A cooperative DDoS attack detection scheme based on entropy and ensemble learning in SDN

Shanshan Yu

Shandong University

Jicheng Zhang (✉ 17861436995@163.com)

Shandong University <https://orcid.org/0000-0003-4295-2950>

Ju Liu

Shandong University <https://orcid.org/0000-0003-3160-9233>

Xiaoqing Zhang

Shandong University

Yafeng Li

Shandong University

Tianfeng Xu

Shandong University

Research

Keywords: Software Defined Network, Distributed Denial of Service, Edge Switch, Entropy, Ensemble learning

Posted Date: January 29th, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-154522/v1>

License: This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Version of Record: A version of this preprint was published at EURASIP Journal on Wireless Communications and Networking on April 13th, 2021. See the published version at <https://doi.org/10.1186/s13638-021-01957-9>.

Abstract

In order to solve the problem of Distributed Denial of Service (DDoS) attack detection in software defined network (SDN), we proposed a cooperative DDoS attack detection scheme based on entropy and ensemble learning. This method sets up a coarse grained initial detection module based on entropy in the edge switch to monitor the network status in real time and report to the controller if any abnormality is found. Simultaneously, a fine grained precise attack detection module is designed in the controller, and a ensemble learning-based algorithm is utilized to further identify abnormal traffic accurately. In this framework, the idle computing capability of edge switches is fully utilized with the design idea of edge computing to offload part of the detection task from the control plane to the data plane innovatively. Simulation results of two common DDoS attack methods, ICMP and SYN, show that the system can effectively detect DDoS attacks and greatly reduce the southbound communication overhead and the burden of the controller as well as the detection delay of the attacks.

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

Figure 1

System model

Figure 2

Architecture of the DDoS attack detection scheme

Match Field	Priority	Counters	Instructions	Timeouts	Cookie
-------------	----------	----------	--------------	----------	--------

Figure 3

Structure of the flow entry

Figure 4

Flowchart of the preliminary detection module

Figure 5

Architecture of the DDoS attack detection scheme

Figure 6

Preliminary detection result in the edge switch (ICMP). (a): Real-time results of information entropy difference (b): Real-time statistic results of flow entries (c): Detection decision in the edge switch (0 represent normal, 1 represent abnormal)

Figure 7

Flow comparison of attacked port (ICMP)

Figure 8

Preliminary detection result in the edge switch (SYN) (a): Real-time results of information entropy difference (b): Real-time statistic results of flow entries (c): Detection decision in the edge switch (0

represent normal, 1 represent abnormal)

Figure 9

Flow comparison of attacked port (SYN)

Figure 10

CPU utilization of the controller (ICMP)

Figure 11

CPU utilization of the controller (SYN)

Figure 12

CPU utilization of the controller in the larger scale network (Normal traffic state)