Ain Shams University

Faculty of Engineering

Computer and Systems Engineering Department

Data Inspection in SDN Networks

by

Soliman Abd Elmonsef Soliman Sarhan
B.Sc. Computer and Systems Engineering
Military Technical college, 2012

A THESIS
SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN ELECTRICAL ENGINEERING
Computer and Systems Engineering Department

Supervised By
Prof. Ayman Mohamed Bahaa-Eldin

Prof. Mohamed Ali Sobh

Cairo, Egypt

August, 2019

Faculty of Engineering
Computer and Systems
Engineering Department

Examiners Committee

Name	**Soliman Abd Elmonsef Soliman Sarhan**
Thesis	**Data Inspection in SDN network**
Degree	**Master of Science**

Signature

- Prof. Iman Ali Saroit Ismail
Professor and Dean of the Faculty of Computers and
Artificial Intelligence
Cairo University

- Prof. Ayman Mohamed Wahba
Professor of Computer & Systems Engineering
Ain Shams University

Prof. Ayman Mohamed Bahaa-Eldin
Professor of Computer & Systems Engineering
Ain Shams University (A Supervisor)

Prof. Mohamed Ali Sobh
Associate Professor of Computer & Systems Engineering
Ain Shams University (A Supervisor)

Abstract

Soliman Abd Elmonsef Soliman Sarhan

Data Inspection in SDN Networks

Master of Science Dissertation

Ain Shams University, 2019

Software-Defined Networks can be considered as the most important development in Computer Networking in the last decade. Deep Packet Inspection (DPI) technology significantly enhances the security and management of current networks, combined with software-defined networking (SDN), DPI becomes an even more powerful tool that can centralize network strategy control and quick automation.

The conversion from the traditional networks to the SDN network has significant challenges that need a careful examination. In this thesis we focus on Improved DPI that can give the exhaustive data to notify the SDN controller about the situation of the network and its activity streams of traffic flows. This enables SDN to regard the network as a comprehensive asset as opposed to a different collection of devices (e.g. switches, security, and other Layer 4-7 elements). Ultimately, connecting SDN and DPI will let network pros apply policy control and automation to the whole network as opposed to individual components or elements.

Leveraging a central DPI capability will give knowledge and intelligence to every important function (security, controller, policy, etc.), instead of the current system of each functional box performing its own DPI.

So, it became a must to inspect the data in SDN architecture that fit the benefits of central control.

Keywords:

Deep Packet Inspection, Software defined networks, Open Flow Protocol, Dpi Controller, DPI Instances, and Traffic Engineering

Statement

This dissertation is submitted to Ain Shams University for the degree of Master of Science in Electrical Engineering

The work included in this thesis was out by the author at Computer and Systems Engineering, Ain Shams University.

No part of this thesis has been submitted for a degree or qualification at other university or institution.

Date : / /2019

Signature :

Name : Soliman Abd Elmonsef Soliman Sarhan

Acknowledgements

I am very thankful to Professor Ayman Bahaa for his continuous support during my work to complete this thesis. I was highly affected by his high standards of conducting research, creative ideas and his passion to discover new research opportunities.

I am very thankful to Professor. Mohamed Sobh for his support and helpful suggestions during the thesis.

I am deeply tankful and grateful to my parents for their continuous encouragement, help and support to complete this journey to obtain my Master's degree.

Finally, I am very thankful to my wife for her continuous support, encouragement and patience to complete this thesis.

Table of Contents

List of Figures

List of Tables

List of ABBREVIATIONS

API	pplication Programming Interface
DDoS	Distributed Denial of Service
DFA	Deterministic Finite Automata
DPI	Deep Packet Inspection
IDS	Intrusion Detection System
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISP	Internet Service Provider
MPLS	Multi-Protocol Label Switching
NDPI	Ntop Deep Packet Inspection
NFA	Nondeterministic Finite Automata
PCE	Path Computing Element
QoS	Quality of Service
SDN	Software Defined-Networking
SNMP	Simple network management protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
TSA	Traffic Steering Application

Chapter 1

Introduction

We need a new architecture to efficiently implement Deep Packet Inspection (DPI) in Software Defined-Networking (SDN) because of the importance of DPI. Functions will be added to SDN to help and enable us to have a good solution to solve SDN Challenges like monitoring, latency, security, etc. Let us start with the limitation of the existing network that we have today. This chapter is divided into six sections. The first section describes the limitations of the legacy networks. Section 2 shows software-defined networks and describes how they are the best solution to switch off the legacy network, as well as the challenges facing SDN such as traffic management, security, analysis, and duplication. Section 3 shows DPI and describes its role in SDN, and how it can solve the SDN challenges. Section 4 illustrates the challenges faced DPI when implementing It in SDN layers. Section 5 describes the contribution of this thesis. Section 6 shows the organization of this thesis.

1.1 Limitations of Legacy IP Networks

The limit of the present internet is getting to be inadequate to meet the massive volumes of traffic types conveyed by the modern services (e.g., cell

phones and content, big data systems, server virtualization functions, and cloud and accounting services), which are produced because of the huge number of clients, sensors, and applications [1,2].

Legacy networks constructed with numerous layers of static Ethernet switches orchestrated in a tree model are currently unsuitable for the dynamic processing and capacity of storage needs. Rather, a new networking establishment is required to give aloft effectiveness, reliability, and power efficiency.

Also, they ought to enhance the network speedup, scalability and submission of a lot of digital services that ensure the quality of service. The implementation of these demands is impossible with the currently available network hardware because of their limited capabilities.

What's more, to actualize policies on a large-scale network and provide new services or support existing services, administrators today need to set the configuration to a huge number of network equipment and protocols. It is hard to achieve a reliable arrangement of security, QoS, and different policies. Networks turn out to be more perplexing with the expansion of thousands of hardware that must be overseen and configured. Also, integration to network appliances is very hard because of the internals contrast from a vendor to another. According to legacy network issues and limitation, we mentioned that we need a new architecture to fit all cases and face the huge increase in traffic, SDN is the best solution to perform this role.

1.2 Software Defined Networking

1.2.1 SDN is the suitable solution to switch off legacy networks

The main principle is separation where the control layer is decoupled from the data layer. SDN [3,4] is a modern methodology for network programmability, which gives the capability to manage and control network behavior through programming. The SDN structure empowers centralized control of data path autonomously from the technique used to link these network equipment which can be sourced from various vendors.

The central control device establishes all the information and keeps up a wide network perspective of the data path components and connections that link them. Figure 1.1 [25] shows the architecture difference between SDNs and traditional IP networks.

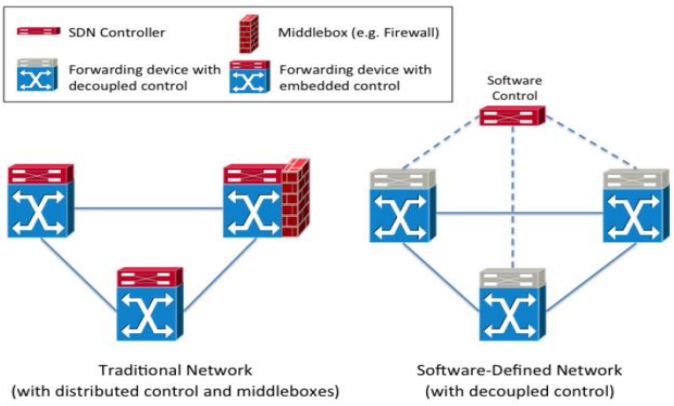

Figure 1.1 Architecture Difference between Traditional IP networks and Software-Defined Network