World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:15, No:11, 2021

BFDD-S: Big Data Framework to Detect and Mitigate DDoS Attack in SDN Network

Authors : Amirreza Fazely Hamedani, Muzzamil Aziz, Philipp Wieder, Ramin Yahyapour

Abstract : Software-defined networking in recent years came into the sight of so many network designers as a successor to the traditional networking. Unlike traditional networks where control and data planes engage together within a single device in the network infrastructure such as switches and routers, the two planes are kept separated in software-defined networks (SDNs). All critical decisions about packet routing are made on the network controller, and the data level devices forward the packets based on these decisions. This type of network is vulnerable to DDoS attacks, degrading the overall functioning and performance of the network by continuously injecting the fake flows into it. This increases substantial burden on the controller side, and the result ultimately leads to the inaccessibility of the controller and the lack of network service to the legitimate users. Thus, the protection of this novel network architecture against denial of service attacks is essential. In the world of cybersecurity, attacks and new threats emerge every day. It is essential to have tools capable of managing and analyzing all this new information to detect possible attacks in real-time. These tools should provide a comprehensive solution to automatically detect, predict and prevent abnormalities in the network. Big data encompasses a wide range of studies, but it mainly refers to the massive amounts of structured and unstructured data that organizations deal with on a regular basis. On the other hand, it regards not only the volume of the data; but also that how data-driven information can be used to enhance decision-making processes, security, and the overall efficiency of a business. This paper presents an intelligent big data framework as a solution to handle illegitimate traffic burden on the SDN network created by the numerous DDoS attacks. The framework entails an efficient defence and monitoring mechanism against DDoS attacks by employing the state of the art machine learning techniques.

Keywords : apache spark, apache kafka, big data, DDoS attack, machine learning, SDN network
Conference Title : ICCNC 2021 : International Conference on Computer and Network Communications
Conference Location : Paris, France
Conference Dates : November 18-19, 2021