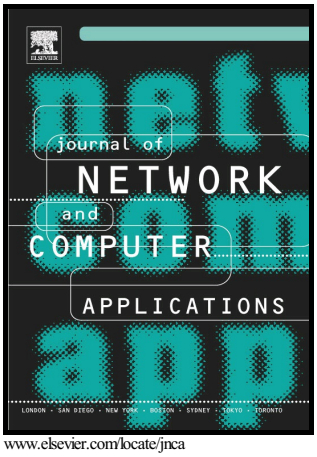
# Distributed-SOM: A Novel Performance Bottleneck Handler for Large-sized Software-Defined Networks under Flooding Attacks

Trung V. Phan, Nguyen Khac Bao, Minho Park




www.elsevier.com/locate/jnca

PII: S1084-8045(17)30164-9
DOI: http://dx.doi.org/10.1016/j.jnca.2017.04.016
Reference: YJNCA1913

To appear in: *Journal of Network and Computer Applications*

Received date: 2 May 2016
Revised date: 22 March 2017
Accepted date: 27 April 2017

Cite this article as: Trung V. Phan, Nguyen Khac Bao and Minho Park, Distributed-SOM: A Novel Performance Bottleneck Handler for Large-sized Software-Defined Networks under Flooding Attacks, *Journal of Network and Computer Applications,* http://dx.doi.org/10.1016/j.jnca.2017.04.016

# Distributed-SOM: A Novel Performance Bottleneck Handler for Large-sized Software-Defined Networks under Flooding Attacks

Trung V. Phan, Nguyen Khac Bao, Minho Park*

*Department of ICMC Convergence Technology, Soongsil University*
*Seoul 156-743, Korea*

**Abstract**

Software-Defined Networking (SDN) is a new programmable networking model that features the detachment of control and data planes. In this network, the network brain is an SDN controller that is used to centrally monitor and control the data plane based on the OpenFlow protocol and applications located in the application layer. In recent years, a vast number of issues relating to security have been seriously debated for this networking paradigm, especially the large-scale model. In particular, flooding attacks have been on the rise, providing great challenges for the SDN architecture to cope with. In this paper, we present a novel mechanism using the Self-Organizing Map (SOM) application to solve the performance bottleneck and overload problems for the upper layers in a large-sized SDN in case of flooding attacks. Our proposed approach integrates a Distributed Self-Organizing Map (DSOM) system to OpenFlow Switches instead of using a standalone SOM. By exploiting SDN advantages, such as flexibility and overhead reduction, we implement and test both a DSOM system and a single SOM system on multi-criteria to compare the performance of our introduced system. Our experimental results show that the DSOM solution can effectively detect abnormal traffic, solve bottleneck problems and increase the system reaction speed to attack traffic, while presenting a smaller overhead to the network system.

*Keywords:* Flooding Attacks, Distributed Denial-of-Service, Self-Organizing Map, Software-Defined Networks



## 1. Introduction

Software-Defined Networking (SDN) [1] has recently been recognized as providing an outstanding network architecture. In this network model, the separation of the control and data planes brings about enormous benefits for network operators in traffic management. OpenFlow protocol [2] is a major component in the SDN paradigm, and it operates as a communicator between the control and data planes (an SDN controller and OpenFlow switches). The SDN controller uses the OpenFlow protocol to configure and update flow-tables inside OpenFlow switches according to network service instructions such as security and routing policies.

### 1.1. Problem Statement

SDN promises a foreseeable solution for a wide range of services and applications in network configuration and management. The SDN technology has been deployed in large-sized networks [4] to manage internal traffic by running network services and applications. However, these networks are facing with following common problems.

In a large-sized network where there are a higher number of OpenFlow switches, the SDN controller naturally becomes a performance bottleneck because of the resource allocation for security services and applications. In particular, security applications always require advanced processing and analyses to operate their functionalities in the network. For example, Figure 1 shows that two upper planes usually consist of three modules of *Stats Collector*, *Security Application* and *Policy Enforcement* to launch just a security service, and there is also

*Corresponding author
*Email addresses:* trungpv@ssu.ac.kr (Trung V. Phan), khacbao@ssu.ac.kr (Nguyen Khac Bao), mhp@ssu.ac.kr (Minho Park)