A New DDoS Detection Method in Software Defined Network

CURRENT STATUS: POSTED

afsaneh banitalebi dehkordi
Islamic Azad University Khorasgan Branch

banitalebi97@gmail.com Corresponding Author

MohammadReza Soltanaghaei
Islamic Azad University Khorasgan Branch

farsad zamani boroujeni
Islamic Azad University Khorasgan Branch

DOI: 10.21203/rs.2.24212/v1

SUBJECT AREAS
Software Engineering

KEYWORDS
Distributed Denial of Service attacks, Software Defined Networks, Network Security, Machine Learning
Abstract
Software Defined Networking (SDN) is a new network architecture in which network control is separated from direct traffic and is programmed directly. Any change in network information and its configuration can be easily implemented in software by using the controller. Although SDN networks with their new structure and controller make way for new and innovative applications for network administrators, but the security challenges and attacks of SDN networks have created problems for these networks. One of these malicious attacks is Distributed Denial of Service (DDoS) attacks. The DDoS attack is aimed at removing machine and network resources from its legitimate users. In this paper, we propose a hybrid method for detecting DDoS attacks in SDN Networks. This method is consisting of statistical and machine learning method. Statistical method calculates the new correlation measure among all features and the dynamic thresholds, then extracts a portion of the data is recognized as attack. This portion is then redirected to the machine learning section to increase the DDoS detection accuracy. The experimental results on UNB-ISCX, CTU-13 and ISOT datasets showed that the proposed method outperforms the existing techniques in terms of the accuracy of detecting DDOS attacks in SDN networks.

Full-text
Due to technical limitations, full-text HTML conversion of this manuscript could not be completed. However, the manuscript can be downloaded and accessed as a PDF.

Figures
SDN Architecture Detailed legend: Fig 1 shows a simple overview of the network architecture, including the SDN controller, the location of the applications running on the controller, and the openflow switches controlled by the controllers through the openflow interface.
Figure 2

Short title of figure: The method presented in this study Detailed legend: Fig. 2 shows the flowchart of the proposed method.
Figure 3

Short title of figure: Comparing the accuracy with different algorithms Detailed legend: The results based on Fig.3 and Table 11 indicated that tree algorithms resulted in better results based on the desired dataset
Figure 4

Short title of figure: Comparing the accuracy of the proposed method to other studies for the UNB-ISCX dataset. Detailed legend: The comparative results are summarized in Fig.4 and Fig.5.
Figure 5

Short title of figure: Comparing the accuracy of the proposed method to other studies for the CTU-13 dataset. Detailed legend: The comparative results are summarized in Fig.4 and Fig.5.