A Novel DDoS Attacks Detection Scheme for SDN Environments

I. Introduction

What is SDN?

Software-Defined Networking separates a network's control logic from switches - it decouples the system that makes decisions about where traffic is sent (The Control Plane) from the underlying systems that forward traffic to the selected destination (The Data Plane).

What is OpenFlow?

OpenFlow is a protocol that standardizes how SDN switches communicate with an SDN controller.

What are DDoS attacks?

DDoS attacks are widely used to run out the target's network bandwidth or process resources.

What is the new DDoS attack discussed in the paper?

The new type DDoS attack specifically points at SDN environments. It aims at weak points of SDN, limited storage in switches and limited calculating ability in controller. It brings more impact on switches and controllers and is difficult to be detected by traditional DDoS detection schemes.

What is the detection scheme used in the paper?

The detection scheme is based on separation of the space of traffic measurements into normal and anomalous subspaces, by means of Principal Component Analysis (PCA).

How is the new DDoS attack different from traditional DDoS attacks?

Unlike traditional attacks which send packets to a common target server, the new attack sends packets to random targets. This behavior change makes the new DDoS attack harder to be detected, and bring more impact on SDN environments.

II. Preliminaries

A. PCA on traditional networks

What is PCA?

PCA is a coordinate transformation method that maps the measured data onto a new set of axes, called the principal axes or components; Each principal component points in the direction of maximum variation or energy remaining in the data, given the energy already accounted for in the preceding components. So, the i^{th} principal component captures the total energy of the original data to the maximal residual energy beside former i–1.

Important terms

(a) OD Pair

OD pair denotes a pair of nodes - the origin node and the destination node of one packet.

(b) OD Flow p

The OD flow consists of all traffic for an OD pair. If the network has k entrance, there will be k^2 PoP pairs maximum, and hence k^2 OD pairs. For short, the number of OD flows is set as p.

(c) Number of successive time intervals of interest t

Collect successive network's traffic for a total of (w × t) seconds and separate the time period into t pieces => each time period = w seconds. The number of time periods t can be adjusted to t_1 by adjusting w to w_1, so that

$$t \times w = t_1 \times w_1$$

III. System Statement and Problem Statement

A. SDN Matching Process

Packet matching process in SDN has limited storage spaces and process resources. These resources could be easily run out when DDoS attacks occur in SDN.

For simplicity, consider that there is only one flow table in a switch. An SDN switch depends on flow tables to instruct traffic packets. The switch extracts match fields (such as Ethernet source address or IPv4 destination address) from packets to lookup a match in flow table. A packet can match more than one different entries. In such a case, the flow entry with the highest priority is selected.

When the controller receives a message, it searches its flow table for a match. If there exists a match, the controller will instruct the switch to install a rule in the flow table, so that the switch knows how to handle the packet. If there is no match, the controller sends PACKET-OUT to all connected switches. If one switch gets a match, it will return a message back to the controller. The controller will record the rule in its own flow table and sends instruction to the original switch.

There are two patterns associated with DDoS attacks:

(i) Lot of packets from different sources to one destination

(ii) Starts in short time

According to the matching problem mentioned above, there will be two extra side effects on SDN environments:

(i) Impact on switches

(ii) Impact on controller