EAI Endorsed Transactions
on Cloud Systems

Research Article EAI.EU

Adaptive Learning Method for DDoS Attacks on Software Defined Network Function Virtualization

S. Janarthanam[1,*], N. Prakash[1] and M. Shanthakumar[2]

[1]Assistant Professor, Department of Computer Science, Gobi Arts & Science College, Gobichettipalayam, Erode, Tamilnadu, India.
[2]Assistant Professor, Department of Computer Science, Kamban College of Arts & Science, Coimbatore, Tamilnadu, India.

Abstract

Software Defined Network (SDN) system controller stands with excessive benefits from the separated promoting devices. The SDN will resolve security issues, inheritance community with acute liabilities. The most important exposure is DDoS attack. The goals of this work to endorse a learning technique on DDoS attacks by SDN based system. Disturb the user's defensible actions elevate to advise Adaptive Learning method (ALM) as advance set of SVM to return certain viabilities. This paper notices two types of flooding-based DDoS attacks. Proposed Virtualization method decreases the exercise and testing time using the key features, namely the volumetric and the asymmetric features. The accurateness of the revealing process is around 97% of fastest practice and investigation time.

Keywords: Denial of Services, Software Defined Network, Support Vector Machine, Virtualization Functions, Networking.

Handling Editor: Sathishkumar Karupusamy, University of Africa, Nigeria

Received on 16 April 2020, accepted on 01 September 2020, published on 07 September 2020

doi: 10.4108/eai.7-9-2020.166286

1. Introduction

The growing absorption of hypermedia amenities and the mandate of extraordinary eminence facilities from consumers have triggered an important change in the administer networks in terms of concept, separation, and planning of progressing, mechanism and organization aspects of facilities. Software defined networking (SDN) has progressed and conveyed a pioneering paradigm transferal in computer networks by developing a programmable software direction with exposed protocols [1].

Network functions, earlier served on devoted hardware, have shifted to network function virtualization (NFV) that permitted commitments to be virtualized and provisioned energetically upon basic hardware. In addition to NFV, edge computing employs the edge properties close to end-users can reduce the end-to-end service interruption and the network traffic volume these pioneering technologies gained important consideration on notion of network virtualization in the telecommunication arena along with software-defined networking (SDN). The network functions, such as firewall, representation, and intrusion detection system (IDS), used to be served by an affluent hardware purpose-built only for certain system utilities [2]. As network functions are CPU concentrated responsibilities, the network providers have to procurement the enthusiastic device to provide the essential utilities to the customers on demand.

The progression of virtualization expertise in cloud computing dynamically scaled, provisioned, and migrated in clouds, virtualized network functions (NFVs) can be also provisioned throughout generic physical machines to provide a certain network function in the uncertainty situation. In the core, the numerous benefits offered by the technologies is on infrastructure for connecting machine learning (ML) algorithms and cloud computing software tools, for illustration in conniving progressive data analytics platforms[3]. The area of increased interest, the information exertion offerings a method of data analytics platform built around the perception of industry 4.0. The platform utilizes the state-of-the-art on IoT platforms for concentrated mini clouds, ML algorithms and big-data software tools on analytics demand in nature. The stand give emphasis to the

*Corresponding author. Email:professorjana@gmail.com

use ML methodology course data analytics but leveraging big-data handling gears and captivating benefit of the currently available industrial evaluation cloud computing platforms[4].

This research work providing an accessible and effective procedure for NFVs placement and chaining combined with protective and responsive mechanisms to address physical link failures and consistency in uncertain network [5]. Also to compute the optimum entrenching is to enumerate the entire entrant hosts used for each virtual means i.e., node and/or link within the somatic network known as hardware nodes and/or paths.

The remainder of the paper is structured as keep an eye on Section 2 discusses existing platforms and simulation tools in the literature. Section 3 contributions on the exhibiting and simulation of NFV in edge and cloud computing environments. The detailed strategy and plan to implementation of the new simulation framework are in Section 4. Use case scenarios and evaluation results using the simulation framework are presented in Section 5. Also discusses the potential extensions of proposed framework, which can be implemented for supporting in different scenarios. Finally, Section 6 summarizes and concludes the paper.

2. Related Work

In this section certain related works are investigate the state-of-the art as reference. A number of mechanisms have been proposed and presented in the collected works to simulate cloud, edge, and fog computing, and networking methods are also established for NFV evaluation.

In [6], authors proposed an Eigen decomposition based approach for joint NFVs placement and traffic steering of the associated forwarding paths and graphs. A heuristic process based on a greedy algorithm is also presented to solve the problem iteratively. The Greedy solution is based on bipartite graph construction and matching techniques and solves the problem in two steps by mapping NFVs then steering traffic between them. This problem is challenging because it involves jointly determining the placement of NFV nodes as well as constructing a multicast topology that connects the source and destination through the NFV node.

In [7], authors proposed an ILP and a heuristic for NFV placement and chaining based on a transformation of the problem by adding new virtual switches. The idea is to model the problem as a Multi-Stage directed graph and to run the Viterbi algorithm [8] on it. All this prior art addresses NFV placement and chaining does not consider resource failures and there have been no attempts to handle failure recovery automatically.

In [9] a novel rendezvous point based algorithm is proposed to build a multicast tree which satisfies several constraints, including delay constraint, link utilization constraint, while minimizing the total cost. However, all of the paper is focused on generating the multicast tree with minimum cost, none of these papers has considered the joint NFV placement and multicast tree construction.

While [10] offers a agenda to transfer the traditional network to SDN by virtualizing the link functionality of the entries, while [11] presents a structure called Open ANFV acts as an accelerator to decrease the gap between the software based network function and the hardware, and [12] presents a software intermediate packet platform quickly boot up virtual machines to run the internal package functions. Meanwhile, NFV has been deployed to facilitate the operations on content delivery network [13], [14] presents analysis and design of the routing function virtualization. [15] Presents a control plane that allows the jointly controlled network topology and NFV placement. And [16] offers a test bed called Empower for research on NFV then none of these studies has focused on the traffic engineering problem involving with NFV on cloud services.

The applications of SDN reside in the application plane of SDN architecture where the northbound application programming interface (API) provides the commutation between the application and control planes [17], which allows implementing a set of network services such as traffic engineering, intrusion detection, quality of service (QoS), firewall and monitoring applications [18]. Northbound API allows developers to write their own applications without the need for a detailed knowledge of the controller functions or understanding how the data plane works. It is worth mentioning that several SDN controllers provide their own northbound APIs [16].

The communication between control and data planes is provided using a southbound API such as forwarding and control element separation (ForCES) [19], open vSwitch database (OVSDB), protocol oblivious forwarding (POF) , Open State , Open Flow (OF) and OpFlex [20], which enables exchanging control messages with forwarding elements As shown in Figure 1.

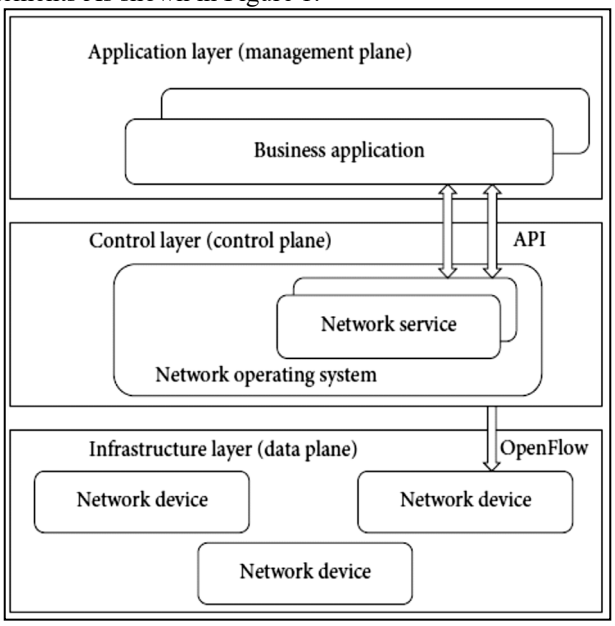

Figure 1. The Eventual Structural design of SDN

3. Service Attacks

Software Defined Networking (SDN) is an up-and-coming network construction that the network control is dynamic, controllable, adjustable, and materially detached from accelerating devices [21]. The main contests of SDN are consistency, scalability, retreat, and interoperability. Among the emphasize encounters on the security of SDN each plane of SDN has susceptibilities. In the information level, single network device switches quite vulnerable to different kind of attacks on provider services such as Denial of Service (DoS) attack, Distributed Denial of Service (DDoS) attack, data alteration, negation, black hole attack, and side channel attack.

DoS and DDoS are the popular attacks on the data plane of the network cannot be accessed by the genuine users. In the control plane, the control is the easiest target of DDoS because the first packet of each flow must be sent to the controller, and in sometimes it can cause a bottle neck condition. The malicious attacks like DoS, black hole, and fake flow rule generation can also occur at the control plane. In the application plane the some vulnerability concerning the DDoS attack considered in Smart City application.

Detections of Service Attacks using SDN

DDoS attacks are detected on the SDN network by using the Advanced Support Vector Machine (ASVM) method. The proposed research presents a customizable DDoS defence structure generates DDoS attack alerts by considering the application's security desires [22]. So the projected work has been enthused by the notion on dissimilar claims need different security requirements.

The proposed context considers the uncertainty of DDoS attack acquaintance response need encompass a customized alert mechanism for generating DDoS attack. So proposed the handler mechanism leverages interface design with active environment and equipment an adaptive DDoS defence NFV mechanism. DDoS attacks are easy to release mainly tough to defend cyber attackers release often the same, a network of computers is named a botnet. For the securing the service processing protection the DDoS attacks are often labelled into categories based at the directed conventions platform [25] as:

Network or sharing proximate DDoS flooding attacks

These contractions terrified the enormous treatment of TCP, UDP, ICMP and DNS protocol packets and specialize in disrupting genuine person's connectivity from end to end along the demanding network's bandwidth.

Application-level DDoS flooding attacks

Individual attacks cognizance on demanding open patrons' abilities of hard the server properties (e.g., Sockets, CPU, memories, disk/database bandwidth, and I/O bandwidth). The reputation of portable gadgets with smartphones and tablets has predictable to materialize as a critical generation attitude for DDoS attacks against cloud computing. The shortage of safety on the general public of cellular expedients coupled with the growing bandwidth and processing.

Electricity makes ripe platform for hackers on the way to concern. Researchers reported noticeable Android malware might to launch DDoS attacks in 2013 [23]. Cruel invaders now bring a powerful physical attack tool inside the rave overview of their impacts need the insignificant ability requests to use.

3.1. Rapid Firmness and Amenity Dealings to a New Breed

Immediate resistance and dignified provision adopters of the fog amenities remain charged based on a demand basis, the fog related link possessions using a conventional model DDoS spasm on connected resources is transformed. Cloud setting renovated a new breed of intruder attacks the targets with the cloud adopter financial stock. The package data will be decorative as the material on the packet header fields together with source port, terminus port, foundation IP address, and destination IP address.

The evidence of the incoming packets checked against the flow entries, if a match is found then a specified action can be executed. Otherwise, the packet will be sent to the Uncluttered Daytime controller via the southbound API using a packet_in control message. Controllers are connected as a cluster. Once the traffics arrived at the Exposed Dawn controller cluster will forwarded via the northbound API to the Recognition of DDoS attack by proposed algorithm of application layer. The package self-control is categorized as DDoS spasm transportation or a normal. The components of proposed structure consists the modules including the transportation peer group, the stream of traffic data collection for the feature extraction and recognition of attack.

3.2. Transportation Peer group

The cohort of twofold DDoS occurrence traffics and normal traffics is realized in this exertion. Two DDoS attacks are UDP saturating attacks and SYN inundating attacks. UDP flooding attack is a type of Denial of Service (DoS) spasm in the random ports on the object's congregation resolve exist inundated per IP packets with User Datagram Protocol (UDP). UDP flooding attack mainly acute the fatalities IP addresses are determined then the foundation port and the destination port are reset to 80 and 1. All time, 2000 containers are generated. The packets bury entrance time for UDP attack traffics is 0.03 seconds. Scapy, a packet peer group tool for processor systems written in python language is used for producing the packets in this work.

Scapy can also switch tasks like skimming, smidgen routing, penetrating, unit tests, spasms, and linkage discovery. Once the packet is created, it must be sent to the target IP address within the time interlude. The step by step procedure of the UDP saturating attack on the SDN network shown in Figure 2. SYN flooding attack is a type of DoS spasm exploits the standard three-way handshake technique to ingest the possessions on the battered server and render it pokerfaced by using the TCP construction. Every time, 1000

packets are produced because the regular number of packs at a normal condition is around 1000 packets. The packets inter arrival time for ordinary traffic flow generation is 0.1 second. The accidental basis IP address is used each time.

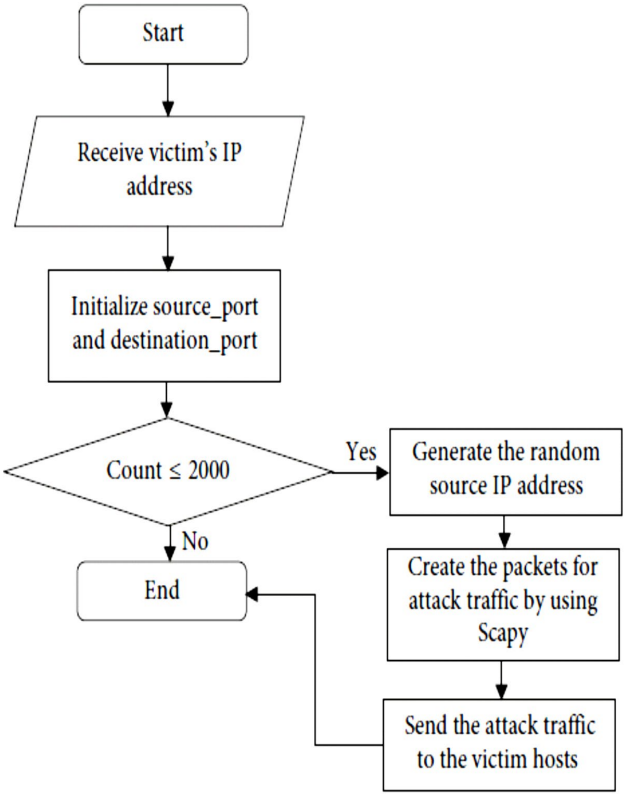

Figure 2. Step by step UDP Flooding Spasm Process.

3.3. Traffic Data Collection

In SDN, the traffic data are stored in the flow table to extract the traffic data, the Exposed Course control responds to the open flow_stats_request communication and intermittently directs this request communication to the organizer. Most DDoS attacks mitigating instruments need to assemble data to construct normal summary or to detect abnormals. DDoS attacks have increased in size in cloud atmospheres, collecting fabulous and dissimilar facts with a squat overhead is flattering more and more difficult. Moreover the facts of fog transportation is disseminated between network devices by contents matching and the multi-tenant environment of fog environs make the undertaking of data collection for marginating DDoS attacks firmer to attain.

The attacks have increased impediment in cloud atmospheres, various intellectual procedures have been used, including artificial neural network, chaotic analysis, Bayesian cataloguing, game theory, hidden semi-markov model (HSMM), and fuzzy logic and so on. Due to the difficulty of DDoS attacks, there is no particular intellectual system can deal with all DDoS attacks. Choose dissimilar brainy systems rendering to altered spasms are problematic complications to solve.

4. The Edge to Core Cloud Model

The correctness of the representations and their capability to assess new data is contingent on the depth of the neural networks and the amount and quality of the training data. The rate at DL datasets produce can be surprising an end-to-end DL model distribution consists of three phases from side to side the data travels: edge (data ingest), core (training clusters, data lake), and cloud (data archival).

This effort of data is identical characteristic in presentations such as IoT data spans with three phases of the data channel. Figure 3 illustrates the stages of the data pipeline. The cloud can be leveraged in several ways can use GPU illustrations for reckoning, and can use cloud for cold storage tiering archives and backups. In many AI applications, the data might span across the edge and/or the core and/or the cloud. As the orchestrate data across these environments leveraging the adaptive method mentioned above and the existing algorithm in machine learning can make a decision for expanding or contracting nodes.

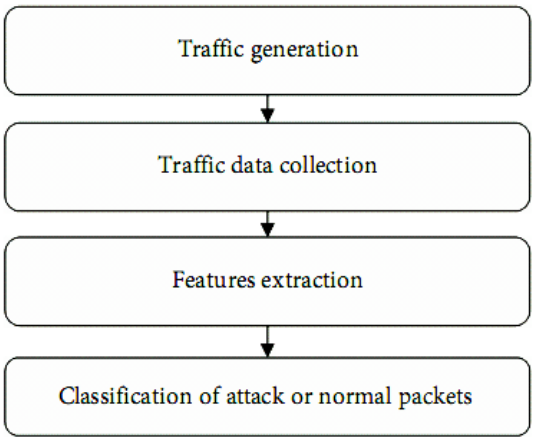

Figure 3. Modules of proposed system framework

The heavy hitters are enigmatic, formerly consider the process as unsupervised learning. The machine learning of the Heavy Hitter Detection is training set, in the current scenario is the flow statistics, ω signifies two causal status of a network.

$$\omega = \begin{cases} 1, & \text{heavy hitter network state} \\ 0, & \text{normal network activity} \end{cases} \quad (1)$$

The persistent upgrading in cloud proficiencies with SDN in Mobile Clouds (SDMC) aims at innovation and development of future converged mobile networks. SDN and NFV [24] combined together leveraging the intelligent services orchestration and dynamic resources management. SDN independently aims at decoupling the networks' mechanism commencing the data planes. The generalization of essential system infrastructure manipulates complete capabilities through the sensibly integrated intellect system influences on SDNs proven in figure 4.

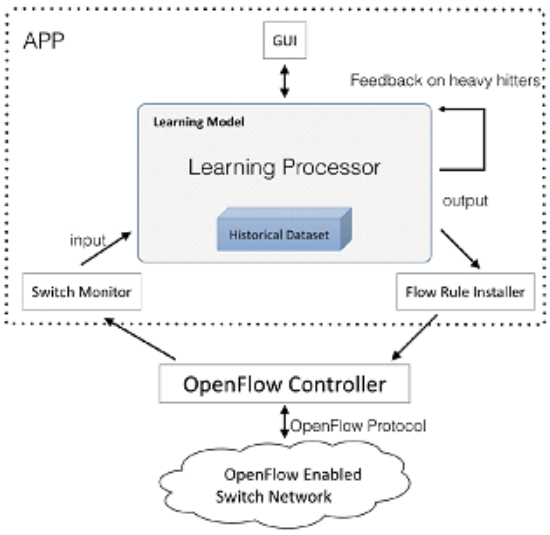

Figure 3. Architecture of heavy hitter Algorithm

SDN allocates signals as recommendations to system controls in the excess of various dropping scalability stress at low-cost. For the packet gateway providers permit flexible traffic handling with Scalability can be drastically raised with actual-time updates. The satisfactory-grained packet dealing instructions on forwarding state at specific subscriber level leads to shared operator mobility with prompt state transformation to preserve missing as of transporter distractions. First-rate-grained traffic quantities tracking with the aid of modifications assure to notice at what time subscribers go beyond their custom limits.

The QoS machine strategies ought to short statistics extent or transcode at ease to concession highest package deal via bits of delaying concerns are addressed by flexible subscriber policies. The huge growth of records, visitors and related nodes has to be assisted with such services.

Developing knowledge on SDN network characteristic Virtualization (NFV) and Cloud Presuming notions are progressing to deal with the necessities of destiny cell networks. The potential benefits of mechanism administration of SDN is a novel system, career positioning and community structure evolvement and additionally those reimbursements should invaluably follow in unique interacting situations like datacentres, wireless networks, broadband get right of entry to networks and campus networks. And also these remunerations could invaluably relate in exceptional networking environments like datacentres, wireless Networks, broadband access networks and campus networks.

This technology offers services according to users' requirements and it is possible to be scaled while keeping low costs. For this reason, the cloud computing environment is being adopted by more and more organizations. However, this quick evolution towards the cloud has increased the concerns on security perspective since some risks and challenges have appeared due to the use of cloud computing. The composed malevolent transportation movements on the SDN system container should analysed by reviewing different distinctive standards of the up-to-date counter.

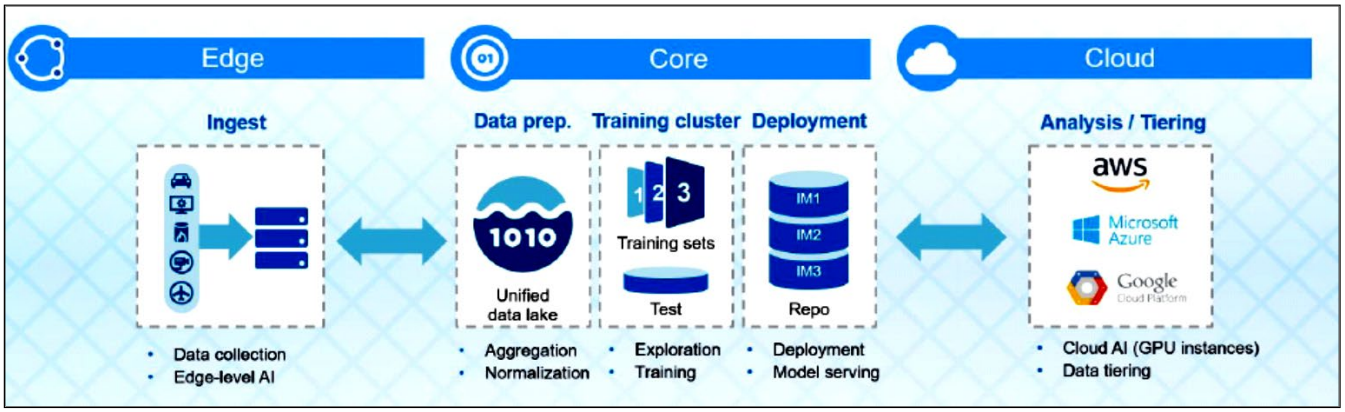

Figure 4. Edge Process to Core Cloud Model

5. Evaluation Results

The inquiries of the portraits are confirmed on the Mininet (version 2.3.0d1) emulator on the method to generate the SDN system topology on an Ubuntu 16.04 VMware. Mininet is a net emulator that runs the group of hosts, controls, routers, and links on a single Linux kernel, and its effects are as identical as a real community [25]. Most of DDoS attacks practice at minimum three hosts, and the wide variety of hosts can be as much as approximately one hundred hosts and the quantity of controllers used can range from one to as a whole lot as feasible.

Proposed Mechanism of SDN check mattress includes one hundred hosts (h1to h100), 9 switches (s1 to s9), and three controllers (c0, c1, c2). Four subnets are organized in our test mattress. The experimentations are established up on Miniedit. Miniedit is an easy GUI editor for Mininet Figure 5 suggests our realistic receipts at test bed.

In every situation, the transportation peer group is started then the traffic flow glide data from every control

might be physically grown on or after every single switch. After processing the time and the gathering of establish invitees particulars intended for each state of activities, five exclusive features are extracted for the proposed algorithm to start crossways of the DDoS attack.

5.1. Feature Extraction

For volumetric and irregular environment of the transportation configurations, the dissimilar procedures of conveyance topographies to be appraised collectively with wide variety normal packets within the control organization interval (CNPI), dissimilarity of glide databases within the cross section (VPI), and ordinary transportations inside the selection period (RITI).

CNPI is the sum of the wide variety of float packages respectively point per total flows on the sampling period as shown in Equation(2). ANPI is used for a revealing the DDoS attack on the SDN open environment of DDoS physical attack is sending a large quantity of plug-ins as a way to incapacitate the organizer.

$$\text{CNPI}=\frac{\sum_{i=1}^{n}\text{flow packet}_i}{\text{total flows}} \qquad (2)$$

VPI is the feature of normal irregularity of the quantity of present variation implication as given in Equation (3). The noticed the DDoS attack on SDN community via bearing in views the VPI utility because maximum DDoS attackers casually create the packets if you want to send to the hosts no longer keep in mind the packed statistics packet and typically void packets are used.

$$VPI=\sqrt{\frac{\sum_{i=1}^{\text{total flows}}(\text{flow packages}_i-\text{CNPI})^2}{\text{total flows}}} \qquad (3)$$

RITI is the sum of every time of the SDN traffic in keeping with a spread interlude as proven in Equation (4) can sense a malicious traffic nature through evaluating the RITI function of the SDN site visitors.

$$\text{RITI}=\frac{\text{All time duration of SDN traffic}}{\text{Selection interval}} \qquad (4)$$

5.2. Estimation of Concern Outcome

Multidimensional facts have resolved Exercises and analysis DS are our studies's principal problem of multiclass. the second trouble of the extended training time and testing time of conventional algorithm has been solved through the usage of the linear kernel with effect constraint of the company fault time period, 'C,' thinking about the price of "gamma" and "OVS" pronouncement function shape. Fake alarm rate, discovery rate, and accuracy are used for comparing our detection result. False alarm value is the error rate of our recognition method is the incorrect result on an conventional performance.

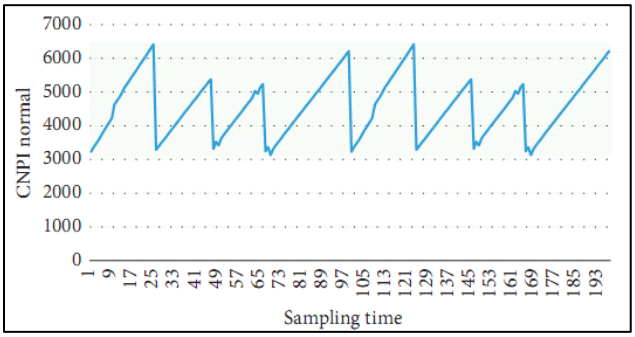

Figure 5. Features of CNPI for Usual Traffic flow

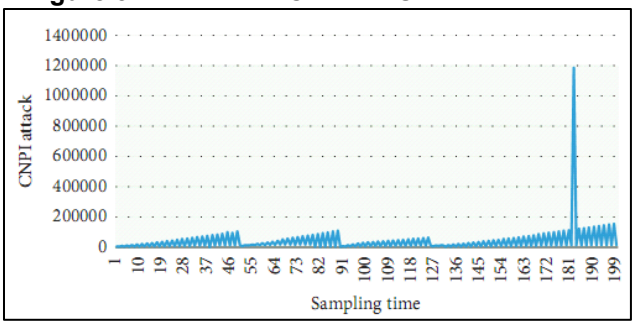

Figure 6. Features of CNPI for Violence Traffic flow

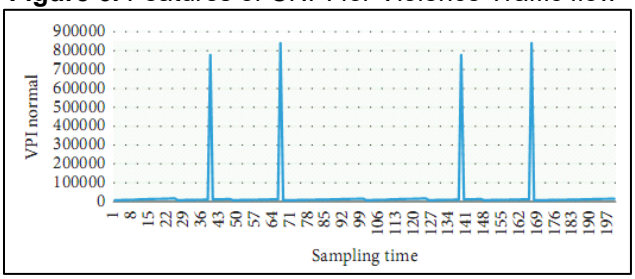

Figure 7. Topographies of VPI for Public Carriages

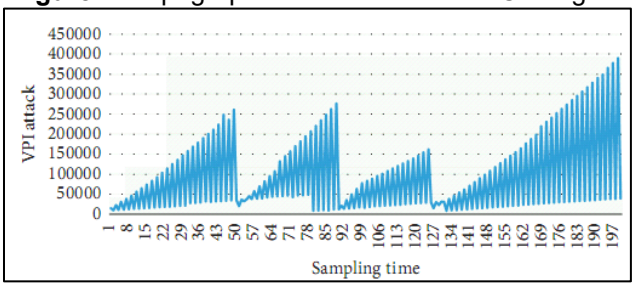

Figure 8. Features of VPI for Violence Carriages

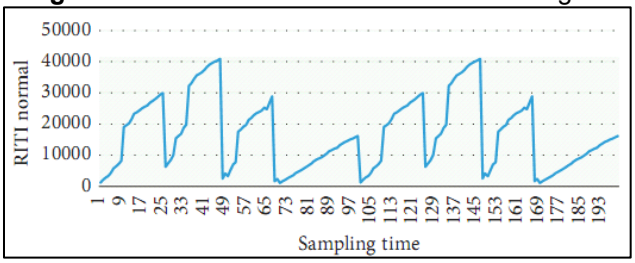

Figure 9. RITI Features for Normal Traffics

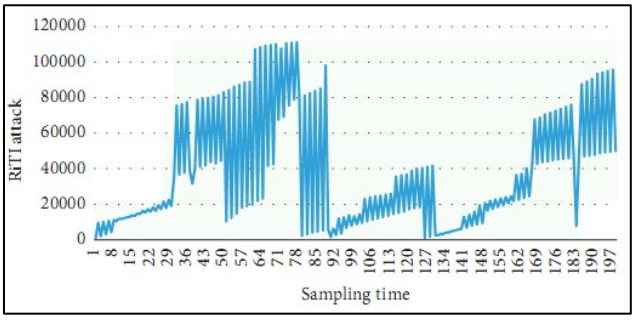

Figure 10. Features of RITI for Attack Traffic flow

Keeping with the experimental significances recognized in table 1, the typical accuracy of the detection is 0.97, the mutual fake alarm rate is 0.02, and the mediocre detection responsibility is 0.97. The initiating period and demanding out time for each subscription are approximately 50 seconds and 55 seconds, respectively.

Table 1. Experimental significances

Split time	Exercise Data	Exciting Data	False alaram rate	Exposur e Rate	Precision
0.1	90	10	0	1	1.0
0.2	80	20	0.06	0.92	0.92
0.3	70	30	0.02	0.98	0.97
0.4	60	40	0.03	0.97	0.97
0.5	50	50	0.01	0.99	0.99
0.6	40	60	0.01	0.98	0.97
0.7	30	70	0.01	0.99	0.99
0.8	20	80	0.02	0.96	0.96
0.9	10	90	0.03	0.97	0.97

6. Conclusion

The SDN transportations from the Open Flow adjustments are composed. The volumetric and imprecise features beginning the SDN transportations are gathered and extracted to create the dataset. Cross-validation approach is employed for instructing and demanding out the perfect classification. Linear kernel is used in our proposed algorithm with the experimental outcomes, the overall accuracy of the proposed version is at 97%. Our destiny works include a web detection device for DDoS violence on SDN system.

References

[1] T. Dang-Van and H. Truong-_u, "A multi-criteria based software defined networking system Architecture for DDoSattack mitigation," REV Journal on Electronics and Communications, vol. 6, no. 3-4, 2016.

[2] T. Evgeniou and M. Pontil, "Support vector machines: theory and applications," Machine Learning and Its Applications: Advanced Lectures, vol. 2049, pp. 249–257, 2001.

[3] S. Badotra and J. Singh, "Open daylight as a controller for software defined networking," International Journal of Advanced Computer, vol. 8, no. 5, 2017.

[4] S. Kolahi, K. Treseangrat, and B. Sarrafpour, "Analysis of UDP DDoS flood cyber-attack and defense mechanisms on Web Server with Linux Ubuntu 13," in Proceedings of the 2015 International Conference on Communications, Signal Processing, and their Applications (ICCSPA'15), London, UK, June 2015.

[5] R. Bani-Hani and Z. Al-Ali, "SYN flooding attacks and countermeasures: a survey," in Proceedings of ICICS, Beijing, China, 2013.

[6] F. Gharvirian and A. Bohlooli, "Neural network based protection of software defined network controller against distributed denial of service attacks," International Journal of Engineering, vol. 30, no. 11, pp. 1714–1722, 2017.

[7] R. T. Kokila, S. _amarai Selvi, and G. Kannan, "DDoS detection and analysis in SDN-based environment using support vector machine classifier," in Proceedings of the 2014 Sixth International Conference on Advanced Computing (ICoAC), Chennai, India, December 2014.

[8] Y. Chi Wu, H. Tseng, W. Yang, and R. Hong Jan, "DDoS detection and traceback with decision tree and grey relational analysis," in Proceedings of the 2009 $ird International Conference on Multimedia and Ubiquitous Engineering, Qingdao, China, June 2009.

[9] L. Linxia, V. C. M. Leung, and L. Chin-Feng, "Evolutionary algorithms in software defined networks: techniques, applications, and issues," ZTE Communications, vol. 15, no. 3, 2017.

[10] N. Anandshree Singh, K. Johnson Singh, and T. De, "Distributed denial of service attack detection using naive bayes classifier through info gain feature selection," in Proceedings of the International Conference on Informatics and Analytics, Pondicherry, India, August 2016.

[11] M. I. W. Pramana, Y. Purwanto, and F. Yosef Suratman, "DDoS detection using modified K-means clustering with chain initialization over landmark window," in Proceedings of the 2015 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC), Bandung, Indonesia, August 2015.

[12] K. Benzekki, A. El Fergougui, and A. Elbelrhiti Elalaoui, "Software-defined networking (SDN): A survey," Security and Communication Networks, 2017.

[13] S. Kazuya, S. Kentaro, T. Nobuyuki et al., "A survey on OpenFlow technologies," IEICE Transactions on Communications, vol. E97.B, no. 2, pp. 375–386, 2014.

[14] N. Zakaria Bawany and J. A. Shamsi, "Application layer DDoS attack defense framework for Smart city using SDN," in third International Conference on Computer Science, Computer Engineering, and Social Media (CSCESM), _essaloniki,Greece, May 2016.

[15] N. Dayal, P. Maity, S. Srivastava, and R. Khondoker, "Research trends in security and DDoS in SDN," Security and Communication Networks, vol. 9, no. 18, pp. 6368–6411,2016.

[16] A. Akamai, "State of the internet/security," SOTI, vol. 4, no. 5, 2018.

[17] A. Akamai, Memcached Reflection Attacks: A NEW era for DDoS, Akamai Technologies, Cambridge, MA, USA, 2018.

[18] S. Acharya and N. Tiwari, “Survey of DDoS attacks based on TCP/IP protocol vulnerabilities,” IOSR Journal of Computer Engineering, vol. 18, no. 3, pp. 68–76, 2016.
[19] M. Bogdanoski, A. Risteski, and T. Shuminoski, “TCP SYN flooding attack in wireless networks,” in Proceedings of theConference: Innovations on Communication $eory, INCT, Istanbul, Turkey, October 2012.
[20] S. H. Mujtiba and G. R. Beigh, “Impact of DDoS attack (UDP flooding) on queuing models,” in Proceedings of the 2013 4th International Conference on Computer and Communication Technology (ICCCT), Allahabad, India, September 2013.
[21] H. Harshita, “Detection and prevention of ICMP flood DDOS attack,” International Journal of New Technology and Research (IJNTR), vol. 3, no. 3, pp. 63–69, 2017.
[22] A. Verma and D. Kumar Xaxa, “A survey on HTTP flooding attack detection and mitigating methodologies,” International Journal of Innovations and Advancement in Computer Science, vol. 5, no. 5, 2016.
[23] F. Yihunie, A. Eman, and A. Odeh, “Analysis of ping of death DoS and DDoS attacks,” in Proceedings of IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, May 2018.
[24] S. Asadollahi, B. Goswami, and A. M. Gonsai, “Implementation of SDN using OpenDayLight controller,” in Proceedings of the International Conference on Recent Trends in IT Innovations-Tec´afe, vol. 52, no .2, India, April 2017.
[25] F. Tang, P. Ti˘nno, P. A. Guti´errez, and H. Chen, “_e benefits of modelling slack variables in SVMs,” Neural Computation, vol. 27, no. 4, 2015.