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/_____

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

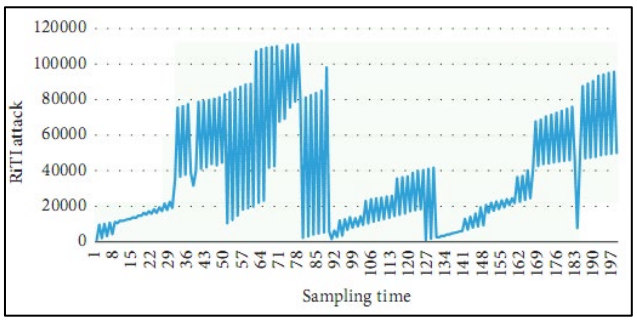

Figure 10. Features of RITI for Attack Traffic flow

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.