IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

Detection and Mitigation of (D)DoS Attacks in SDN Environment Using Entropy

[1]Akanksha Shah, [2] Riddhi Ghate, [3] Sakshi Kalekar, [4] Ruchi Nitsure, [5]Jibi Abraham, [6]Ashwini Matange
Department of Computer Engineering[1,2,3,4,5,6]
College of Engineering, Pune, India
[1]shahas18.comp@coep.ac.in, [2]ghaterp18.comp@coep.ac.in, [3]kalekarss18.comp@coep.ac.in,
[4]nitsurerm18.comp@coep.ac.in, [5]ja.comp@coep.ac.in, [6]asm.comp@coep.ac.in

Abstract: *Software Defined Networking (SDN) is a paradigm for the networks, where the control planes and data planes are separated. It provides centralized network control by separating the network's control logic from the underlying hardware devices. However, like traditional networks SDN is also susceptible to Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. This paper aims to detect and mitigate DoS and DDoS attacks in an SDN environment using an entropy-based approach. The proposed mechanism calculates the entropy of the network over the collected traffic, and derives a dynamic threshold according to the network traffic conditions to determine whether the environment is subject to DoS or DDoS attacks. In the event of the attack, the proposed mechanism installs a drop flow rule into underlying forwarding devices, discarding the traffic sent from attacking host to victim host.*

Keywords: Software Defined Networking, Denial of Service, Entropy, Dynamic Threshold, POX

REFERENCES

[1] Nada M AbdelAzim, Sherif F Fahmy, Mohammed Ali Sobh, and Ayman M BahaaEldin. A hybrid entropy-based dos attacks detection system for software defined networks (sdn): A proposed trust mechanism. Egyptian Informatics Journal, 22(1):85–90, 2021.

[2] ZakariaAbou El Houda, AbdelhakimSenhajiHafid, and LyesKhoukhi. Cochain-sc: An intra-and inter-domain ddos mitigation scheme based on blockchain using sdn and smart contract. IEEE Access, 7:98893–98907, 2019.

[3] Wolfgang Braun and Michael Menth. Software-Defined Networking Using OpenFlow: Protocols, Applications and Architectural Design Choices.Published in Future Internet, 2014.

[4] J Dalou, Basheer Al-Duwairi, and M Al-Jarrah. Adaptive entropy-based detection and mitigation of ddos attacks in software defined networks. International Journal of Computing, 19(3):399–410, 2020.

[5] Jisa David and Ciza Thomas. Ddos attack detection using a fast entropy approach on flow-based network traffic. Procedia Computer Science, 50:30–36, 2015.

[6] Guo-Chih Hong, Chung-Nan Lee, and Ming-Feng Lee. Dynamic threshold for ddos mitigation in sdn environment. In 2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), pages 1–7. IEEE, 2019.

[7] Yajie Jiang, Xiaoning Zhang, Quan Zhou, and Zijing Cheng. An entropy based ddos defense mechanism in software defined networks. In the International Conference on Communications and Networking in China, pages 169–178. Springer, 2016.

[8] Prashant Kumar, MeenakshiTripathi, Ajay Nehra, Mauro Conti, and ChhaganLal. Safety: Early detection and mitigation of tcpsyn flood utilizing entropy in sdn. IEEE Transactions on Network and Service Management,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

15(4):1545–1559, 2018.

[9] BabatundeHafisLawal and A. T. Nuray. Real-time detection and mitigation of distributed denial of service (ddos) attacks in software defined networking (sdn). pages 1–4, 2018.

[10] KashifNisar, Emilia Rosa Jimson, MohdHanafi Ahmad Hijazi, Ian Welch, Rosilah Hassan, AzanaHafizahMohdAman, Ali Hassan Sodhro, Sandeep Pirbhulal, and Sohrab Khan. A survey on the architecture, application, and security of software defined networking: Challenges and open issues. Internet of Things, 12:100289, 2020.

[11] Maninder Pal Singh and Abhinav Bhandari. New-flow based ddos attacks in sdn: Taxonomy, rationales, and research challenges. Computer Communications, 154:509–527, 2020.

[12] Rochak Swami, Mayank Dave, and VirenderRanga. Defending ddos against software defined networks using entropy. In 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), pages 1–5. IEEE, 2019.

[13] POX Installation and Documentation - https://noxrepo.github.io/pox-doc/html/

[14] Scapy network traffic generation and packet manipulation https://scapy.readthedocs.io/en/latest/index.html

[15] Mininet - http://mininet.org/

[16] https://www.netscout.com/report/