

Early Classification of Network Traffic for Software-Defined Network Management



1

Introduction

Motivation

- ❑ The paradigm of Software-Defined Networking (SDN) is increasingly gaining attention as a technology for the future networks
- ❑ OpenFlow has evolved to become today's main enabler of SDN
- ❑ Due to the increasing interest of OpenFlow, the major vendors of network devices have incorporated OpenFlow support into their switches and routers
- ❑ Traffic classification is crucial for network management tasks, such as traffic engineering or capacity planning

Objectives

- ✓ Early classification of traffic as elastic / inelastic in SDN networks
- ✓ Use OpenFlow protocol for network management
- ✓ Use only first few packets of each flow (TCP or UDP) for classification
- ✓ Automatic reconfiguration of the OpenFlow devices
- ✓ Low computational and bandwidth overhead
- ✓ Highly scalable system

2

Methodology

Combination of flow-level and packet-level data as input for traffic classification with OpenFlow

Packet-level input

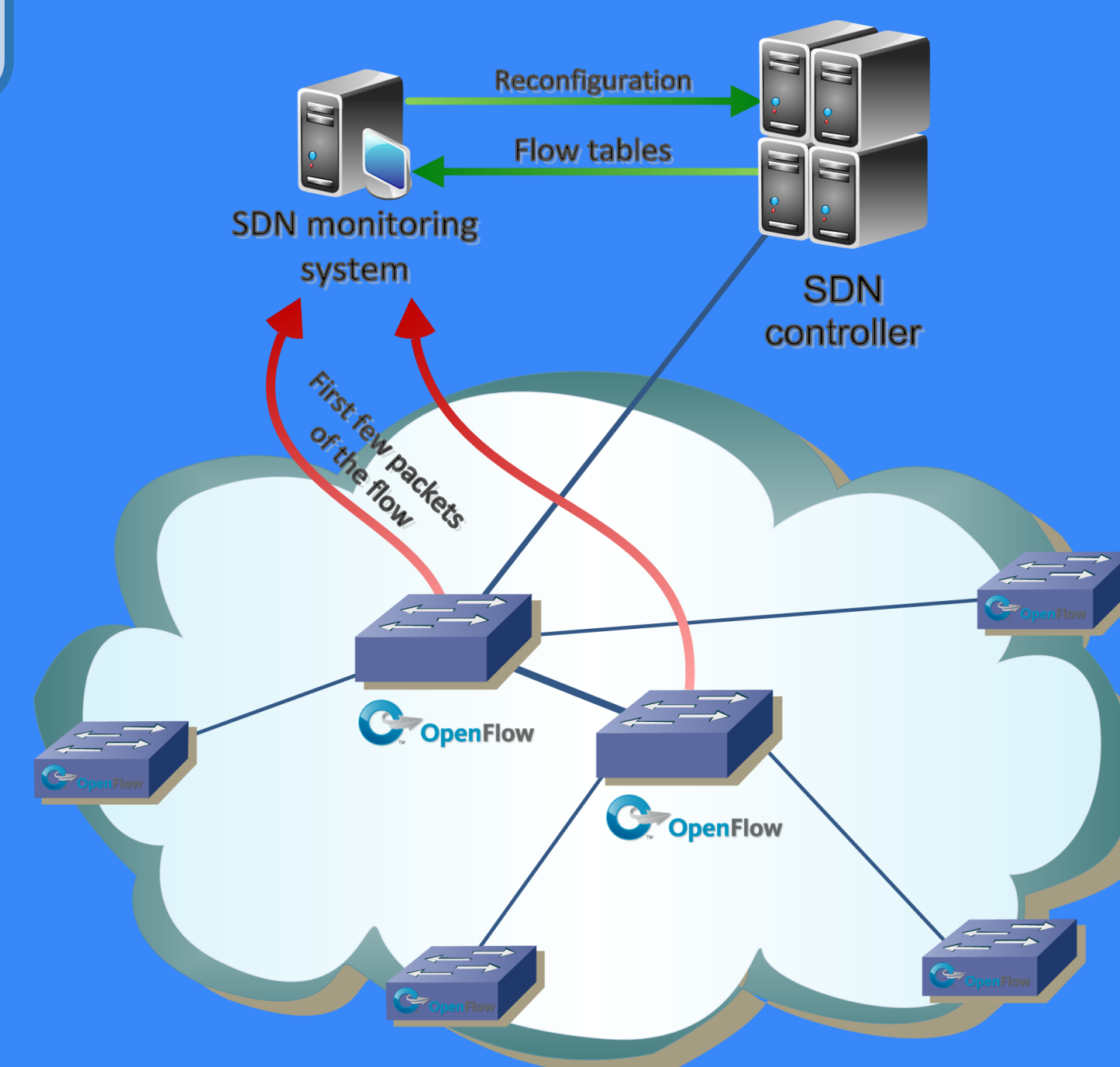
- Early classification
 - UDP → first one or two packets of the flow
 - TCP → first five packets of the flow
- Retraining system. Combined DPI techniques (e. g. PACE, OpenDPI, L7-Filter) as an automatic ground-truth generator
- High resources consumption

Flow-level input

- Unidirectional flows are identified by a 5-tuple (source and destination IP, source and destination ports, protocol)
- Combined classification techniques
 - IP-based
 - Service-based
 - Host-behavior-based
 - Machine learning-based (e. g. c4.5 or C5.0 decision trees)
 - ...
- Flow-level as a complement of packet-level techniques
- Lightweight but slower classification

3

Proposed system



1

The SDN monitoring system collects first few packets of each flow (TCP or UDP) with OpenFlow

2

Early classification of elastic and inelastic traffic and generation of a ground-truth for other techniques as machine learning-based ones

3

The SDN monitoring system checks the flow tables of the OpenFlow devices and reconfigures the SDN controller (e.g. to prioritize inelastic traffic)