IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

SPECIAL SECTION ON SECURITY AND PRIVACY FOR VEHICULAR NETWORKS

Received June 10, 2018, accepted July 5, 2018, date of publication July 9, 2018, date of current version September 5, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2854567

An Efficient SDN-Based DDoS Attack Detection and Rapid Response Platform in Vehicular Networks

YAO YU, (Member, IEEE), LEI GUO, (Member, IEEE), YE LIU, JIAN ZHENG, AND YUE ZONG
School of computer science and engineering, Northeastern University, Shenyang 110819, China

Corresponding authors: Yao Yu (yuyao@mail.neu.edu.cn) and Lei Guo (guolei@cse.neu.eud.cn)

This work was supported in part by the Fundamental Research Funds for the Central Universities under Grant N161613004 and in part by the General Armament Department and Ministry of Education United Fund under Grant 6141A02033307.

ABSTRACT With the prosperity of wireless networks, vehicular networks (VNs) have been extensively studied in recent years. It is deployed to ensure road safety, enhance the driving experience, and reduce traffic congestion. However, VNs are vulnerable to various attacks, especially Distributed Denial of Service (DDoS) that attackers control a large number of compromise nodes inside the networks to occupy the network resources of legitimate users and impact the communication among vehicles and between vehicles and infrastructure. In this paper, we design a platform to efficiently detect and rapidly respond to the DDoS attack in VNs based on software-defined networking (SDN). The proposed platform not only contains the trigger mechanism based on the message of OpenFlow protocol (i.e., PACKET_IN message) for a response not timely but also involves a flow feature extraction strategy based on the multi-dimensional information. Moreover, we construct an effective global network flow table feature values based on OpenFlow flow table feature and the entropy feature of flow table entry. We determine all flow table entry by the trained SVM. By analyzing the simulation results, we verify that the detection scheme effectively reduces the time for starting attack detection and classification recognition and has a lower false alarm rate.

INDEX TERMS Vehicular and wireless tehnoloiesia, software defined networking, DDoS, detection algorithms, support vector machines.

I. INTRODUCTION

Vehicular Networks (VNs) have been envisioned to meet the imminent demands for improving transportation efficiency and road safety, reducing accidents, and mitigating the overall impacts of heavy traffic congestion. VNs are no longer a futuristic promise, but potentially provide surveillance services, safety traffic management services, and mobile vehicular cloud services [1]. Due to the lack of centralized control nodes in the VNs, data is stored and forwarded between vehicles. It means that the role of each vehicle node is critically important, equivalent to the storage and forwarding functions of routers and switches in common networks. Vehicle nodes cooperate with each other, forwarding data and delivering messages. Because of compromised nodes maliciously occupying network resources and reducing network performance, Distributed Denial of Service (DDoS) attack greatly reduces the degree of collaboration of data forwarding between vehicle nodes, decreases the packet transmission speed and throughput in VNs, affect the quality of network communications, and cause serious consequences.

Software Defined Networking (SDN), as a new type of network architecture, has certain advantages in DDoS attack detection. Compared with traditional circuit-switched networks, SDN adopts a separated control and forwarding mode of operation and make the network programming. With the deepening and development of SDN research, the application of SDN network architecture in the traditional VNs architecture has better performance in security management.

The emergence of SDN paradigm has created tremendous potential for the development of VNs. Different from traditional VNs, Software Defined Vehicular Networks (SDVNs) have rich management advantages due to the centralized intelligent control brought by SDN [2]. As shown in Figure 1, the SDN framework introduces application plane and control plane to VNs. The application plane is designed to provide a set of services and applications. The control plane,

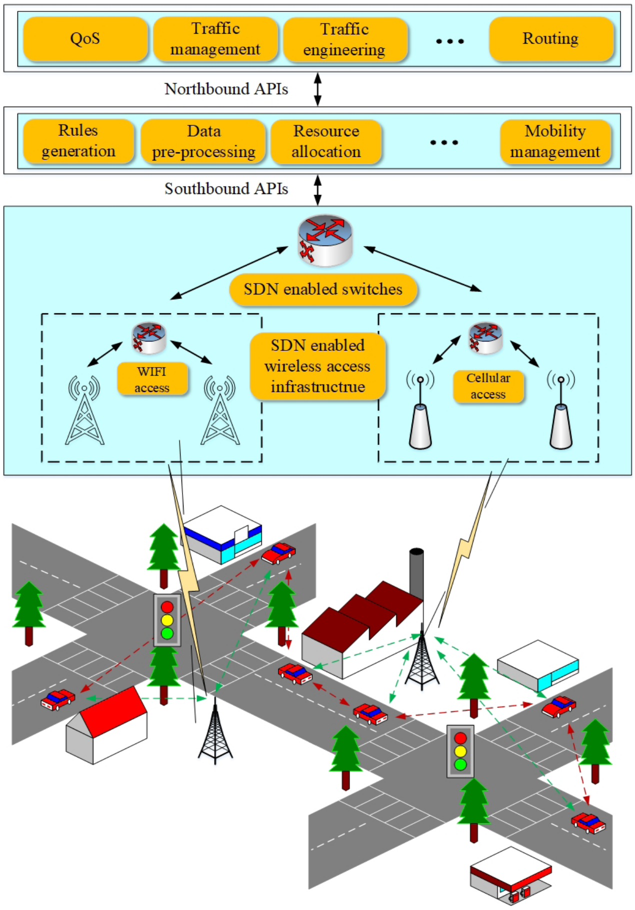

FIGURE 1. Deploying SDN framework in VNs.

namely the control plane of SDN, contains the controller of the software platform which represents the centralized core of the network intelligence and is the core decision point of the entire SDVNs architecture. In addition, the control plane contributes to the programmability of the network and the abstraction of the underlying resources. The data plane of SDVNs mainly contains the underlying network resources. The upper data plane contains forwarding hardware, e.g. SDN-capable switches and routers. This plane is also called the infrastructure plane of SDN system. The lower data plane is primarily constructed and networked VNs, including vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) [3]. In addition, the northbound interface represents the enablement of application-to-control plane communication through the Application Programming Interface (API). The southbound interface represents the enablement of the control plane to the data plane through the API. The eastbound and westbound APIs are used to communicate back and forth between controllers in a network environment.

In this paper, we design a DDoS attack detection system platform based on SDN by researching the DDoS attack detection scheme based on SDN network architecture in VNs. The objectives of our work can be summarized as follows:

1) Design a trigger module based on PACKET_IN message, optimize the performance of the controller and shorten the attack time of the platform.

2) Describe a DDoS attack detection method based on the feature combined with the feature of OpenFlow protocol.

3) Analyze the flow table of the SDN network architecture and combine the feature of entropy for feature extraction.

4) Propose a flow feature selection scheme based on protocol type on the basis of flow feature extraction to further the network detection performance.

The rest of the paper is structured as follows. In the next section we briefly introduce the relevant preliminary knowledge of platform implementation. In Section III we introduce the entire platform architecture and describe the workflow of the platform. In Section IV we present the core mechanisms of the detection trigger module, flow table item collection module, and attack detection module function. In Section V we describe the simulation of the platform and give simulation analysis. We conclude the paper in Section VI.

II. RELATED WORK

The concept of VNs comes from the Internet of things (IoT) [4], which is an integrated network that implements intelligent traffic management [5], intelligent dynamic information services and vehicle intelligent control [2] in accordance with the agreed communication protocols and data interaction standards [30], [31]. Efficient and lightweight intrusion detection mechanism for vehicular network (ELIDV) [3] that aims to protect the network against three kinds of attacks: Denial of Service (DoS), integrity target, and false alert's generation. ELIDV is based on a set of rules that detects malicious vehicles promptly and with high accuracy. DoS attacks have high impact on periodical exchanged messages of safety applications in VNs. A real-time Medium-Access Control-based (MAC-based) detection method [7] is proposed to meet the requirements of safety applications in VNs. An efficient broadcast authentication scheme called Prediction-Based Authentication (PBA) [8] can not only defend against computation-based DoS attacks, but also resist packet losses caused by high mobility of vehicles. Therefore, DDoS attack is an obstacle that needs to be overcome in the future deployment of VNs to realize the intelligent transportation network [9], [10].

Just like [13], most of the existing DDoS attack anomaly detection algorithms in SDN [11] is employed in the anomaly detection method in the traditional network. The entropy-based statistical analysis algorithm [14], [15] is a common DDoS detection method, this method is real-time and can handle a lot of traffic data. What‘s more, this method has lower cost of calculation. Many researches such as [16], [17] have used entropy-based methods to solve security problems. Therefore, the paper combines the flow-based feature of SDN and the statistical analysis algorithm based on entropy to propose a scheme of flow-based entropy feature extraction. This method can reduce communication overhead due to detecting OpenFlow network attacks on a small time scale.

Another network anomaly detection algorithm is based on machine learning and cognitive algorithms, and it is also effectively applied to SDN-based DDoS attack detection. Lightweight DDoS attack detection algorithm based on traffic flow feature is proposed in [19], the algorithm uses the NOX controller to process switch information and performs flow analysis based on Self Organizing Maps (SOM). An Artificial Neural Network (ANN) algorithm is selected by [20]. The SVM classifier detects DDoS attack by analyzing data and classifying them through using feature attribute patterns [21]. This paper adopts DDoS attack detection based on flow table entry analysis and uses machine learning methods to identify DDoS attack based on the advantages of machine learning technology for detecting abnormal behaviors based on the network.

III. PRELIMINARIES

A. CORRELATION MEASURE

Correlation measure, also known as association criterion or similarity criterion, reflects the closeness of correlation between variables by correlation coefficients. The correlation coefficient between and can be formulated as (1):

$$r(X,Y) = \frac{\sum_{i=1}^{N}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{N}(x_i-\bar{x})^2\sum_{i=1}^{N}(y_i-\bar{y})^2}} \tag{1}$$

In (1), $\bar{y}$ and $\bar{x}$ represent the expected value of the feature variables X and Y, respectively. If $r(X,Y)$ is large, it means that X and Y are highly related; otherwise, X and Y are less related.

B. SVM

Support Vector Machine (SVM) is a new learning method based on statistical learning theory proposed by Vapnik. It is a two-class classification model whose basic model is the linear classifier with the largest interval defined in the feature space [22]. The basic idea of SVM learning is to solve the separated hyperplanes that can divide the training datasets correctly and have the largest geometric interval. Finding the hyperplane with the largest geometrical interval for the training datasets means classifying the training data with sufficient confidence.

The SVM becomes a virtually non-linear classifier because it includes kernel techniques. The idea of nuclear techniques is to define only the kernel functions in the process of learning and forecasting without explicitly defining the mapping functions.

Definition of Kernel Function: Assuming χ is the input space, H is the feature space. If there is a mapping from χ to H: $\phi(x) : \chi \rightarrow H$, makes the function $K(x,z)$ satisfy the condition $K(x,z) = \phi(x) \cdot \phi(z)$ for all $x, z \in \chi$. $K(x,z)$ is a kernel function, $\phi(x)$ is a mapping function, and $\phi(x) \cdot \phi(z)$ is the inner product between $\phi(x)$ and $\phi(z)$.

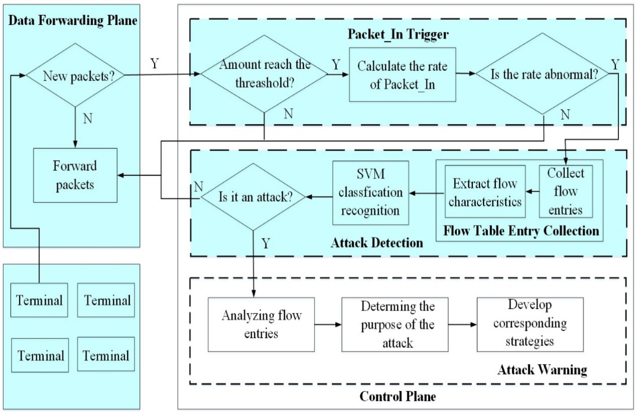

FIGURE 2. DDoS attack detection system framework.

The following are several commonly used kernel functions:

1) Linear kernel function: $K(x,z) = (x \cdot z + 1)^p$;
2) Polynomial kernel function: $K(x,z) = (x \cdot z + 1)^p$;
3) Gaussian kernel function: $K(x,z) = \exp\left(-\frac{\|x-z\|^2}{2\sigma^2}\right)$

IV. SYSTEM PLATFORM ARCHITECTURE

Figure 2 shows the system framework of the DDoS attack detection system platform based on SDN, there are mainly four modules in the DDoS attack detection process, including: detection trigger module, flow table item collection module, attack detection module, and attack warning module. In this paper, we primarily discuss the first three modules. The module design for the platform is based on the Floodlight controller. Floodlight is an open source SDN controller based on Java. Some existing Floodlight modules have been used in the entire structure, and the improved and added function modules are mainly located in control plane and application plane.

Data forwarding plane is used to forward network traffic, including switches and terminals supporting the OpenFlow protocol. The switch matches the received data packet and flow entry according to the matching rules, performs the corresponding operations on the flow entry for successful packets, and updates the counter at the same time. In addition, the terminal generates traffic to simulate normal flow and abnormal flow and applies it into the SDN network.

In order to achieve optimized services, control plane abstracts the control part of the traditional switching equipment into a network operating system, centralizes maintenance and management of network equipment through the southbound interface, and provides northbound programming interfaces to upper-plane services and applications. The SDN controller controls the network devices in the global scope. Therefore, the instant network traffic information may be obtained through a PACKET_IN message uploaded by the network devices or the flow entry periodically queried on the device. Specifically, the attack detection trigger module in the control plane determines when to start the attack detection module through the PACKET_IN message abnormality

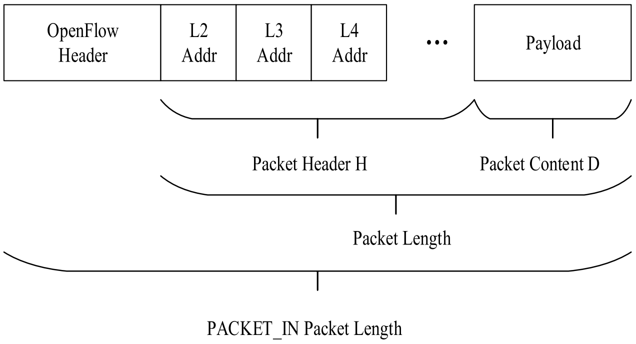

FIGURE 3. **PACKET_IN composition.**

detection algorithm. The activated attack detection module determines whether a DDoS attack occurs through the operation steps of flow table entry collection, flow signature extraction, and SVM classification and identification.

V. IMPLEMENTATION OF PLATFORM FUNCTIONS

A. EQUATIONS

The existing periodic detection trigger mechanisms used by systems for against DDoS attack is difficult to quickly identify and defend against attack, resulting in excessive workload for controllers and switches when attacks occur. In order to deal with the above problems, this paper proposes a PACKET_IN message anomaly detection algorithm as a platform detection trigger mechanism.

Figure 3 shows the composition of the PACKET_IN packet. Each time the SDN controller receives the PACKET_IN, it can parse out the entire original data packet to obtain the head of the data packet. Then it will create a new flow record, and fill in the corresponding head matching field in the record according to the parsed result. Finally, the number of packets PACKET_COUNT is set to 1 in the flow, and the byte count BYTE_COUNT is set as the packet size.

Whether or not a DDoS attack is initiated by IP spoofing, a large number of PACKET_IN messages are created and sent to the controller. We propose the PACKET_IN trigger mechanism based on the feature of PACKET_IN message, and detect the PACKET_IN message through its rate anomaly.

In our algorithm, we first initialize some variables. We initialize *Windows_value* to a certain number of PACKET_IN and set *Speed_threshold* to a large enough number. We use *PkIn_count* to count the number of PACKET_IN messages received by the controller. *Windows_value* and *PkIn_count* do the modular arithmetic. If the calculation result is zero, current time t_{now} will be recorded, and then calculate the time interval ΔT between the current time t_{now} and the last time t_{pre}. Otherwise, the controller is notified to process the PACKET_IN. Then calculate the rate of PACKET_IN *PkIn_speed* by dividing window value by time interval ΔT. If *PkIn_speed* exceeds the rate threshold, an abnormal condition will be reported. Otherwise, the controller is notified to process the PACKET_IN.

The PACKET_IN trigger mechanism captures the symptoms of a DDoS attack when symptoms occur and initiate attack detection. Compared with the periodic triggering, the PACKET_IN trigger can significantly reduce the response time to the attack, and it can also reduce the controller's negative.

The algorithm steps as follows:

Algorithm 1 PACKET_IN Message Anomaly Detection

```
Input: PACKET_IN messages
Output: Whether the PACKET_IN message is abnormal?
1: Initialize $Windows\_value$, $Speed\_threshold$
2: if a PACKET_IN message arrives then
3:   $PkIn\_count = PkIn\_count + 1$;
4:     if $PkIn\_count$ mod $Windows\_value == 0$ then
5:     Record the time $t_{now}$;
6:     $\Delta T = t_{now} - t_{pre}$;
7:     $PkIn\_speed = Windows\_value/\Delta T$;
8:   else
9:       Notify the controller to process PACKET_IN messages;
10:  end if
11:  if $PkIn\_speed > Speed\_threshold$ then
12:    return abnormal alarm;
13:  else
14:      Notify the controller to process PACKET_IN messages;
15:  end if
16: end if
```

B. FLOW TABLE ENTRY COLLECTION MODULE

When the controller receives an attack detection trigger instruction, the flow table entry collection module is started. The following seven-tuple information as shown in (2) is extracted by collecting the original flow table entries, that is, the network quintuple and count value in the flow entry are extracted as flow feature enter.

$$< srcIP, dstIP, srcPort, dstPort, IP \text{ Protocl}, packet\_count, byte\_count > \quad (2)$$

1) MULTI-DIMENSIONAL FLOW FEATURE EXTRACTION

We mainly extract the eight-dimensional data feature vectors required for model training in the SDN network attack detection process [24]–[26]:

$$\{APF, ABF, RF, PPF, PGS, H(srcIP), H(dstIP), H(flows)\} \quad (3)$$

2) AVERAGE NUMBER OF PACKETS IN PER FLOW(APF)

The number of packets in per flow is different between normal and attacked states. False IPs are generated in an attack frequently and randomly, so the flow generation speeds up, and each flow decreases the amount of packets. APF is formulated by (4).

$$APF = \left(\sum_{j=1}^{FlowNum} packet\_count_j \right) / FlowNum \tag{4}$$

In (4), $packet\_count_j$ is the number of packets in the flow j within a certain time interval and $FlowNum$ is the number of all packets in the interval.

3) AVERAGE NUMBER OF BYTES IN PER FLOW(ABF)

The content of a DDoS attack packet is usually filled with only a small number of bytes in per flow to increase attack efficiency. ABF is formulated by (5).

$$ABF = \left(\sum_{j=1}^{FlowNum} \text{byte\_count}_j \right) / FlowNum \tag{5}$$

4) RATE OF FLOW TABLE ENTRIES(RF)

When an attack occurs, requests for specific hosts on the network increase, causing the number of flow table entries to increase for a fixed period of time. RF is formulated by (6).

$$RF = FlowNum/interval \tag{6}$$

5) PERCENTAGE OF PAIR FLOWS(PPF)

The IP address of normal network traffic is interactive to obtain or provide services. For example, given any two flows, Flow1 and Flow2, if the source/destination IP address of Flow1 is the same as the destination/source IP address of Flow2, and the communication protocol is the same, then Flow1 and Flow2 are called one pair of convection flows. $PairNum$ is the number of convections. PPF is formulated by (7).

$$PPF = 2 * PairNum/FlowNum \tag{7}$$

6) PORTS GENERATING SPEED(PGS)

DDoS attack not only uses IP spoofing, but also randomly generates port numbers. Therefore, the speed of port generation is significantly higher than that of normal network conditions. PGS is formulated as (8).

$$PGS = PortNum/interval \tag{8}$$

7) FLOW TABLE FEATURE ENTROPY

As known, information entropy is an index used to measure the diversity, uncertainty, and randomness of random variables in information theory. Entropy in DDoS detection can determine the randomness of network traffic. The higher entropy, the higher the randomness of the traffic; on the contrary, the higher the certainty of the traffic. Therefore, the entropy can be used to describe the normal state of the mapping relationship between the source address, the destination port, and the destination addresses, and describe the feature of the DDoS attack.

The DDoS detection is performed by entropy calculation [27]. An attribute value of X in the network information flow is denoted as N, $X = \{n_i, i = 1, 2, \ldots, N\}$ indicates that the feature value has appeared n_i times in the measurement data. S indicates the occurrence number of the feature value. The information entropy of attribute X in the information flow is calculated as (9):

$$H(X) = -\sum_{i=1}^{N} (\frac{n_i}{S}) \ln(\frac{n_i}{S}) \tag{9}$$

The DDoS detection algorithm based on entropy feature depends on the distribution of traffic feature. Entropy values can be calculated using traffic feature such as packet header (address, port and flag), packet size, and behavior feature (inbound and outbound). Based on the analysis of existing studies, this paper proposes the following properties of entropy features:

a: ENTROPY BASED ON SOURCE IP ADDRESS

Compared to legal traffic, the large number of zombies controlls by the initiators of DDoS attack and their IP addresses are more concentrated, resulting in lower entropy. The main reason for choosing the source IP address to calculate entropy is that the source IP address has a strong correlation with the number of source ports and the number of destination ports.

b: ENTROPY BASED ON DESTINATION IP ADDRESS

The statistical method based on the source IP address shows great limitations in the face of the decentralized IP address of the zombie. The attack traffic usually points to a single site or a network segment. The destination IP address is centralized, and the calculated entropy is small. Therefore, the entropy of the destination IP address is selected as an important parameter.

c: ENTROPY BASED ON FLOW COUNT

DDoS attackers usually ignore the victim's response and only generate attack traffic by attack scripts. For a match in the flow table, the packet size of the traffic is usually relatively fixed. The value of Flow Count is decentralized and the calculated entropy is small. Conversely, legitimate traffic has different packet sizes due to different requests, responses, and data. Hence, the entropy value of Flow Count is different for normal traffic. Therefore, the entropy value of Flow Count with different normal flow rate is larger. Consider the change rule of the flow entry under the SDN network architecture when the DDoS flood attack occurs, and propose the entropy feature attribute of the flow entry.

d: FLOW FEATURE SELECTION BASED ON PROTOCOL TYPE

The feature of DDoS attack is largely divergent for different transport protocols. Accordingly, this paper analyzes the feature of DDoS attack under the TCP/UDP/ICMP protocol and proposes a feature selection method based on the protocol type. As shown in Figure 4, for a given feature set $S = \{s_1, s_2, \ldots, s_n\}$, after feature selection, a feature set $S_{TCP} = \{s_1, s_2, \ldots, s_p\}$, $S_{UDP} = \{s_1, s_2, \ldots, s_q\}$, $S_{ICMP} = \{s_1, s_2, \ldots, s_r\}$ under different protocol types is obtained,

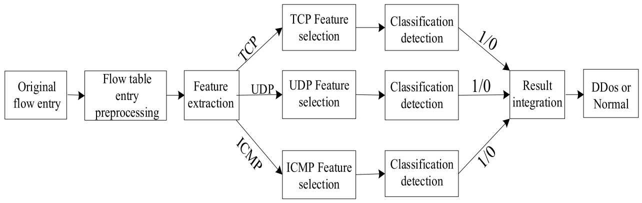

FIGURE 4. Protocol-based detection scheme.

and then a trained SVM classification model is input for determination.

Correlation measure is adopted to deal with feature selection in detection, based on the importance of correlation measure between categories and features and the selection of optimal feature sets proposed in the previous section to overcome the impact of irrelevant redundancy on learning algorithms. With a higher correlation between a certain feature S and a category c, a higher dependency between features and categories is found, and a subset of features is then determined. Considering the correlation and redundancy among feature properties, we use the feature selection algorithm based on correlation coefficient proposed by [28] to reduce dimension, specifically based on maximum correlation $D(S, c)$ and minimum redundancy $D(S, c)$. And $R(S)$ is calculated as follows, where x_i represents the *ith* feature.

$$D(S, c) = \max(\frac{1}{|S|}\sum_{x_i \in S} r(x_i, c)) \tag{10}$$

$$R(S) = \min(\frac{1}{|S|^2}\sum_{x_i, x_j \in S} r(x_i, x_j)) \tag{11}$$

Feature selection algorithm based on correlation coefficient included in the protocol-based flow feature selection algorithm gives a reasonable feature ranking for each protocol which is in descending order according to the weight $D - R$ of each dimension feature. This paper only gives the sort of features used to detect the number of features of purpose according to the requirements such as the expected degree of detection, accuracy, etc.

C. ATTACK DETECTION MODULE

The platform embeds the SVM in the controller and uses the SVM to detect DDoS attack. It can identify benign flow entries generated by normal traffic and malicious flow entries generated by DDoS attack traffic. Attack detection can be roughly divided into two steps: the training phase of the SVM model and the real-time detection phase.

In the training phase, a series of malicious attack traffic, benign traffic flow feature, and corresponding target values (i.e. 0 for benign traffic and 1 for malicious attack traffic) are used as training data sets. An available SVM model is established with the extracted feature parameters as input parameters of the SVM and the target values as output parameters.

In the real-time detection phase, the flow table entry collection module first obtains all the flow table entries of each switch, and then processes the flow entries in the flow entry flow statistics message one by one and extracts the feature values of the flow entries. The feature values will be transferred to the SVM training model according to different protocol types to determine whether the flow entry is benign or malicious. If it is determined to be malicious traffic, a DDoS attack alert will be generated first. Subsequently, the processing of traffic statistics messages will stop.

VI. SIMULATION-BASED ANALYSIS

A. SIMULATION ENVIRONMENT IMPLEMENTATION

This paper verifies the effectiveness of the above scheme application in DDoS attack detection by deploying a software-defined network. The simulation environment is constructed as follows:

- ***Infrastructure Plane:*** Adopt open source Mininet network simulator supporting OpenFlow protocol.
- ***Control Plane:*** Adopt the Improved Floodlight controller as a control plane. Floodlight is cross-platform so that it is easy to run and configure.
- ***Application Plane:*** The attack detection module acts as an application plane. It implements the application of DDoS attack detection, which is convenient for update and functional conditions.

Based on Linux, the system is set up and configured in Ubuntu environment. Seven OVS switches and 14 virtual machines are deployed as terminal host. The simulation experiment network topology is shown in Figure 5.

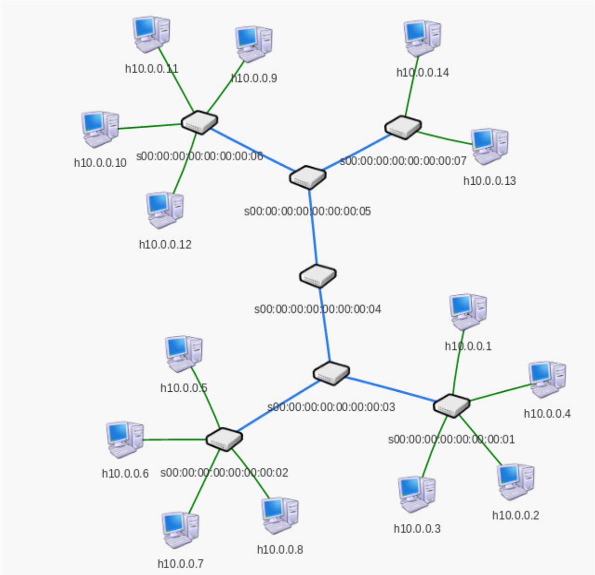

FIGURE 5. Experimental network topology.

B. EXPERIMENTAL DATA

In the experimental flow, normal traffic is generated by analyzing the transfer traffic between Japan and the United States over seven years [29], including 80% of TCP traffic, 15% of UDP traffic, and 5% of other traffic. DDoS attack traffic is mainly generated through the Scapy, ICMP Flooding attack traffic is from the hping3. In order to improve the authenticity of the DDoS attack, the experiment sets different attack payload data lengths under the premise of setting multiple attack methods. In an abnormal situation, a DDoS attack exists along with some normal packets. Table 1 shows the type of attacks initiated during the training and testing phases and their estimated generation traffic.

TABLE 1. Experimental data samples.

Type of attack	Training data	Test Data
UDP Flood	300	500
ICMP Flood	100	200
TCP/SYN Flood	800	1000

C. PERFORMANCE ANALYSIS

In this paper, we use the Detection Ratio (DR) and False Alarm Ratio (FR) to evaluate the experiment results, which are defined as follow:

$$DR = \frac{TN}{TN + FN} \tag{12}$$

$$FR = \frac{FP}{TP + FP} \tag{13}$$

In (12), *TN* represents the number of attack states that are correctly identified, while *FN* represents the number of attack states that are identified as normal. In (13), *TP* represent the number of normal states that are correctly identified, while *FP* represents the number of normal states that are identified as attack.

1) TRIGGER MODULE PERFORMANCE ANALYSIS

To evaluate the performance of PACKET_IN trigger, periodic trigger and PACKET_IN trigger are tested respectively. DDoS attack is initiated five times in 30 minutes for each test. Therefore, periodic trigger and PACKET_IN trigger run respectively in 30 minutes. Trigger period of periodic trigger is 2 minutes, and the window value triggered by PACKET_IN is 100 PACKET_IN packets and the rate threshold is 50 packets per second.

Figure 6 shows the average response time comparison between periodic trigger and PACKET_IN trigger. We can find that the average response time of the periodic trigger is up to 75s, and the PACKET_IN trigger can start detection within 3 seconds. Hence, PACKET_IN trigger can respond to DDoS attack more quickly.

The SDN controller monitors the traffic and flow rate of the entire network, periodically collects the network state, obtains the real-time flow rate corresponding to each link, and obtains the average network load on this basis. Figure 7 shows the comparison of the average network load under both trigger modes. When a DDoS attack occurs, a great deal PACKET_IN messages are sent to the controller. If periodic trigger is used as the trigger mechanism, plenty of PACKET_IN messages and flow modification messages will be generated due to its longer response time. However, using the PACKET_IN trigger will shorten the response time and reduce the number of PACKET_IN messages and flow modification messages. Therefore, the controller's load will be declined by reducing the response time for detecting the attack.

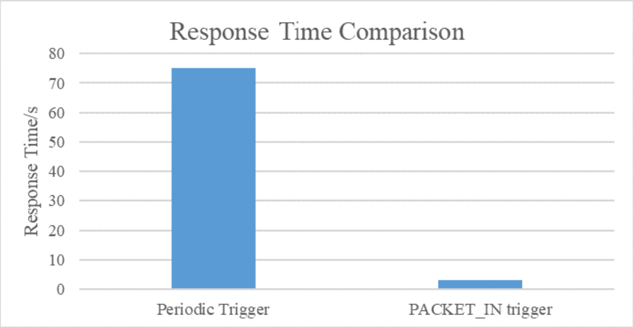

FIGURE 6. Average Response Time.

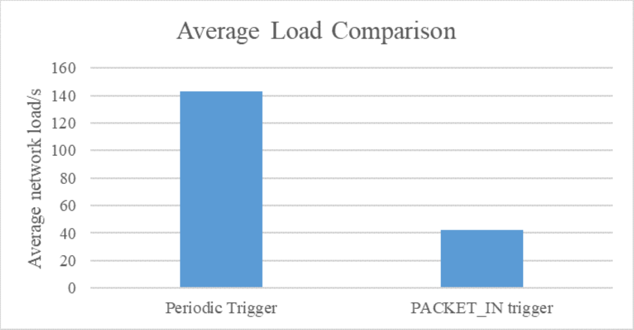

FIGURE 7. Average network load.

2) FEATURE SELECTION ALGORITHM BASED ON PROTOCOL TYPE PERFORMANCE ANALYSIS

In this section, we first verify the feasibility of feature extraction based on flow table entry, mainly analyzing the distribution of entropy feature and feature attributes. In this paper, we adopt datasets from existing networks for analysis. We use DARPA 1999 first week dataset as normal datasets, and use DARPA 2000 dataset and CAIDA DDoS 2007 dataset as the basis for generating anomalous traffic. Finally, we apply the feature selection algorithm of correlation coefficient metrics to sort the attributes of DDoS attack detection by different transport protocols (e.g., TCP, ICMP) respectively.

a: ENTROPY FEATURE ANALYSIS

In this part, we mainly analyze the distribution of the flow count entropy feature in normal and attacked conditions. Figure 8 shows a comparison of 100 samples extracted from the DARPA 1999 normal traffic dataset and the DARPA

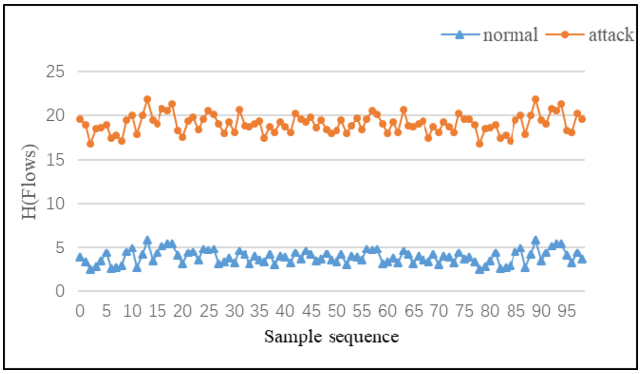

FIGURE 8. Contrast between TCP protocol normal and attack flow count entropy.

2000 attacked traffic dataset, respectively. As shown in the figure, the entropy value of the normal traffic is small, and the entropy value of the attacked traffic is large, so the segmentation is more obvious, which can be used as a feature value of the classification and identification.

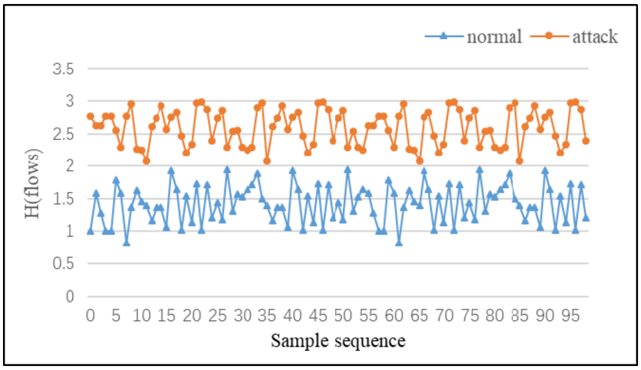

FIGURE 9. Contrast Between ICMP protocol normal and attack entropy.

In addition, we analyze the data of ICMP Flood attack type and extract 100 samples of the Echo (Ping) request Flood attack in the CAIDA DDoS 2007 data set. Figure 9 shows the comparison of the distribution between the normal ICMP protocol and attacked flow counts. According to the figure, $H(flows)$ of normal traffic is small, and $H(flows)$ of attack traffic is large. Under the TCP protocol, the interval between normal distribution and attack traffic is large.

$H(flows)$ is a standard for classification and identification of DDoS. We have verified through experiments that $H(flows)$ of attack states are higher than those in normal state under both TCP and ICMP protocols, but $H(flows)$ is different under the two protocols. Therefore, it is necessary to select feature attributes for traffic under different protocols.

b: DISTRIBUTION OF FEATURE ATTRIBUTES ANALYSIS

In this section, we will analyze the distribution of normal traffic and attack traffic under different feature attributes (value of flow packet and flow count entropy).

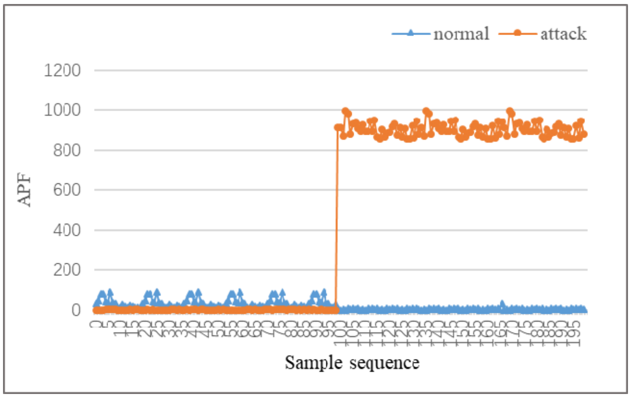

FIGURE 10. Average number of packets in per flow distribution.

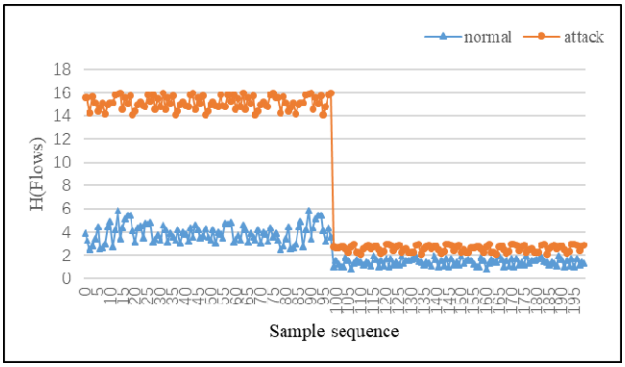

FIGURE 11. Flow count entropy contribution.

Figure 10 and 11 show the distribution of APF and flow count entropy, respectively. When TCP traffic and ICMP traffic are mixed, the classification interval is not obvious, which will have a great influence on the accuracy of recognizing attacks. Therefore, it is necessary to perform feature selection for different protocols.

TABLE 2. Sorting of feature attributes under different protocol types.

No.	Feature attributes	TCP attack attribute ranking	ICMP attack Attribute ranking
1	APF	2	1
2	ABF	3	3
3	RF	7	4
4	PPF	6	5
5	PGS	4	7
6	H(srcIP)	5	6
7	H(Flows)	1	2

c: SORTING OF FEATURE ATTRIBUTES ANALYSIS

In this paper, we propose a feature selection method based on correlation coefficient. When a set number of feature attributes are obtained according to the protocol, the search feature subsets are immediately stopped, resulting in different feature subset sorted from different protocols. Table 2 shows the ranking of feature attributes of the TCP and the ICMP.

3) ATTACK DETECTION PERFORMANCE ANALYSIS

In this paper, we comprehensively analyze the detection effect of SVM classifiers on DDoS attack and the classification efficiency of the best feature samples under different number of feature selections through the feature selection algorithm. Then, three attributes of APF, ABF, and H (Flows) are selected as feature variables according to the ranking of the protocol after feature selection. Using the SVM classification algorithm for feature properties obtained experiment, the performance evaluation indexes of the classification effect contain detection rate and false alarm rate.

Table 3 and Table 4 show the comparison of classification performance pre and after feature selection for ICMP traffic and TCP traffic, respectively. It is noted that the classification detection rate after feature selection is higher than the former, and it has a lower false alarm rate. At the same time, the input test feature sequences have different dimensions, so that the selected flow table feature set has a higher classification efficiency.

TABLE 3. ICMP traffic classification performance comparison.

Flow feature	Test results	Classification time /s

Pre-selection	DR=97.59%
	FR=0.5%
		0.125

After-selection	DR=97.49%
	FR=0.3%
		0.038

TABLE 4. TCP traffic classification performance comparison.

Flow feature	Test results	Classification time /s

Pre-selection	DR=98.26%
	FR=0.52%
		0.148

After selection	DR=98.56%
	FR=0.32%
		0.048

TABLE 5. Different kernel functions on the classification performance.

Kernel function type	DR
Linear: $K(x,z)=x\cdot z$	97.68%
Polynomial: $K(x,z)=(\mathrm{x}\cdot\mathrm{z}+1)^p$	93.25%
RBF: $K(x,z)=\exp\left(-\frac{\left\|x-z\right\|^2}{2\sigma^2}\right)$	95.4%

According to the feature selection experiment, the optimal flow table feature attributes can be obtained. After that, we analyze the different kernel functions in the SVM classifier, as shown in Table 5. We also select SVM for different kernel functions and compare the classification performance of the sample data. Through comparison, we find that the classification performance of the linear kernel function is better.

VII. CONCLUSION

In this paper, we design DDoS attack detection system platform based on the open source Floodlight controller in SDN. In the attack detection trigger module, we propose a detection trigger mechanism based on the PACKET_IN message to significantly reduce the response time to the attack and the burden on the controller. In the flow table entry collection module, we combine the feature of the OpenFlow protocol and DDoS attack to design a flow-table feature-based DDoS attack detection method, also known as a flow table detection method. By obtaining the flow table entries in the OpenFlow switch, after statistical analysis, the corresponding flow features are extracted, and the redundancy feature is removed in combination with the feature selection algorithm under different protocol types. In the attack detection module, a classification algorithm is used to train the samples and build a detection model to determine whether there is a DDoS attack in the network. The author verifies the effectiveness and advantages of the system through experiments.

REFERENCES

[1] Z. Ning, F. Xia, X. Hu, Z. Chen, and M. S. Obaidat, "Social-oriented adaptive transmission in opportunistic Internet of smartphones," *IEEE Trans. Ind. Inf*, vol. 13, no. 2, pp. 810–820, Apr. 2017.

[2] Z. Ning *et al.*, "A cooperative quality-aware service access system for social Internet of vehicles," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1527–1538, 2018.

[3] H. Sedjelmaci, S. M. Senouci, and M. A. Abu-Rgheff, "An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks," *IEEE Internet Things J.*, vol. 1, no. 6, pp. 570–577, Dec. 2014.

[4] Z. Ning, L. Liu, F. Xia, B. Jedari, I. Lee, and W. Zhang, "CAIS: A copy adjustable incentive scheme in community-based socially aware networking," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3406–3419, Apr. 2017.

[5] W. Hou, Z. Ning, L. Guo, and X. Zhang, "Temporal, functional and spatial big data computing framework for large-scale smart grid," *IEEE Trans. Emerg. Topics Comput.*, to be published, doi: 10.1109/TETC.2017.2681113.

[6] Y. Yu, Z. Ning, and L. Guo, "A secure routing scheme based on social network analysis in wireless mesh networks," *Sci. China Inf. Sci.*, vol. 59, Dec. 2016, Art. no. 122310.

[7] A. Benslimane and H. Nguyen-Minh, "Jamming attack model and detection method for beacons under multichannel operation in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 6475–6488, Jul. 2017.

[8] C. Lyu, D. Gu, Y. Zeng, and P. Mohapatra, "PBA: Prediction-based authentication for vehicle-to-vehicle communications," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 1, pp. 71–83, Jan. 2016.

[9] Z. Ning, F. Xia, N. Ullah, X. Kong, and X. Hu, "Vehicular social networks: Enabling smart mobility," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 49–55, May 2017.

[10] X. Wang, Z. Ning, and L. Wang, "Offloading in Internet of vehicles: A fog-enabled real-time traffic management system," *IEEE Trans. Ind. Inf*, to be published, doi: 10.1109/TII.2018.2816590.

[11] W. Hou, Z. Ning, L. Guo, Z. Chen, and M. S. Obaidat, "Novel framework of risk-aware virtual network embedding in optical data center networks," *IEEE Syst. J.*, to be published, doi: 10.1109/JSYST.2017.2673828.

[12] Y. Yu, Y. Peng, X. Li, J. Gao, and X. Cong, "Distributed packet-aware routing scheme based on dynamic network coding," *China Commun.*, vol. 13, no. 10, pp. 20–28, Oct. 2016.

[13] S. A. Mehdi, J. Khalid, and S. A. Khayam, "Revisiting traffic anomaly detection using software defined networking," in *Proc. Int. Conf. Recent Adv. Intrusion Detection*, 2011, pp. 161–180.

[14] A. Olabelurin, S. Veluru, A. Healing, and M. Rajarajan, ''Entropy clustering approach for improving forecasting in DDoS attacks,'' in *Proc. IEEE Int. Conf. Netw., Sens. Control*, Apr. 2015, pp. 315–320.

[15] X. Qin, T. Xu, and C. Wang, ''DDoS attack detection using flow entropy and clustering technique,'' in *Proc. Int. Conf. Comput. Intell. Secur.*, Dec. 2016, pp. 412–415.

[16] S. Yu, W. Zhou, R. Doss, and W. Jia, ''Traceback of DDoS attacks using entropy variations,'' *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 3, pp. 412–425, Mar. 2011.

[17] Y. Yu, L. Guo, J. Huang, F. Zhang, and Y. Zong, ''A cross-layer security monitoring selection algorithm based on traffic prediction,'' *IEEE Access*, to be published, doi: 10.1109/ACCESS.2018.2851993.

[18] Y. Yu, Y. Peng, Y. Yu, and T. Rao, ''A new dynamic hierarchical reputation evaluation scheme for hybrid wireless mesh networks,'' *Comput. Elect. Eng.*, vol. 40, no. 2, pp. 663–672, 2014.

[19] B. Braga, M. Mota, and P. Passito, ''Lightweight DDoS flooding attack detection using NOX/OpenFlow,'' in *Proc. IEEE Local Comput. Netw. Conf.*, Oct. 2010, pp. 408–415.

[20] A. Saied, R. E. Overill, and T. Radzik, ''Detection of known and unknown DDoS attacks using artificial neural networks,'' *Neurocomputing*, vol. 172, pp. 385–393, Jan. 2016.

[21] R. T. Kokila, S. T. Selvi, and K. Govindarajan, ''DDoS detection and analysis in SDN-based environment using support vector machine classifier,'' in *Proc. 6th Int. Conf. Adv. Comput.*, Dec. 2014, pp. 205–210.

[22] B. Fei and J. Liu, ''Binary tree of SVM: A new fast multiclass training and classification algorithm,'' *IEEE Trans. Neural Netw.*, vol. 17, no. 3, pp. 696–704, May 2006.

[23] Y. Yu, L. Guo, X. Wang, and C. Liu, ''Routing security scheme based on reputation evaluation in hierarchical Ad Hoc networks,'' *Comput. Netw.*, vol. 54, no. 9, pp. 1460–1469, 2010.

[24] X. Zhang, L. Guo, W. Hou, Q. Zhang, and S. Wang, ''Failure recovery solutions using cognitive mechanisms based on software-defined optical network platform,'' *Opt. Eng.*, vol. 56, no. 1, p. 016107, 2017.

[25] Y. Xu and Y. Liu, ''DDoS attack detection under SDN context,'' in *Proc. IEEE INFOCOM*, Apr. 2016, pp. 1–9.

[26] X. Zhang *et al.*, ''Experimental demonstration of an intelligent control plane with proactive spectrum defragmentation in SD-EONs,'' *Opt. Exp.*, vol. 25, no. 20, pp. 24837–24852, 2017.

[27] A. Sgora, D. D. Vergados, and P. Chatzimisios, ''A survey on security and privacy issues in wireless mesh networks,'' *Secur. Commun. Netw.*, vol. 9, no. 13, pp. 1877–1889, 2013.

[28] F. Amiri, M. R. Yousefi, C. Lucas, A. Shakery, and N. Yazdani, ''Mutual information-based feature selection for intrusion detection systems,'' *J. Netw. Comput. Appl.*, vol. 34, no. 4, pp. 1184–1199, 2011.

[29] J. Mirkovic, S. Fahmy, P. Reiher, and R. K. Thomas, ''How to test DoS defenses,'' in *Proc. Cybersecur. Appl. Technol. Conf. Homeland Secur.*, Mar. 2009, pp. 103–117.

[30] W. Hou *et al.*, ''On-chip hardware accelerator for automated diagnosis through human-machine interactions in healthcare delivery,'' *IEEE Trans. Automat. Sci. Eng.*, to be published, doi: 10.1109/TASE.2018.2832454.

[31] L. Guo, Z. Ning, W. Hou, B. Hu, and P. Guo, ''Quick answer for big data in sharing economy: Innovative computer architecture design facilitating optimal service-demand matching,'' *IEEE Trans. Automat. Sci. Eng.*, to be published, doi: 10.1109/TASE.2018.2838340.

YAO YU (M'10) received the Ph.D. degree from Northeastern University, China, in 2010. From 2010 to 2011, she was a Post-Doctoral Fellow with The Hong Kong Polytechnic University, Hong Kong, China. She is currently an Associate Professor with Northeastern University, Shenyang, China. Her current research interests include social network, network security, and big data. She has authored over 30 papers in the above areas.

LEI GUO (M'06) received the Ph.D. degree from the University of Electronic Science and Technology of China in 2006. He is currently a Professor with Northeastern University, Shenyang, China. His current research interests include communication networks, optical communications, and wireless communications. He has published over 200 technical papers in the above areas in international journals and conferences, such as the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE JOURNAL OF LIGHTWAVE TECHNOLOGY, the IEEE JOURNAL OF OPTICAL COMMUNICATIONS AND NETWORKING, the IEEE GLOBECOM, and the IEEE ICC. He is a member of the OSA and also a Senior Member of the CIC. He is serving as an Editor for several international journals, such as *Photonic Network Communications* and *The Open Optics Journal*.

YE LIU received the bachelor's degree from Shenyang Ligong University, Shenyang, China, in 2016. He is currently pursuing the master's degree with Northeastern University. His research focuses on network security.

JIAN ZHENG received the bachelor's degree from Northeastern University, Shenyang, China, in 2016, where she is currently pursuing the master's degree. Her research focuses on network security.

YUE ZONG received the B.S. degree in communication engineering from Northeastern University, Shenyang, China, in 2013, where she is currently pursuing the Ph.D. degree. Her research interests include network optimization and data center networks.