Hierarchical Policies for Software Defined Networks

Andrew Ferguson, Arjun Guha, Chen Liang, Rodrigo Fonseca, and Shriram Krishnamurthi
Participatory Networking
TCPNice: A Mechanism for Background Transfers

Arun Venkataramani

Abstract

TCPNice is a mechanism for improving the performance of background transfers over TCP by making use of idle connections. The mechanism is implemented in the Linux kernel and is activated by a new kernel module. The module dynamically decides when to activate the mechanism, based on the state of the network and the availability of idle connections. The mechanism has been tested on a variety of networks and has been shown to improve performance by up to 50% in some cases.

1 Introduction

TCP is a connection-oriented protocol that provides reliable, ordered, and flow-controlled delivery of data over a network. It is the most widely used protocol for internet communication. TCP is used to transport data over the internet, including web pages, email, and other applications. However, TCP is not optimized for background transfers, which are transfers that do not require user interaction.

Arjun Venkataramani

September 2013

Send comments to arun@cs.washington.edu
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
Barack Obama

David Plouffe

Correspondence
Field
Policy
Operations...
Communications
New Media
Paid Media
Finance
Marketing
Email
Blog
Analytics
Design
Video
Organizing
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

Hierarchy of Policies:

1. (dstPort = 22, Deny)
   - (dstIP=10.0.0.2, GMB=30)
     - (dstPort=80, GMB=10)
       - (srcIP=10.0.0.1, Allow)
<table>
<thead>
<tr>
<th>Rule Description</th>
<th>Flow Table Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>(dstPort = 22, Deny)</td>
<td></td>
</tr>
<tr>
<td>(dstIP=10.0.0.2, GMB=30)</td>
<td></td>
</tr>
<tr>
<td>(dstPort=80, GMB=10)</td>
<td>(srcIP=10.0.0.1, Allow)</td>
</tr>
</tbody>
</table>

Packet:
src 10.0.0.1
dst 10.0.0.2:80

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)
Hierarchical Flow Table

Packet:
src 10.0.0.1
dst 10.0.0.2:80

Allow

GMB=10

(srcIP=10.0.0.1, Allow)

(dstPort=80, GMB=10)

(dstIP=10.0.0.2, GMB=30)

(dstPort = 22, Deny)
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
+ S
Allow

(dstIP=10.0.0.2, GMB=30)
Hierarchical Flow Table

Packet:
src 10.0.0.1
dst 10.0.0.2:80

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

(dstPort = 22, Deny)
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

GMB = 10

Allow
Hierarchical Flow Table
Hierarchical Flow Table
Hierarchical Flow Table
Hierarchical Flow Table

Only Requirements: Associative, 0-identity
PANE’s HFT Operators

In node

Sibling

Parent-Sibling

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

Child overrides Parent for Access Control GMB combines as max
Implementation
(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)
PANE

Policy Tree

Share Tree

PANE user requests

OpenFlow Controller

OpenFlow messages

Switches
PANE

Policy Tree

Share Tree

Network Flow Table

Linearization

PANE user requests

OpenFlow Controller

OpenFlow messages

Switches
PANE

Policy Tree

Share Tree

Network Flow Table

Forwarding & Queue Configuration

Network Information Base (NIB)

OpenFlow Controller

Valid Configuration

Linearization

PANE user requests

OpenFlow messages

Switches
PANE
PANE

5Mbps
8Mbps
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

Share Tree

Network Flow Table

Forwarding & Queue Configuration

Network Information Base (NIB)

Linearization

Valid Configuration

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 user requests
Proof of Correctness
Hierarchical Flow Tables

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=30
GMB=10
GMB=10
GMB=30

+P

Allow
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

GMB 30

Theorem
Packet:
src 10.0.0.1
dst 10.0.0.2:80

Theorem
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
Questions?

Andrew Ferguson
adf@cs.brown.edu

Co-authors

- Arjun Guha
- Chen Liang
- Rodrigo Fonseca
- Shriram Krishnamurthi
Backup Slides