International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:12, No:6, 2018

An Earth Mover's Distance Algorithm Based DDoS Detection Mechanism in SDN

Yang Zhou, Kangfeng Zheng, Wei Ni, Ren Ping Liu

***Abstract*—**Software-defined networking (SDN) provides a solution for scalable network framework with decoupled control and data plane. However, this architecture also induces a particular distributed denial-of-service (DDoS) attack that can affect or even overwhelm the SDN network. DDoS attack detection problem has to date been mostly researched as entropy comparison problem. However, this problem lacks the utilization of SDN, and the results are not accurate. In this paper, we propose a DDoS attack detection method, which interprets DDoS detection as a signature matching problem and is formulated as Earth Mover's Distance (EMD) model. Considering the feasibility and accuracy, we further propose to define the cost function of EMD to be a generalized Kullback-Leibler divergence. Simulation results show that our proposed method can detect DDoS attacks by comparing EMD values with the ones computed in the case without attacks. Moreover, our method can significantly increase the true positive rate of detection.

***Keywords*—**DDoS detection, EMD, relative entropy, SDN.

I. Introduction

DISTRIBUTED denial of service (DDoS) attack severely threatens the security of large data networks, especially the emerging network architecture Software-Defined Networking (SDN) [1]. The DDoS attack detection methods are promising techniques that attract many researchers attentions. However, it lacks efficient and accurate solutions to detect DDoS attacks which aim at saturating the particularly crucial controller-switch channels and controllers in SDN.

In general, DDoS attacks are generated by injecting significant amount of packets with forged fields to the designated targets in the network. As a result, the detection methods have been mostly concentrated on studying the statistical features of packets. Entropy is popular in analyzing the randomness of the probability distributions of packets.In SDN, the DDoS attack can be easily launched by sending new packets to saturate the controller or the controller-switch channel [1]. In this case, the entropy of the corresponding field, such as destination IP address, becomes smaller than the one without attacks [2]. However, the entropy metric only focuses on analyzing one feature, which lacks the ability of comprehensive analysis and the result is not accurate enough. Other methods have also been extensively studied, such as the machine learning method [3]. But it usually spends time on training network traffic, which decreases the time efficiency of detection.

In this paper, we propose a DDoS detection method based on Earth Mover's Distance (EMD) algorithm, of which the cost function is defined as an extended Kullback-Leibler divergence (also called relative entropy). The key idea is to interpret DDoS detection as a signature matching problem and develop a new distance metric based on relative entropy. Another important aspect of our algorithm is that we collaboratively analyze the features of IP address and the number of OpenFlow packets in SDN, and increase the difference between the values of normal traffic and attack traffic. Simulation results show that our methods can early detect DDoS attacks in SDN with high accuracy.

The rest of paper is organized as follows. Section II presents related work. In Section III, we discuss the detail of designed algorithm. Section IV evaluates the experiment results and performance of our algorithm. In Section V, we conclude the paper.

II. Related Work

DDoS attack takes place dispersedly on multiple end-hosts and is usually powered by botnets, to affect or even overwhelm the target network infrastructures. As a measure of disorder or randomness of a system, entropy has been applied in many researches to detect the DDoS attack. In [4], a distributed method was proposed to analyze the entropy of flows in each ISP domain. To improve the accuracy of detection, [5] developed a method based on chaos theory to analyze the variation of network traffic between realistic and predicted ones. They utilize the Lyapunov exponent to measure the degree of separation between source IPs and destination IPs. However, the results were affected by the accuracy of prediction algorithms. A metric of symmetric Rényi entropy was proposed in [6] to detect low-rate DDoS attacks. The detection modules were implemented on routers and this method was designed for traditional networks.

Exploiting the decoupled data plane and control plane of SDN, attackers usually carry out DDoS attack by injecting a surge of spoofed packets into network [7]. Reference [2] firstly proposed a lightweight method to detect DDoS attacks in SDN, by comparing the entropy of destination IP addresses with the threshold. However, it was difficult to detect

This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFB0802703 and in part by the National Natural Science Foundation of China under Grant 61602052.

Y. Zhou is with the School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, China (corresponding author, e-mail: zhouyang@bupt.edu.cn).

K. Zheng is with the School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, China (e-mail: kfzheng@bupt.edu.cn).

W. Ni is with CSIRO, Sydney, NSW 2122, Australia (e-mail: Wei.Ni@data61.csiro.au).

R. P. Liu is with the Global Big Data Technologies Centre, University of Technology Sydney, Sydney, NSW 2007, Australia (e-mail: RenPing.Liu@uts.edu.au).

accurately when attack traffic was similar to the normal traffic. Different machine learning methods, including Naive Bayes, K-nearest neighbor, K-means, and K-medoids, were introduced in [8] to classify the anomaly and normal traffic in SDN. Reference [9] developed a statistical method by comparing the counting number of source IP addresses with the pre-set threshold, to decrease the bandwidth occupation in the controller-switch channel. Reference [10] designed a hybrid approach that combined with time series prediction and entropy comparison to detect DDoS attacks in SDN. However, the results were mostly related to the accuracy of the prediction method.

III. Proposed Algorithm

We present our algorithm together with a pre-introduction of EMD in the following sections.

A. Background of EMD

EMD [11] is a well-known algorithm that is widely used to measure the difference of two images [12]. The computation of EMD is based on linear transportation problem, with an objective of minimizing transmission cost. The cost is defined as the amount of earth transported by the distance.

In image applications, pixels are quantified as coordinates for convenience of calculations. Suppose that figure P is composed of m clusters, and $P = \{(p_1, \omega_{p_1}), \cdots, (p_m, \omega_{p_m})\}$ is the signature of P. p_i represents cluster i, ω_{p_i} is the weight of cluster i. $Q = \{(q_1, \omega_{q_1}), \cdots, (q_n, \omega_{q_n})\}$ is the signature of figure Q having n clusters. Moreover, d_{ij} is the ground distance between p_i and q_j, which can be defined as the Euclidean distance, or other distance measures. The objective is to find out the optimal flow $F = [f_{ij}]$, of which f_{ij} denotes the flow from p_i to q_j, making sure that the overall moving cost is minimized, which is presented as follows,

$$\min \sum_{i=1}^{m} \sum_{j=1}^{n} d_{ij} f_{ij} \tag{1}$$

The moving process should satisfy following constraints,

$$f_{ij} \geq 0, 1 \leq i \leq m, 1 \leq j \leq n \tag{2a}$$

$$\sum_{j=1}^{n} f_{ij} \leq \omega_{p_i}, 1 \leq i \leq m \tag{2b}$$

$$\sum_{i=1}^{m} f_{ij} \leq \omega_{q_j}, 1 \leq j \leq n \tag{2c}$$

$$\sum_{i=1}^{m} \sum_{j=1}^{n} d_{ij} f_{ij} = \min \left(\sum_{i=1}^{m} \omega_{p_i}, \sum_{j=1}^{n} \omega_{q_j} \right) \tag{2d}$$

where (2a) restricts that the flows can only move from P to Q and not vice versa. Equation (2b) restrains that the amount of earth that can move out from p_i should not exceed its weight ω_{p_i}. Also q_j cannot receive more earth than its weight ω_{q_j}, as shown in (2c). Equation (2d) forces to move the amount of earth as much as possible.

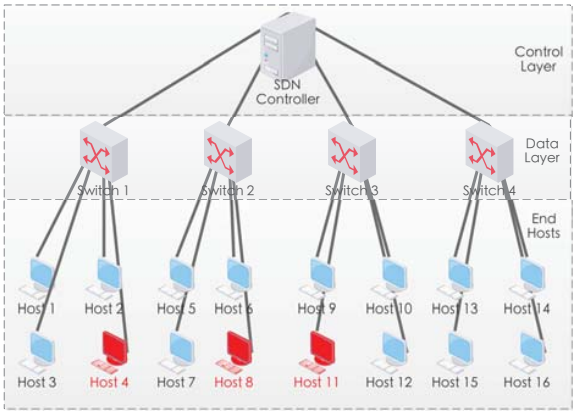

Fig. 1 An illustration of SDN topology

In this context, the EMD is defined as the overall moving work normalized by the total amount of earth moved, as specified by,

$$\text{EMD(P, Q)} = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} d_{ij} f_{ij}}{\sum_{i=1}^{m} \sum_{j=1}^{n} f_{ij}} \tag{3}$$

In our previous works, EMD was leveraged to solve the routes mutation [17] and switches assignment problems [18]. Route mutation problem modeled with EMD was introduced to instantly mutate routes and disguise strategically important nodes in large-scale SDN. Moreover, an elastic switch migration method was designed to balance the loads of controllers by using EMD, to protect the important controllers in SDN. In this paper, we propose to utilize EMD with an extended definition of cost to detect DDoS attacks in SDN.

B. Detection Algorithm

In our paper, we focus on a DDoS attack, where adversaries exploit the vulnerability of OpenFlow protocol and keep sending forged or spoofed packets that switches cannot match according to their current flow tables [1], [13]. As a result, switches send corresponding OpenFlow packet_in packets to controllers to request for rules that determine how to forward flows. This case can significantly impact the performance of the controller and the bandwidth of links between controllers and switches in SDN.

Fig. 1 illustrates the simplified SDN topology under consideration, where switches are controlled by the controller and end hosts send and receive packets. We assume that the controller has the central view of the whole network, and are also responsible for detecting traffic anomaly.

In detail, host 4, 8 and 11 are these attackers, sending forged packets and aiming at overwhelming the SDN controller.

Our proposed algorithm attempts to leverage EMD to measure the difference between two distributions of traffic features. We construct signatures P and Q as one-dimensional distributions of the probabilities of traffic features. Let m and n represent the number of clusters for P and Q, respectively. Each cluster represents one feature, such as cluster 1 denotes the distribution of source IP address,

cluster 2 denotes the destination IP address distribution. The first signature $P = \{(P_1, \omega_{P_1}), (P_2, \omega_{P_2}), \cdots, (P_m, \omega_{P_m})\}$ represents the distributions in the last time interval. To be specific, for any cluster i, $P_i = \{p_{i1}, p_{i2}, \cdots, p_{ik}\}$, where $p_{il}, \forall l \in [1, k]$ denotes the probability of IP address l appearing with feature i, k denotes the total number of different IPs appear in this interval; ω_{P_i} denotes the accumulative number of OpenFlow packets with feature i received by controller during the interval. Similarly, $Q = \{(Q_1, \omega_{Q_1}), (Q_2, \omega_{Q_2}), \cdots, (Q_n, \omega_{Q_n})\}$ represents the IP addresses distribution in the current time interval. $Q_j = \{q_{j1}, q_{j2}, \cdots, q_{jk}\}$. In our paper, we define P and Q to be the sets of IP addresses, thus $m = n = 2$. $P = \{(P_1, \omega_{P_1}), (P_2, \omega_{P_2})\}$ represents the distributions of source IP and destination IP, respectively, in the last time interval. $Q = \{(Q_1, \omega_{Q_1}), (Q_2, \omega_{Q_2})\}$ denotes the distributions in current time interval. Given P and Q, the EMD can be defined to measure the difference between these two signatures, as shown in (3).

In image applications, the d_{ij} defined in (1) usually goes to the Euclidean distance to measure the difference between two pixels. We propose an extended relative entropy of order α to be the cost function in our paper. The relative entropy of order α between P_i and Q_j is shown below,

$$D_\alpha(P_i \| Q_j) = \frac{1}{\alpha - 1} \log \left(\sum_{z=1}^{k} p_{iz}^{\alpha} q_{jz}^{1-\alpha} \right) \tag{4}$$

where $0 < \alpha < \infty$ and $\alpha \neq 1$. When $\alpha \to 1$, (4) defines the Kullback-Leibler divergence, i.e., the relative entropy, as follows,

$$D_1(P_i \| Q_j) = \sum_{z=1}^{k} \left(p_{iz} \log \frac{p_{iz}}{q_{jz}} \right) \tag{5}$$

We note that $D_\alpha(P_i \| Q_j) \neq D_\alpha(Q_j \| P_i)$. The cost, i.e., d_{ij} in (3), requires to be symmetric if (3) is a true metric. Therefore, we proceed to define the cost to be an expanded form of relative entropy of order α between P_i and Q_j, as specified by,

$$\begin{aligned} d_\alpha(i,j) &= D_\alpha(P_i \| Q_j) + D(Q_j \| P_i) \\ &= \frac{1}{\alpha - 1} \log \left(\sum_{z=1}^{k} p_{iz}^{\alpha} q_{jz}^{1-\alpha} \right) + \\ &\frac{1}{\alpha - 1} \log \left(\sum_{z=1}^{k} q_{jz}^{\alpha} p_{iz}^{1-\alpha} \right) \\ &= \frac{1}{\alpha - 1} \log \left(\sum_{z=1}^{k} p_{iz}^{\alpha} q_{jz}^{1-\alpha} * \sum_{z=1}^{k} q_{jz}^{\alpha} p_{iz}^{1-\alpha} \right) \end{aligned} \tag{6}$$

In this context, our EMD is defined as the metric of the minimized amount of work to turn Q into P, where the distance of moving each unit of work is set to be the symmetric relative entropy of order α between P_i and Q_j. We summarize our detection algorithm in Algorithm 1.

IV. Simulation and Evaluation

In this section, we carry out simulations to evaluate the feasibility and effectiveness of our proposed method.

Algorithm 1 DDoS Detection Algorithm Based on EMD Model

Input: Time interval T; the signature P in the last time interval; the signature Q in current time interval; threshold σ.
Output: $EMD(P, Q)$

repeat
  update Q_1, the probability distribution of source IP addresses in current interval; ω_{Q_1}, the total number of OpenFlow packets that controller receives with source IP $\{q_{11}, q_{12}, \cdots, q_{1k}\}$;
  similarly, update Q_2 and ω_{Q_2} for destination IP;
  calculate $d_\alpha(i,j)$ using (6), for $i \in [1,2]$, $j \in [1,2]$;
  substitute $d_\alpha(i,j)$, $\omega_{P_1}, \omega_{P_2}, \omega_{Q_1}$ and ω_{Q_2} into the linear transportation problem (2), and solve it optimally using simplex method to obtain solution set $\mathrm{F} = \{f_{ij}, \forall i \in [1,2], j \in [1,2]\}$;
  calculate $EMD(P, Q)$ with F and $d_\alpha(i,j)$ using (3)
  compare $EMD(P, Q)$ with threshold σ
  if $EMD(P, Q) \geq \sigma$ **then**
    alert attacks
  else
    no attacks, wait until next time instant
  end if
until next time instant.
update $P \leftarrow Q$

TABLE I
Different Attack Intensities on Hosts

Hosts Roles	Sending Intervals $(s/packet)$	Rate $(packets/s)$	Attack intensity
Normal Hosts	0.1	10	\
Attack Hosts	0.05	20	2
	0.033	30	3
	0.025	40	4
	0.02	50	5
	0.0199	60	6
	0.0125	80	8
	0.01	100	10
	0.0083	120	12
	0.00625	160	16

A. Experiments Setup

We choose Mininet [14], which is widely used to simulate SDN network, to perform the data plane of the experimental network as Fig. 1 shown. The topology is composed of sixteen end-hosts, four switches, and one SDN controller. The controller is built upon a 64-bit Ubuntu system with Floodlight [15], which is physically separated but logically connected with Mininet.

In our experiment, the traffic in the network is composed of two parts, the background traffic, and the attack traffic. We generate network traffic by using Scapy [16] and constructing UDP packets on each end-host. The background traffic is generated on hosts at a rate of 10 packets per second. To reproduce the scenario of real DDoS attacks, we inject packets on host 4, 8 and 11, respectively, which play roles as attackers. As mentioned in Sections I and II, we launch DDoS attacks by sending packets with randomized source IP address field. We introduce attack intensity as the times of attack traffic injecting speed to the normal traffic sending speed. To explain it clearly, we list different cases of the attack intensities as shown in Table I.

Firstly, we evaluate the effects of our attacks by measuring the bandwidth of the link between controller and switches, i.e., the southbound link. In Fig. 2, each line represents the average

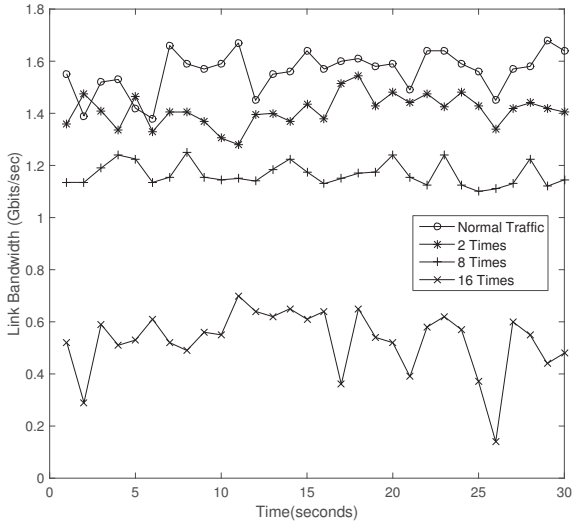

Fig. 2 Link utilization with different attack intensities

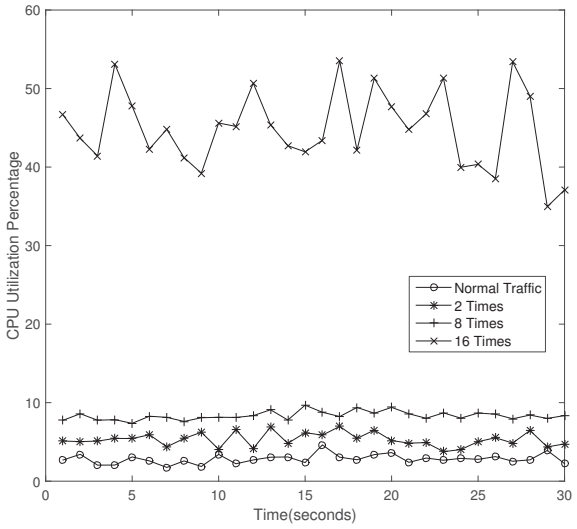

Fig. 3 Controller CPU utilization with different rates of packets injection

bandwidth of southbound link under different restrictions of attack intensity. We can conclude from Fig. 2 that with the increasing of attack intensity, the southbound link utilization rate decreases drastically.

To clearly explain the impacts of DDoS attack, we proceed to evaluate the CPU utilization of the controller as Fig. 3 shown. The scenarios of attacks are the same as the ones displayed in Fig. 2. When the attack intensity achieves sixteen, it occupies nearly fifty percent of controller's CPU. Therefore, the controller is severely affected by our DDoS attack. In this context, we can conclude from Figs. 2 and 3 that our simulations of DDoS attacks are rational and effective.

B. Results and Evaluation

For comparison purpose, we simulate our proposed method together with the Shannon entropy metric (SHA) proposed

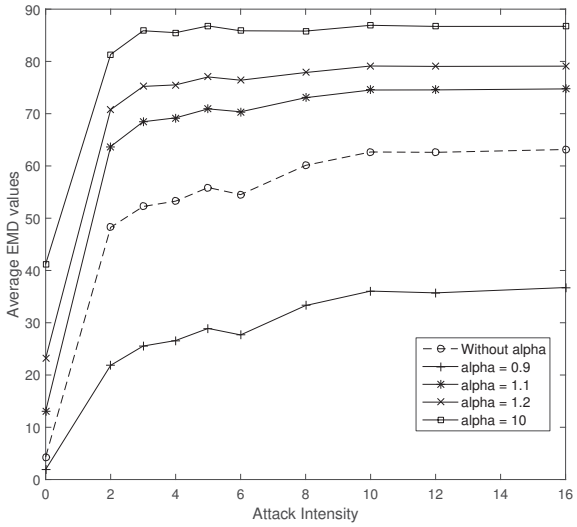

Fig. 4 Values of EMD under different rates of attacks

in [2], the Lyapunov metric (LYP) proposed in [5] and the information distance metric (IDM) in [6].

Firstly, we illustrate the average values of our method during attack intervals in Fig. 4. The x-axis of Fig. 4 represents the attack intensity. In Fig. 4, we denote the results of our method when there is no attack in the network as the ones with x equaling to zero. Each line in Fig. 4 corresponds to a different value of α, which is a parameter defined in (4) and (6). We can see from Fig. 4 that with the increase of α, the average value of our method during attacks also increase. For a certain α, our EMD values are increasing when attack intensity increases. We can also conclude from Fig. 4 that the EMD value suddenly increase when the DDoS attack happens.

Fig. 5 compares the spaces between network traffic with and without attacks of different detection methods. We see that our method outperforms other metrics, i.e., IDM, LYP, and SHA, as it has larger spacings. A larger spacing denotes a more significant difference between normal and abnormal network traffic, which makes it easier to distinguish and identify attacks. We can also conclude from this figure that for our method and IDM, the spacings are getting larger when α grows. However, a bigger α doesn't always represent a better result. This is because when α changes, the detection results of both the normal traffic and abnormal traffic vary. The values of normal traffic are also increasing, and the variances of this distribution become greater. Therefore, the chance of normal traffic being estimated as abnormal traffic is getting bigger.

To further illustrate the detection accuracy, we introduce false positive rate (FPR) and true positive rate (TPR), as given by,

$$FPR = \frac{F}{F_D} \tag{7}$$

$$TPR = \frac{T}{T_D} \tag{8}$$

Here, F represents the number of normal packets that are detected as attack packets, F_D is the total number of

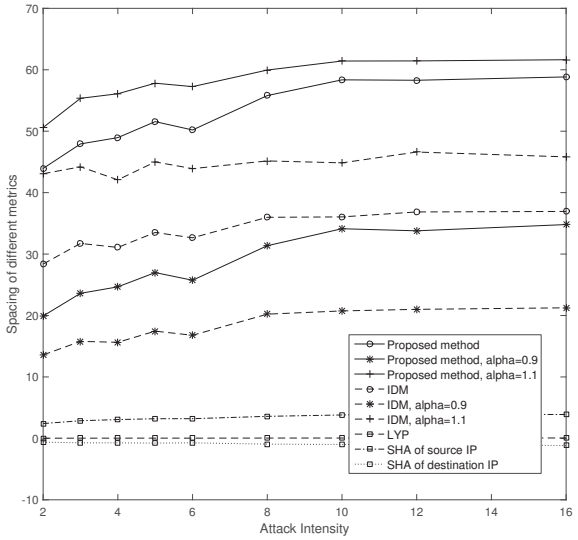

Fig. 5 Space between normal traffic and attack traffic

TABLE II
COMPARISON OF FPR AND TPR FOR DIFFERENT METHODS

Methods	Attack Intensity	α	$FPR(\%)$	$TPR(\%)$
IDM Method	2	\	0	86.96
		0.9	0	80.43
		1.1	0.24	91.30
	4	\	0	83.64
		0.9	0	76.36
		1.1	0.24	92.73
	8	\	0	85.71
		0.9	0	76.62
		1.1	0.24	92.21
	16	\	0	89.72
		0.9	0	80.37
		1.1	0.24	94.39
Proposed Method	2	\	0	89.13
		0.9	0	89.13
		1.1	3.4	93.48
	4	\	0	90.91
		0.9	0	85.45
		1.1	1.46	98.18
	8	\	0	90.91
		0.9	0	81.82
		1.1	0.73	98.70
	16	\	0	93.46
		0.9	0	87.85
		1.1	0.49	99.07

non-attack packets, T denotes the attack packets that are correctly identified, T_D represents all of the truly attack packets. Therefore, FPR indicates the degree of false detection and TPR shows the accuracy of correct detection.

Table II shows the details of FPR and TPR of our method and the information distance metric, i.e., IDM. In this table, the TPR of our method is higher than the IDM's under the same conditions, that is to say, our method is more accurate than IDM. Furthermore, for the case of sixteen times attacks, our method can achieve the detection accuracy of 99.07%. We can also conclude from Table II that FPR increases along with the growing of α. With the increasing of attack intensity, the FPR of our method also decreases.

V. CONCLUSION

In this paper, we propose a DDoS attack detection method based on the algorithm developed in image retrieval area, i.e., the earth mover's distance algorithm. Furthermore, to improve the accuracy of detection, we propose to define an expanded relative entropy to be the distance metric in EMD. Simulation results show that our proposed method can significantly increase the difference between values of normal traffic and attack traffic. Detection accuracy can also be greatly improved, as a large difference always indicates a straightforward recognition of attack traffic.

REFERENCES

[1] P. Zhang, H. Wang, C. Hu, and C. Lin, "On denial of service attacks in software defined networks," IEEE Network, vol. 30, no. 6, pp. 28-33, 2016.
[2] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers," in Computing, Networking and Communications (ICNC), 2015 International Conference on. IEEE, 2015, pp. 77-81.
[3] R. Kokila, S. T. Selvi, and K. Govindarajan, "DDos detection and analysis in SDN-based environment using support vector machine classifier," in Advanced Computing (ICoAC), 2014 Sixth International Conference on. IEEE, 2014, pp. 205-210.
[4] K. Kumar, R. Joshi, and K. Singh, "A distributed approach using entropy to detect DDoS attacks in ISP domain," in Signal Processing, Communications and Networking, 2007. ICSCN'07. International Conference on. IEEE, 2007, pp. 331-337.
[5] X. Ma and Y. Chen, "DDoS detection method based on chaos analysis of network traffic entropy," IEEE Communications Letters, vol. 18, no. 1, pp. 114-117, 2014.
[6] Y. Xiang, K. Li, and W. Zhou, "Low-rate DDoS attacks detection and traceback by using new information metrics," IEEE Transactions on Information Forensics and Security, vol. 6, no. 2, pp. 426-437, 2011.
[7] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges," IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 602-622, 2016.
[8] L. Barki, A. Shidling, N. Meti, D. Narayan, and M. M. Mulla,"Detection of distributed denial of service attacks in software defined networks," in Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on. IEEE, 2016, pp. 2576-2581.
[9] N.-N. Dao, J. Park, M. Park, and S. Cho, "A feasible method to combat against DDoS attack in SDN network," in Information Networking (ICOIN), 2015 International Conference on. IEEE, 2015, pp. 309-311.
[10] X. Huang, X. Du, and B. Song, "An effective DDoS defense scheme for SDN," in Communications (ICC), 2017 IEEE International Conference on. IEEE, 2017, pp. 1-6.
[11] Y. Rubner, C. Tomasi, and L. J. Guibas, "The earth mover's distance as a metric for image retrieval," International journal of computer vision, vol. 40, no. 2, pp. 99-121, 2000.
[12] D. Zhang and G. Lu, "Evaluation of similarity measurement for image retrieval," in Neural Networks and Signal Processing, 2003. Proceedings of the 2003 International Conference on, vol. 2. IEEE, 2003, pp. 928-931.
[13] K. Benton, L. J. Camp, and C. Small, "OpenFlow vulnerability assessment," in Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. ACM, 2013, pp. 151-152.
[14] M. Team, "Mininet," 2014.
[15] S. Floodlight, "OpenFlow controller," Web: https://github.com/floodlight/floodlight.
[16] P. Biondi, "Scapy, a powerful interactive packet manipulation program," 2010.
[17] Y Zhou, W Ni, K Zheng, R. P. Liu, and Y. Yang, "Scalable Node-Centric Route Mutation for Defense of Large-Scale Software-Defined Networks," Security and Communication Networks, 2017.
[18] Y Zhou, K Zheng, W Ni, and R. P. Liu. "Elastic Switch Migration for Control Plane Load Balancing in SDN," IEEE Access, 2018, DOI 10.1109/ACCESS.2018.2795576.

Yang Zhou received the B.S. degree from Beijing University of Posts and Telecommunications, Beijing, China in 2012. She is currently pursuing the Ph.D. degree with the School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, China. She visited CSIRO, Australia, in 2015. Her main research interests lie in software-defined networking, optimization, and cybersecurity defense.

Kangfeng Zheng received the Ph.D. degree in information and signal processing from the Beijing University of Posts and Telecommunications in 2006. He is currently an Associate Professor with the School of Cyberspace Security, Beijing University of Posts and Telecommunications. His research interests include network security and network data analysis.

Wei Ni (M'09–SM'15) received the B.E. and Ph.D. degrees in electronics engineering from Fudan University, Shanghai, China, in 2000 and 2005, respectively. He was a Research Scientist and Deputy Project Manager with the Bell Labs R&I Center, Alcatel/Alcatel-Lucent, from 2005 to 2008, and a Senior Researcher with Devices R&D, Nokia, from 2008 to 2009. He is currently a Senior Scientist, Team Leader, and Project Leader in CSIRO, Australia. He also holds adjunct positions with the University of New South Wales, Macquarie University, and the University of Technology, Sydney. His research interests include optimization, game theory, graph theory, and their applications to network and security.

Dr. Ni has been serving as an Editor of the Hindawi Journal of Engineering since 2012, the Secretary of the IEEE NSW VTS Chapter since 2015, and the Track Chair of VTC-Spring 2017, and served as the PHY Track Co-Chair of the IEEE VTC-Spring 2016 and the Publication Chair for BodyNet 2015. He also served as the Student Travel Grant Chair of WPMC 2014, a Program Committee Member of CHINACOM 2014, and a TPC Member of the IEEE ICC'14 Workshop on body area networks, ICCC'15, EICE'14, and WCNC'10.

Ren Ping Liu (M'09–SM'14) was a Principal Scientist of CSIRO, where he leads wireless networking research activities. He joined the University of Technology Sydney as a Professor of Networking Technologies with the School of Computing and Communications in 2016. He specializes in protocol design and modeling, and has delivered networking solutions to a number of government agencies and industry customers. His research interests include Markov analysis and QoS scheduling in WLAN, VANET, IoT, LTE, 5G, SDN, and network security.He has over 100 research publications, and has supervised over 30 Ph.D. students.

Prof. Liu received the B.E. (Hons.) and M.E. degrees from the Beijing University of Posts and Telecommunications, China, and the Ph.D. degree from the University of Newcastle, Australia. He is the Founding Chair of the IEEE NSW VTS Chapter. He served as a TPC Chair of BodyNets2015, ISCIT2015, and WPMC2014, as an OC Co-Chair of VTC2017-Spring, BodyNets2014, ICUWB2013, ISCIT2012, SenSys2007, and on the Technical Program Committee in a number of the IEEE conferences.