Hierarchical Policies for Software Defined Networks

Andrew Ferguson, Arjun Guha, Chen Liang, Rodrigo Fonseca, and Shriram Krishnamurthi
Participatory Networking
TCP Nice: A Mechanism for Background Transfers
Arun Venkataramani Ravi Kokkala Mike Dahlin

Laboratory of Advanced Systems Research
Department of Computer Science
University of Texas at Austin, Austin, TX 78712
{arun, kskokkala, mcd}@cs.utexas.edu

Abstract
Many distributed applications can make use of large background transfers — transfers of data that humans are not waiting for to improve availability, reliability, latency or consistence. However, given the rapid fluctuation of available network bandwidth and changing resource costs due to technology trends, handling the aggressiveness of background transfers (i) simplifying applications, (ii) having two aggressively and mutually dependent flows, and (iii) not granting the benefits of background transfers. Our goal is for the operating system to manage network resources in order to provide a simple abstraction of near-zero-cost background transfers. Our system, TCP Nice, can provably bound the interference inflicted by background flows on foreground flows in a centralized network model. And we use microbenchmarks and case study applications suggest that in practice it interfere little with foreground flows, requires a large fraction of space network bandwidth, and simplifies application conversation and deployment.

1 Introduction
Many distributed applications can make use of large background transfers — transfers of data that humans are not waiting for to improve availability, reliability, latency or consistence. However, given the rapid fluctuation of available network bandwidth and changing resource costs due to technology trends, handling the aggressiveness of background transfers (i) simplifying applications, (ii) having two aggressively and mutually dependent flows, and (iii) not granting the benefits of background transfers. Our goal is for the operating system to manage network resources in order to provide a simple abstraction of near-zero-cost background transfers. Our system, TCP Nice, can provably bound the interference inflicted by background flows on foreground flows in a centralized network model. And we use microbenchmarks and case study applications suggest that in practice it interfere little with foreground flows, requires a large fraction of space network bandwidth, and simplifies application conversation and deployment.
Participatory Networking
Occupy Everything

#OccupyWallSt

We already know that we own everything—The task is to exclude the intrusions of capital and power.
Participatory Networking

Safe?  Secure?  Fair?
Loop freedom?  Black holes?
Participatory Networking

1. semantics + protocol (Hot-ICE ’12)
Participatory Networking

1. semantics + protocol (Hot-ICE ’12)

2. implementation (this talk)
Participatory Networking

1. semantics + protocol (Hot-ICE ’12)
2. implementation (this talk)  PANE
Hierarchical Flow Tables
Hierarchy of Privileges
Hierarchy of Policies
Hierarchy of Policies

(dstPort = 22, Deny)

(dstIP=10.0.0.2, GMB=30)

(dstPort=80, GMB=10)

(srcIP=10.0.0.1, Allow)
Hierarchy of Policies

Packet:
src 10.0.0.1
dst 10.0.0.2:80
Hierarchical Flow Table

Packet:  
src 10.0.0.1  
dst 10.0.0.2:80
Hierarchical Flow Table

Packet:
src 10.0.0.1
dst 10.0.0.2:80

_instruction_(dstPort = 22, Deny)_

_instruction_(dstIP=10.0.0.2, GMB=30)_

_instruction_(dstPort=80, GMB=10)_

_instruction_(srcIP=10.0.0.1, Allow)_
Hierarchical Flow Table
Hierarchical Flow Table
Hierarchical Flow Table

Packet:
src 10.0.0.1
dst 10.0.0.2:80

(dstPort = 22, Deny)
(dstIP=10.0.0.2, GMB=30)
(dstPort=80, GMB=10)
(srcIP=10.0.0.1, Allow)

GMB=10

+)P

Allow
Hierarchical Flow Table

Packet:
src 10.0.0.1
dst 10.0.0.2:80
GMB=10
Allow

Packet:
src 10.0.0.1
dst 10.0.0.2:80
GMB=10

(dstPort = 22, Deny)
(dstIP = 10.0.0.2, GMB = 30)
(dstPort = 80, GMB = 10)
(srcIP = 10.0.0.1, Allow)
Hierarchical Flow Table

Packet:
src 10.0.0.1
dst 10.0.0.2:80

(dstIP = 10.0.0.2, GMB = 30)
(dstPort = 22, Deny)
(srcIP = 10.0.0.1, Allow)
(dstPort = 80, GMB = 10)
Hierarchical Flow Table
Hierarchical Flow Table
Only Requirements: Associative, 0-identity

Hierarchical Flow Table
In node

Sibling

D and S identical.
Deny overrides Allow.
GMB combines as max

Parent-Sibling

Child overrides Parent for Access Control
GMB combines as max

PANE’s HFT Operators
PANE
(dstPort = 22, Deny)

(dstIP=10.0.0.2, GMB=30)

(dstPort=80, GMB=10)

(srcIP=10.0.0.1, Allow)
(dstPort = 22, Deny)

(dstIP=10.0.0.2, GMB=30)

(dstPort=80, GMB=10)

(srcIP=10.0.0.1, Allow)

OpenFlow
PANE
PANE

Policy Tree

Share Tree

Network Flow Table

Linearization

PANE user requests

OpenFlow Controller

OpenFlow messages

Switches
PANE

Policy Tree

Share Tree

Linearization

Network Flow Table

Forwarding & Queue Configuration

Network Information Base (NIB)

Valid Configuration

OpenFlow Controller

OpenFlow messages

Switches
PANE
PANE

- Policy Tree
- Share Tree
- Network Flow Table
- Forwarding & Queue Configuration
- Network Information Base (NIB)
- OpenFlow Controller

Linearization

Valid Configuration

OpenFlow messages

Switches

PANE user requests
PANE

Policy Tree

Network Flow Table

Forwarding & Queue Configuration

Network Information Base (NIB)

Share Tree

PANE user requests

Linearization

Valid Configuration

OpenFlow Controller

OpenFlow messages

Switches
PANE

Policy Tree

Share Tree

Network Flow Table

Forwarding & Queue Configuration

Network Information Base (NIB)

OpenFlow Controller

Linearization

Valid Configuration

OpenFlow messages

Switches
PANE

Policy Tree

Share Tree

Network Flow Table

Forwarding & Queue Configuration

Network Information Base (NIB)

OpenFlow Controller

Switches

Linearization

Valid Configuration

PANE user requests

OpenFlow messages
Proof of Correctness
Packet:
src 10.0.0.1
dst 10.0.0.2:80

(dstPort = 22, Deny)
(dstPort = 80, GMB = 10)
(srcIP = 10.0.0.1, Allow)
(dstIP = 10.0.0.2, GMB = 30)

GMB = 30
GMB = 10

Hierarchical Flow Tables
Compiler Correctness
Compiler Correctness
Compiler Correctness
Packet:
src 10.0.0.1
dst 10.0.0.2:80

Theorem
Packet:
src 10.0.0.1
dst 10.0.0.2:80

Theorem
Packet:
src 10.0.0.1
dst 10.0.0.2:80

GMB 30

Theorem
Packet:
src 10.0.0.1
dst 10.0.0.2:80

compile

GMB 30

Theorem
Theorem

Packet:
src 10.0.0.1
dst 10.0.0.2:80

GMB 30
Current Status
1. working controller
1. working controller
2. client libraries
1. working controller
2. client libraries
3. pane.cs.brown.edu
1. working controller
2. client libraries
3. pane.cs.brown.edu
4. github.com/brownsys/pane
Questions?

Andrew Ferguson
adf@cs.brown.edu
Co-authors

• Arjun Guha
• Chen Liang
• Rodrigo Fonseca
• Shriram Krishnamurthi

Questions?

Andrew Ferguson
adf@cs.brown.edu
Backup Slides