features analysis and multiple attacks detection	Further verifying in real environment	Universal model in experimental environment

6.4 Discussion

In our experiment, we simulated respectively four typical cyber attacks in SDN. During time 200 to 400, we simulated OpenFlow flooding attack. During time 600 to 800, we simulated network scanning attack. During time 1000 to 1200, we simulated ARP attack. During time 1400 to 1600, we simulated switch compromised attack. Other remaining 5 sustained 200 time periods had no attacks, that means during this periods, the cyber attack situation is at the normal level.

The trend of features about OpenFlow flooding attack are shown in Fig. 5 and Fig. 6. Obviously, there are sharp changes when the attack was lunched. In the same way, there also are sharp changes when network scanning attack, ARP attack and switch compromised attack occurred as same as shown from Fig. 6 to Fig. 9. Therefore, as shown in the chart, our cyber attack features extraction method is reasonable and effective to indicate the four typical kinds of cyber attack in our experiment.

We considered the cyber attack features extraction and the interrelations and restrictive correlations between any two different cyber attack features. Because Fuzzy Cognitive Maps (FCM) has the ability to describe the causal relationship between any two concept nodes, we used FCM model to describe the interrelations and restrictive correlations between any two different features in order to find the interrelationships among features during the process of continuous attack in the experiment. Fig. 4 shows the FCM structure about attack feature, where the directed arcs reflect the inner causal relationship, and weights of directed edges describe the influence degree of causal relationship. We determined the adjacent matrix of FCM model using the weight learning method according to the history data, that was generated in network2 before.

The inner causal relationships were obviously displayed in Fig. 5 to Fig. 9. For example, there is a positive correlation between ANPF and ANBF, and the linear correlation coefficient is 0.31, that is determined by the weight learning method according to the history data. In reality, the mean is as follow. During the attack process, when the average number of bytes per flow is increased, the average number of packets per flow will also be increased, and there is a positive correlation growth rate between them. Furthermore, as shown in form Fig. 10 to Fig. 13, we can verify the effectiveness of the inner relationships between any two different cyber attack features from another view. As from the Fig. 14, we can find the different cyber attack situation levels (one poor level and three danger levels) when the SDN network is under attack. In our experiment, the results show our method can accurately reflect the cyber attack situation in software defined network.

7 Conclusion

In this paper, we proposed an improved method to evaluate cyber attack situation in the software defined networks. Our 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, we referred to the relevant literature, then defined 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. We collected all the original network information from the flow tables and calculated all the values of features according to our computation and statistics methods. In the process of cyber attack features relationships analysis, we completed the features data normalization based on the features extraction, and structured model using fuzzy cognitive maps (FCM) to analyze the interrelations and restrictive correlations between any two different features. Then, we calculated the final values of cyber attack features and worked out the four typical attack situations and integrated cyber attack situation in SDN.

In experiment, our cyber attack feature computation and statistics methods were achieved in SDN environment by programming to detect the typical four cyber attacks and generated all 13 values of cyber attack feature. Then we choose all the 13 cyber attack features as the concept nodes, and determined the adjacent matrix of FCM model using the least squares method to learn the weights in FCM model. Finally, we calculated 13 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 our method can accurately reflect the trend of cyber attack situation in software defined network

While our method is used in practical application, several problems should be considered. Firstly, how to extend more reasonable cyber attack features to describe a certain cyber attack. Secondly, the accurate and enough SDN network information collection is needed. In summary, this paper is just a first step toward the cyber attack situation evaluation in SDN environment, and we will continue this work for further enhancement. The future research will include adding computation methods for other kinds of cyber attack feature and improving the relationship represent model. Furthermore, strengthening the accuracy of our method will also be considered.

Acknowledgements

This work is supported in part by the National Key R & D Program of China under Grant 2017YFC0803702 and 2017YFB0802302.

References

[1] K. Benzekki, A.E. Fergougui, A.E. Elalaoui, Software-defined networking (SDN): a survey, Security and Communication Networks 9(18)(2016) 5803-5833.

[2] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, J. Turner, Openflow: Enabling innovation in campus network, ACM SIGCOMM Computer Communication Review 38(2)(2008) 69-74.

[3] Z. Fan, Y. Xiao, A. Nayak, C. Tan, An improved network security situation assessment approach in software defined networks, Peer-to-Peer Networking and Applications 12(22)(2017) 1-15.

[4] R.L.S. de Oliveira, A.A. Shinoda, C.M. Schweitzer, L. R. Prete, Using mininet for emulation and prototyping software-defined networks, in: Proc. 2014 IEEE Colombian Conference on Communications and Computing (COLCOM), 2014.

[5] E. Haleplidis, K. Pentikousis, S. Denazis, J.H. Salim, D. Meyer, O. Koufopavlou, RFC 7426: Software Defined Networking (SDN): Layers and Architecture Terminology, IETF, 2015.

[6] S. Scott-Hayward, G. O'Callaghan, S. Sezer, SDN security: a survey, in: Proc. 2013 IEEE SDN for Future Networks and Services (SDN4FNS), 2013.

[7] H.-C. Wei, Y.-H. Tung, C.-M. Yu, Counteracting UDP Flooding Attacks in SDN, in: Proc. 2016 IEEE NetSoft Conference and Workshops (NetSoft), 2016.

[8] T.V. Phan, N.K. Bao, M. Park, Distributed-SOM A novel performance bottleneck handler for large-sized software-defined networks under flooding attacks, Journal of Network and Computer Applications 91(1)(2017) 14-25.

[9] A. Kalliola, K. Lee, H. Lee, T. Aura, Flooding DDoS Mitigation and Traffic Management with Software Defined Networking, in: Proc. 2015 IEEE 4th International Conference on Cloud Networking (CloudNet), 2015.

[10] T.V. Phan, T.V. Toan, D.V. Tuyen, T.T. Huong, OpenFlowSIA: an optimized protection scheme for software-defined networks from flooding attacks, in: Proc. 2016 IEEE Sixth International Conference on Communications and Electronics (ICCE), 2016.

[11] F. Schneider, R. Bifulco, A. Matsiuk, Better ARP handling with InSPired SDN switches, in: Proc. 2016 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), 2016.

[12] H. Ma, H. Ding, Y. Yang, Z. Mi, J.-Y. Yang, Z. Xiong, Bayes-based ARP attack detection algorithm for cloud centers, Tsinghua Science and Technology 21(1)(2016) 17-28.

[13] D. Smyth, V. Cionca, S. McSweeney, D. O'Shea, Exploiting pitfalls in software-defined networking implementation, in: Proc. 2016 International Conference on Cyber Security And Protection of Digital Services (Cyber Security), 2016.

[14] F. Ubaid, F.B. Ubaid, R. Amin, M.M. Iqbal, Mitigating address spoofing attacks in hybrid SDN, International Journal of Advanced Computer Science and Applications 8(4)(2017) 562-570.

[15] K. Sun, S. Jajodia, Protecting enterprise networks through attack surface expansion, in: Proc. 2014 ACM Workshop on Cyber Security Analytics, Intelligence and Automation, 2014.

[16] J. Xu, P. Guo, M. Zhao, R.F. Erbacher, M. Zhu, P. Liu, Comparing different moving target defense techniques, in: Proc. 2014 ACM SIGSAC Conference on Computer and Communications Security, 2014.

[17] J.H. Jafarian, E. Al-Shaer, Q. Duan, Openflow random host mutation: transparent moving target defense using software defined networking, in: Proc. The ACM first workshop on hot topics in software defined networks, 2012.

[18] J.H. Jafarian, E. Al-Shaer, Q. Duan, Spatio-temporal address mutation for proactive cyber agility against sophisticated attackers, in: Proc. The First ACM Workshop on Moving Target Defense, 2014.

[19] D. Yu, A.W. Moore, C. Hall, R. Anderson, Authentication for resilience: the case of SDN, Cambridge International Workshop on Security Protocols 8263(2013) 39-44.

[20] M. Antikainen, T. Aura, M. Sarela, Spook in your network: attacking an SDN with a compromised OpenFlow switch, in: Proc. Nordic Conference on Secure IT Systems, 2014.

[21] P.-W. Chi, C.-T. Kuo, J.-W. Guo, C.-L. Lei, How to detect a compromised SDN switch, in: Proc. 2015 1st IEEE Conference on Network Softwarization (NetSoft), 2015.

[22] Y. Jia, X. Wang, YHSSAS: large-scale network oriented security situational awareness system, Computer Science 41(11)(2011) 259-262.

[23] R. Braga, E. Mota, A. Passito, Lightweight DDoS flooding attack detection using NOX/OpenFlow, in: Proc. 2010 IEEE 35th Conference on Local Computer Networks (LCN), 2010.

[24] W. Fuertes, P. Zambrano, M. Sanchez, P. Gamboa, Alternative engine to detect and block port scan attacks using virtual network environments, International Journal of Computer Science and Network Security 11(11)(2011) 14-23.

[25] M.Z. Masoud, Y. Jaradat, I. Jannoud, On preventing ARP poisoning attack utilizing Software Defined Network (SDN) paradigm, in: Proc. 2015 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT), 2015.

[26] V. Tilborg, H.C. Henk, J. Sushil, Encyclopedia of Cryptography and Security, Springer Science & Business Media, 2014.

[27] B. Kosko, Fuzzy cognitive maps, International Journal of Man-Machine Studies 24(1996) 65-75.

[28] Y. Zhang, X. Liu, Weights learning of fuzzy cognitive maps, Journal of Chinese Computers Systems 34(5)(2013) 1147-1153.

[29] Z. Wang, Research of network security situation evaluation based on index system, [dissertation] Changsha: National University of Defense Technology, 2010.

[30] B. Ballmann, Understanding Network Hacks: Attack and Defense with Python, Springer Science & Business Media, 2015.

[31] M. Jones, Virtual networking in Linux, IBM developer works. <https://www.ibm.com/developerworks/linux/library/l-virtual-networking/>, 2010 (accessed 17.09.14).

[32] A. Shalimov, D. Zuikov, D. Zimarina, V. Pashkov, R. Smeliansky, Advanced study of SDN/OpenFlow controllers, in: Proc. The ACM 9th Central & Eastern European Software Engineering Conference in Russia, 2013.

[33] T.H. Kobayashi, A.B. Batista, A.M. Brito, P.S.M. Pires, Using a packet manipulation tool for security analysis of industrial network protocols, in: Proc. 2007 IEEE Conference on Emerging Technologies and Factory Automation (EFTA), 2007.

[34] S. Luo, M. Dong, K, Ota, J. Wu, J. Li, A security assessment mechanism for software-defined networking-based mobile networks, Sensors 15(12)(2015) 31843-31858.

[35] J. Zhou, N. Liu, Attack detection research for software defined network, International Journal of Security and Its Applications 10(8)(2016) 343-352.

[36] D. Jankowski, M. Amanowicz, Intrusion detection in software defined network with self-organized maps, Journal of Telecommunications and Information Technology 4(2015) 3-9.