Traffic Engineering and QoS Differentiation to Handle Malicious Network Flows

Joaquin Garcia-Alfaro

Institut Mines-Telecom, Telecom SudParis

Joint work with

Hervé Debar and Nabil Hachem

Motivation

- Adaptive mitigation solution using MPLS to handle network attacks

- **How?**
  - Affecting labels to suspicious packets based on information received from detection engines
  - Implementing traffic engineering and QoS functions

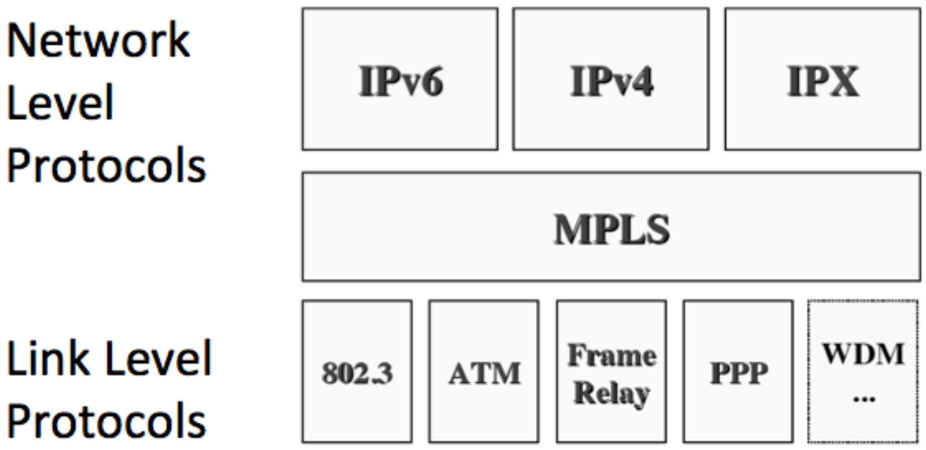
- **Why MPLS?**
  - Widely used by network operators and service providers
  - Effectively separates traffic in multiple classes
  - De-facto standard practice for traffic engineering & QoS
  - Potentially interoperable (VLANs & operators)

[IPCCC, 2012] N. Hachem, H. Debar, and J. Garcia-Alfaro. HADEGA: A Novel MPLS-based Mitigation Solution to Handle Network Attacks, 31st IEEE International Performance Computing and Communications Conference (IPCCC 2012). Austin, Texas, December, 2012.

Outline

- Motivation
- Background on MPLS
- MPLS-based mitigation
- Conclusion & Perspectives

MPLS: MultiProtocol Label Switching



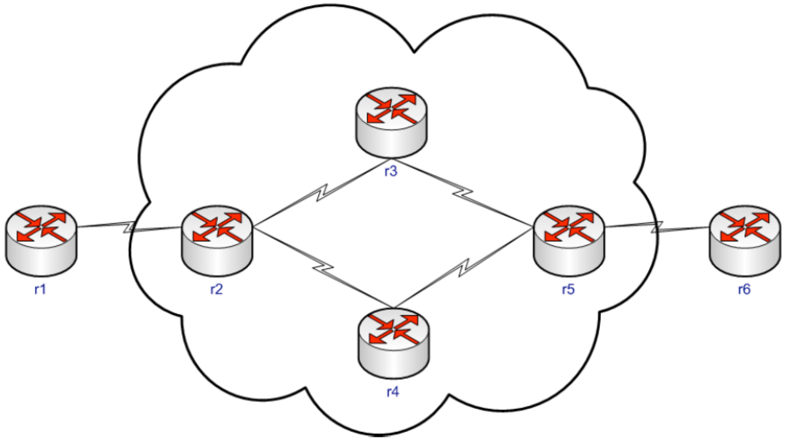
Network Level Protocols

IPv6 IPv4 IPX

MPLS

Link Level Protocols

802.3 ATM Frame Relay PPP WDM ...



- IP routing + packet switching
  - Every packet entering the cloud is assigned a traffic class and gets labeled
  - Packets with same class ID get processed in the same way
    - same virtual link (*path*), same QoS parameters, ...
  - Transit nodes just look at the label to decide the next hop

Vocabulary & definitions

- *MP* for MultiProtocol (IPv4 + 802.3, IPv6 + ATM, ...)

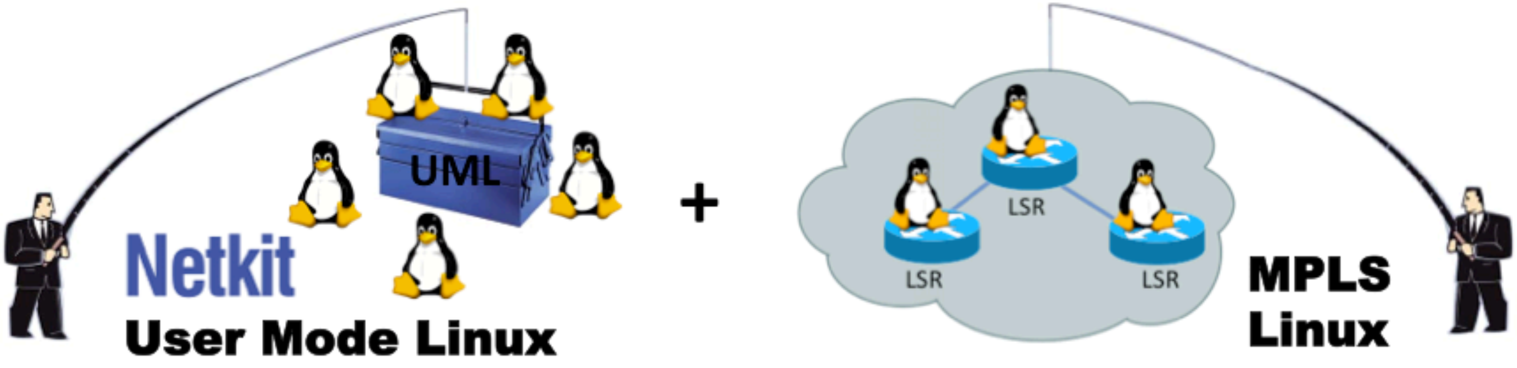
- Label
  - Short integer, locally assigned to a FEC between two LSRs

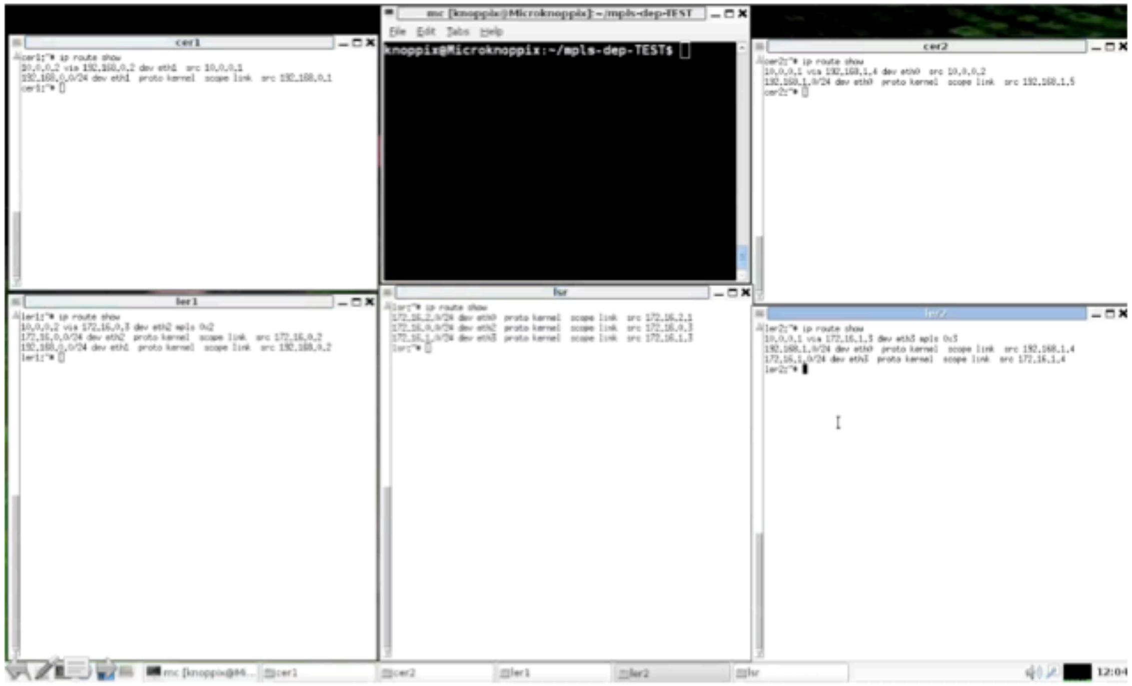
- FEC (*Forward Equivalence Class*)
  - Identifies a traffic flow (set of IP datagrams) that shall traverse the MPLS network using the same path

- LSR (*Label Switch Router*)
  - MPLS router, in charge of handling routing & switching tables and forward labeled IP packets

- LSP (*Label Switched Path*)
  - End-to-end path through an MPLS network, in which all the IP datagrams are equally treated (e.g., in terms of QoS)
    - Set up by a signaling protocol (e.g., LDP, RSVP-TE, BGP, ...)

"… how I learned to stop worrying and love the MPLS technology"





cer1

```
cer1:~# ip route show
10.0.0.2 via 192.168.0.2 dev eth1  src 10.0.0.1
192.168.0.0/24 dev eth1  proto kernel  scope link  src 192.168.0.1
cer1:~# 
```

```
knoppix@Microknoppix:~/mpls-dep-TEST$ 
```

cer2

```
cer2:~# ip route show
10.0.0.1 via 192.168.1.4 dev eth0  src 10.0.0.2
192.168.1.0/24 dev eth0  proto kernel  scope link  src 192.168.1.5
cer2:~# 
```

ler1

```
ler1:~# ip route show
10.0.0.2 via 172.16.0.3 dev eth2 mpls 0x2
172.16.0.0/24 dev eth2  proto kernel  scope link  src 172.16.0.2
192.168.0.0/24 dev eth1  proto kernel  scope link  src 192.168.0.2
ler1:~# 
```

lsr

```
lsr:~# ip route show
172.16.2.0/24 dev eth0  proto kernel  scope link  src 172.16.2.1
172.16.0.0/24 dev eth2  proto kernel  scope link  src 172.16.0.3
172.16.1.0/24 dev eth3  proto kernel  scope link  src 172.16.1.3
lsr:~# 
```

ler2

```
ler2:~# ip route show
10.0.0.1 via 172.16.1.3 dev eth3 mpls 0x3
192.168.1.0/24 dev eth0  proto kernel  scope link  src 192.168.1.4
172.16.1.0/24 dev eth3  proto kernel  scope link  src 172.16.1.4
ler2:~# 
```

Outline

- Motivation
- Background on MPLS
- MPLS-based mitigation
- Conclusion & Perspectives

MPLS-based mitigation

- Affect labels to suspicious packets based on information received from defense equipment (e.g., IDSs, IPSs, ...)
  - Alert Information
    - Network attributes (e.g., source, destination, ports, etc.)
    - Assessment attributes (e.g., Impact Level and Confidence Level)
- Implement TE and Diffserv for suspicious flows to, e.g.,
  - Nullroute or delay those flows
  - Optimize services only for legitimate traffic
- Requirements
  - Ability to map labels to a given mitigation strategy

[IPCCC, 2012] N. Hachem, H. Debar, and J. Garcia-Alfaro. HADEGA: A Novel MPLS-based Mitigation Solution to Handle Network Attacks, 31st IEEE International Performance Computing and Communications Conference (IPCCC 2012). Austin, Texas, December, 2012.

Mitigation strategies

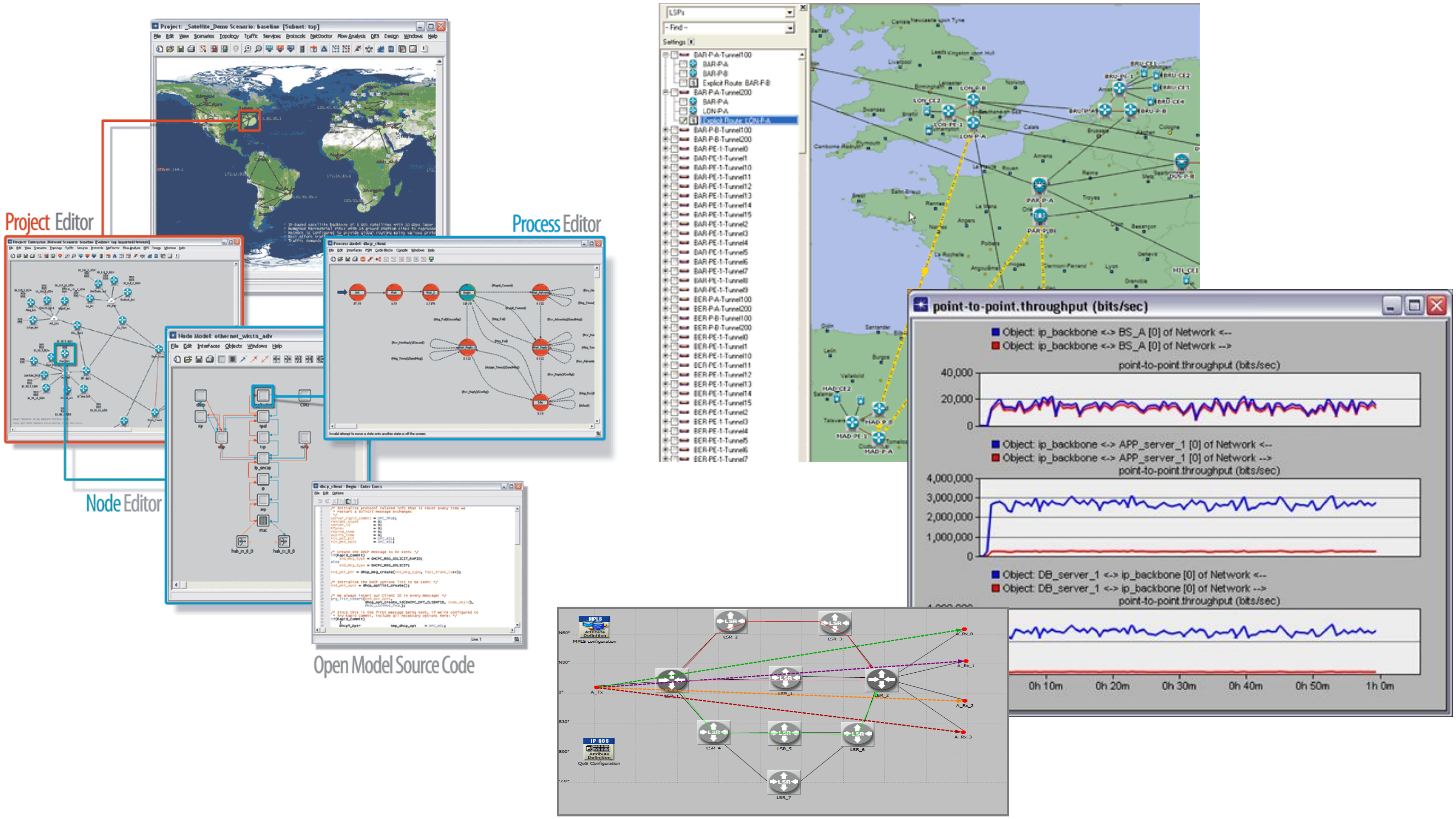
- TE Mitigation:
  - dynamic construction of end-to-end paths with reduced QoS
  - paths built upon attributes such as Bandwidth, # of Hops, Link Quality, priority, ...
  - differentiation of treatment mainly decided by the edge routers

- PHB Mitigation:
  - differentiation of treatment as per-hop relaying at intermediate routers
  - queuing and scheduling priority assigned to every packet w.r.t. its behavior

- TE+PHB Mitigation:
  - combination of both previous approaches (end-to-end & per-hop)
  - adaptation of initial paths defined (end-to-end) but treatment by intermediate routers

[IPCCC, 2012] N. Hachem, H. Debar, and J. Garcia-Alfaro. HADEGA: A Novel MPLS-based Mitigation Solution to Handle Network Attacks, 31st IEEE International Performance Computing and Communications Conference (IPCCC 2012). Austin, Texas, December, 2012.

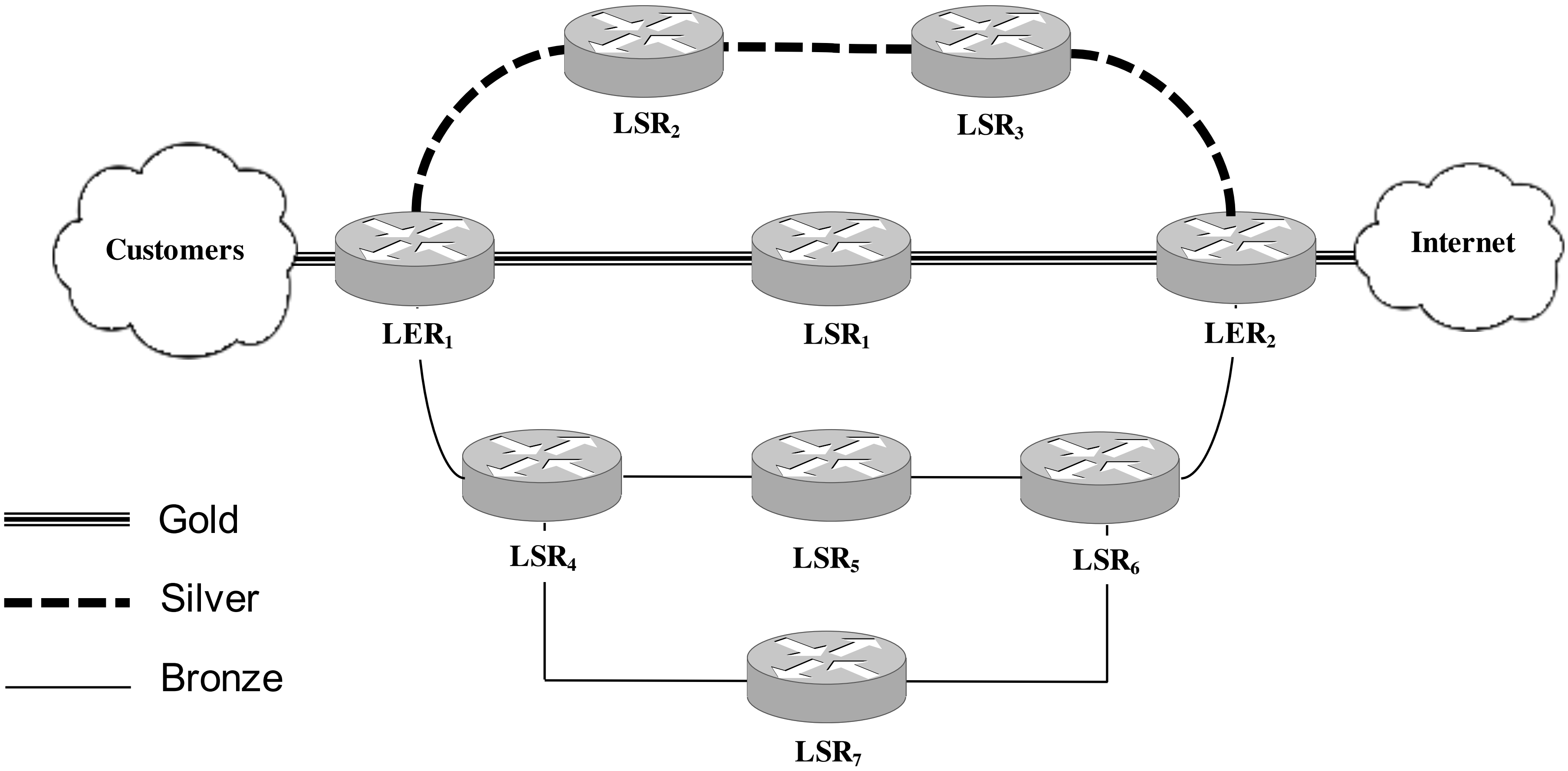
OPNET Modeler experiments


Project Editor
Process Editor
Node Editor
Open Model Source Code
point-to-point.throughput (bits/sec)
Object: ip_backbone <-> BS_A [0] of Network <--
Object: ip_backbone <-> BS_A [0] of Network -->
point-to-point throughput (bits/sec)
40,000
20,000
0
Object: ip_backbone <-> APP_server_1 [0] of Network <--
Object: ip_backbone <-> APP_server_1 [0] of Network -->
point-to-point throughput (bits/sec)
4,000,000
3,000,000
2,000,000
1,000,000
0
Object: DB_server_1 <-> ip_backbone [0] of Network <--
Object: DB_server_1 <-> ip_backbone [0] of Network -->
point-to-point throughput (bits/sec)
0h 10m
0h 20m
0h 30m
0h 40m
0h 50m
1h 0m
LSR_1
LSR_2
LSR_3
LSR_4
LSR_5
LSR_6
LSR_7
MPLS configuration
QoS Configuration
LON-P-A
LON-P-B
PAR-P-A
PAR-P-B
BRU-P-A
BRU-P-B
HAD-P-A
HAD-P-B

[IPCCC, 2012] N. Hachem, H. Debar, and J. Garcia-Alfaro. HADEGA: A Novel MPLS-based Mitigation Solution to Handle Network Attacks, 31st IEEE International Performance Computing and Communications Conference (IPCCC 2012). Austin, Texas, December, 2012.

Topology

- All routers capacity similarly configured & different QoS paths:
  - Gold: path having 155Mbps capacity and 2 hops
  - Silver: path with 45Mbps capacity & 3 hops
  - Bronze: remaining paths



Network traffic

- Traffic flows

Class	Description	%
L	Legitimate flows	67.80%
S1	False positive flows & suspected spam mails	7.53 %
S2	Suspected botnet channels & port scanning	10.87 %
S3	Suspected DDoS & worm spreading flows	13.80 %

- Traffic intensity phases

Phase	Load	Description
1	61.75 %	Core network unstable (Critical phases)
2	73.50 %	
3	85.75 %	
4	98.00 %	
5	110.25 %	Great instability (Saturation phases)
6	122.00 %	

Network traffic

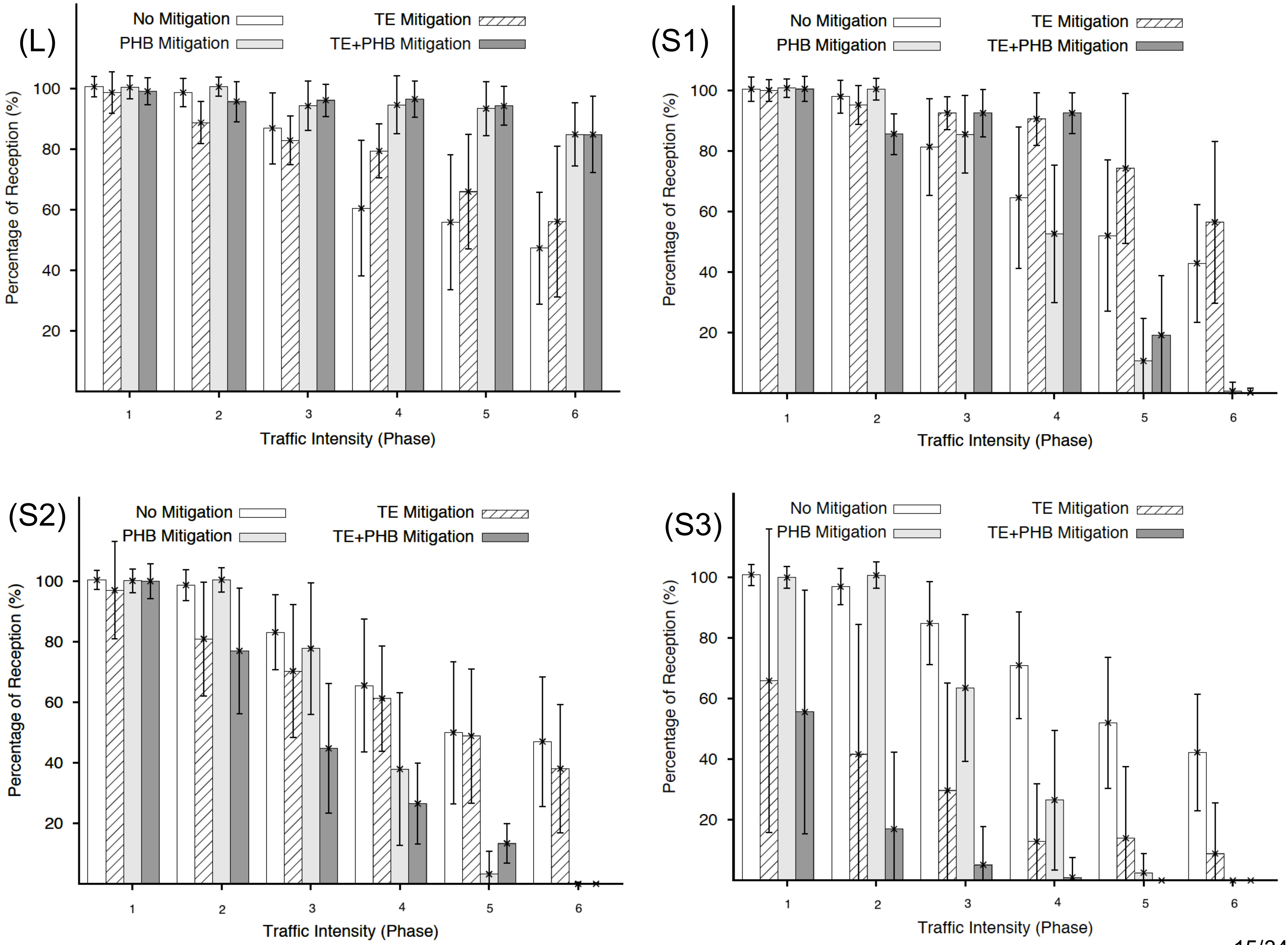
- Traffic flows

Class	Description	%
L	Legitimate flows	67.80%
S1	False positive flows & suspected spam mails	7.53 %
S2	Suspected botnet channels & port scanning	10.87 %
S3	Suspected DDoS & worm spreading flows	13.80 %

Impact level	Confidence level	Class
Low	Low	S1
Low	Medium	S2
Low	High	S2
Medium	Low	S1
Medium	Medium	S2
Medium	High	S3
High	Low	S2
High	Medium	S3
High	High	S3

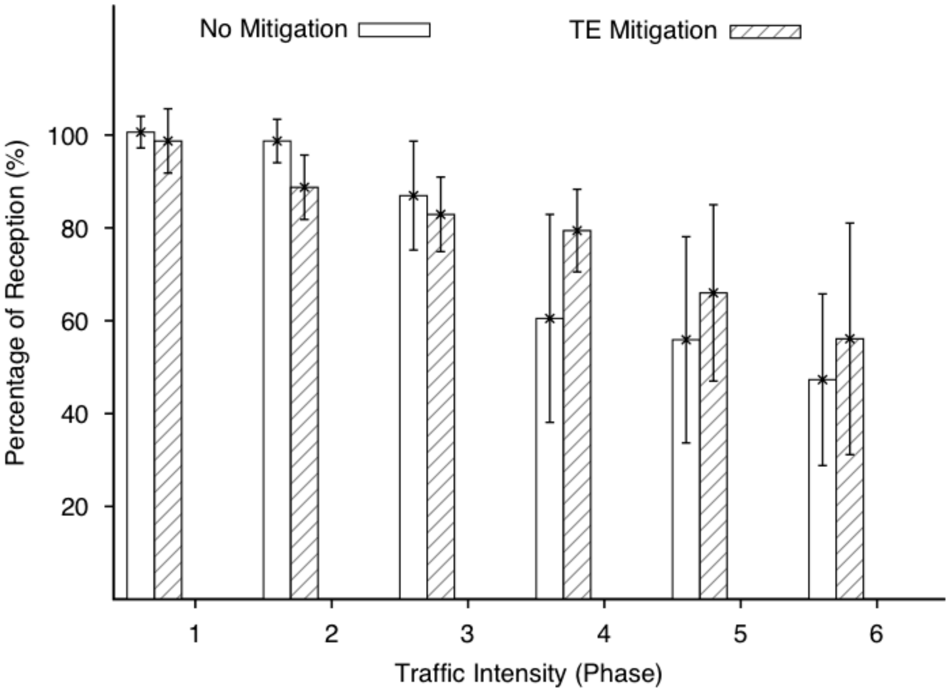
Simulations

- 4 Scenarios:
  - No Mitigation
  - TE Mitigation (End-to-end mitigation)
  - PHB Mitigation (Per-hop mitigation)
  - PHB+TE Mitigation
- 15 simulations each scenario
- Time per simulation time ≈ 15 hours
- Evaluation criteria: PoR (Percentage-of-Reception)
  - traffic received over the traffic sent

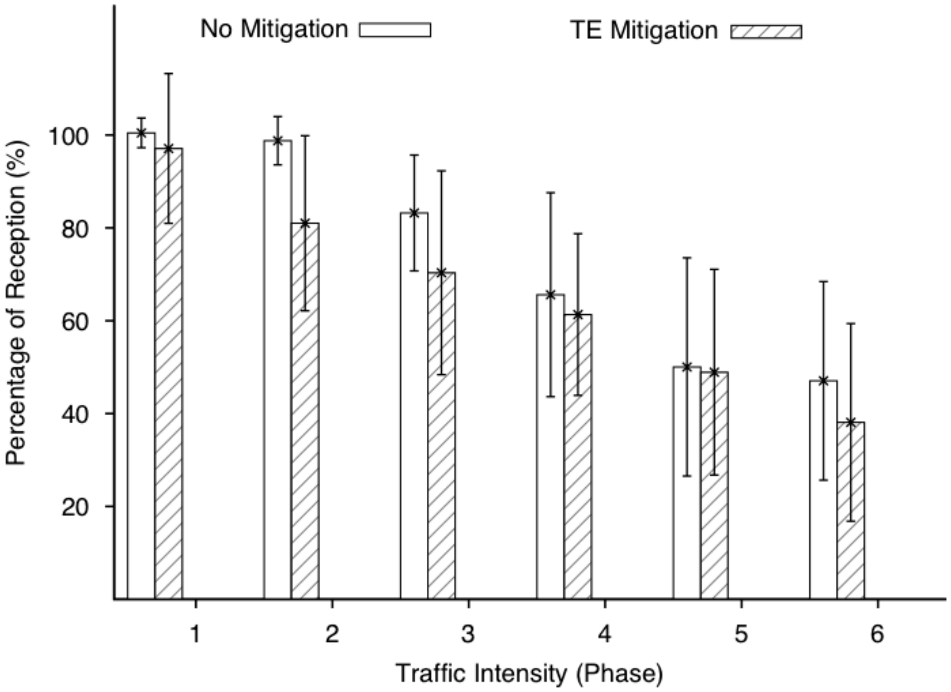
(L)
(S1)
(S2)
(S3)
No Mitigation
PHB Mitigation
TE Mitigation
TE+PHB Mitigation
Percentage of Reception (%)
100
80
60
40
20
1
2
3
4
5
6
Traffic Intensity (Phase)

End-to-end approach 1/2

- No Mitigation: flows equally balanced & FIFO queuing/scheduling on every router
- TE Mitigation: different routing treatment of suspicious vs. legitimate flows
  - legitimate flows: regular treatment
  - low suspicious: load-balancing over Gold and Silver + reduced bandwidth + reduced priority
  - high suspicious: mapped to Bronze + highest restriction on bandwidth + lowest priority



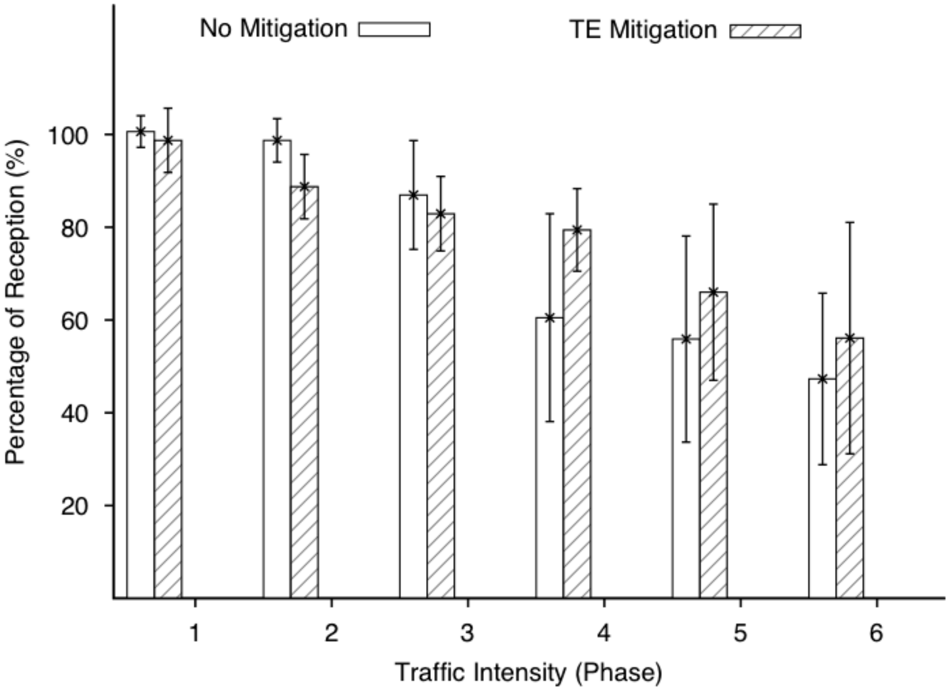
(a) Legitimate flows



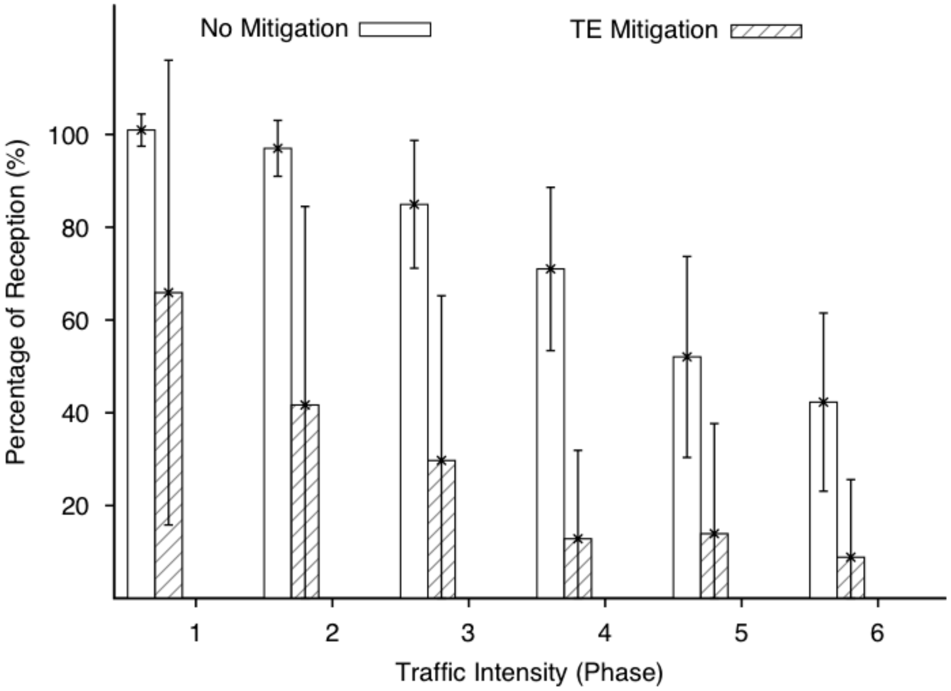
(b) Low suspicious flows

End-to-end approach 2/2

- No Mitigation: flows equally balanced & FIFO queuing/scheduling on every router
- TE Mitigation: different routing treatment of suspicious vs. legitimate flows
    - legitimate flows: regular treatment
    - low suspicious: load-balancing over Gold and Silver + reduced bandwidth + reduced priority
    - high suspicious: mapped to Bronze + highest restriction on bandwidth + lowest priority



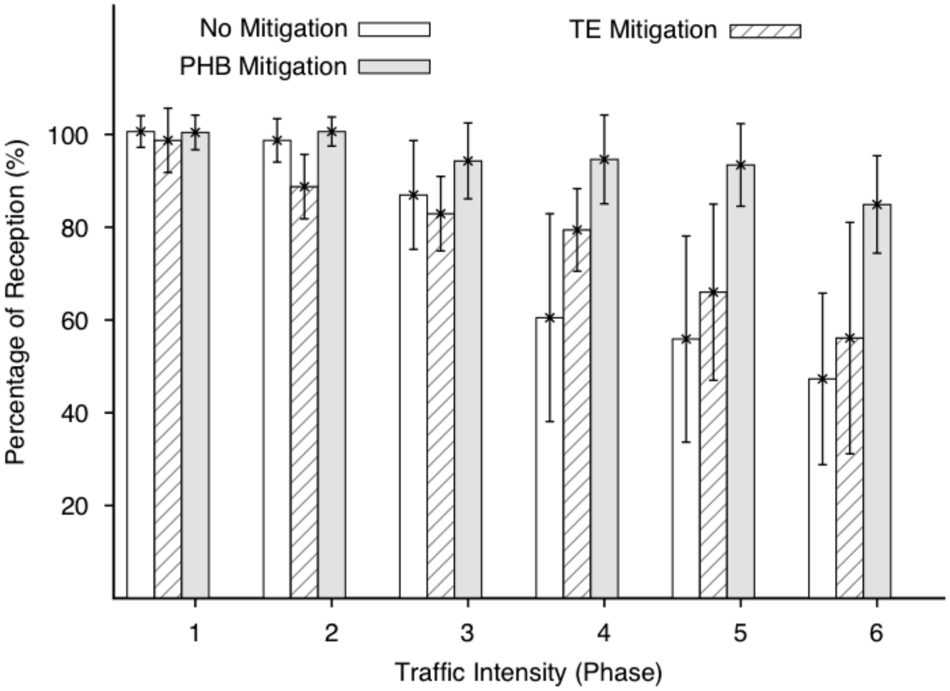
(a) Legitimate flows



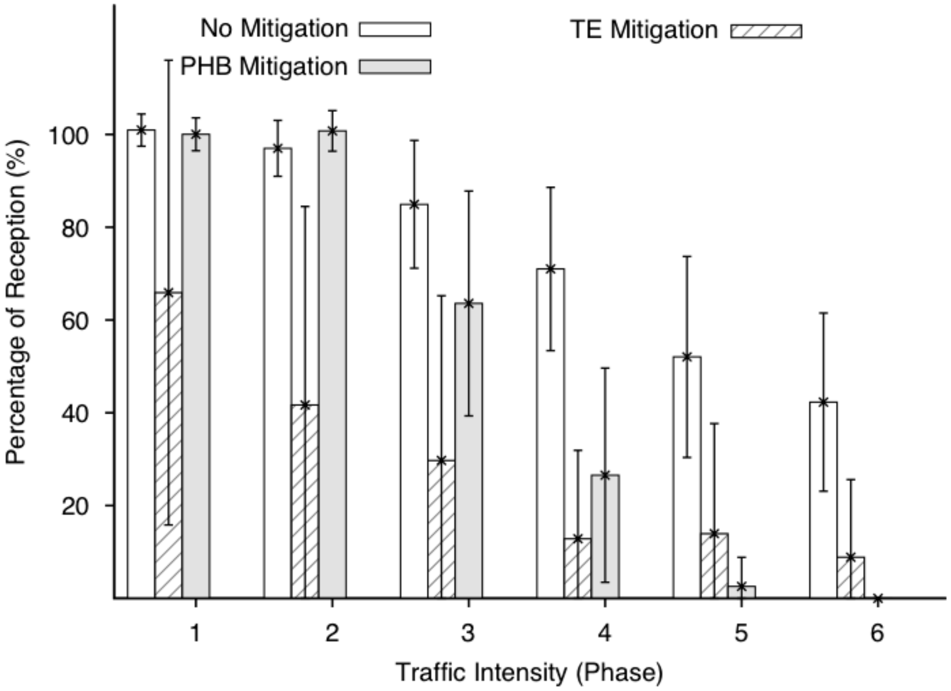
(d) High suspicious flows

Per-hop approach

- No Mitigation: flows equally balanced & FIFO queuing/scheduling on every router
- PHB Mitigation: applied at intermediate routers configured with Weighted Fair Queuing
  - legitimate flows: processed into low latency queue
  - suspicious flows: increasing weights, leading to lowest priority



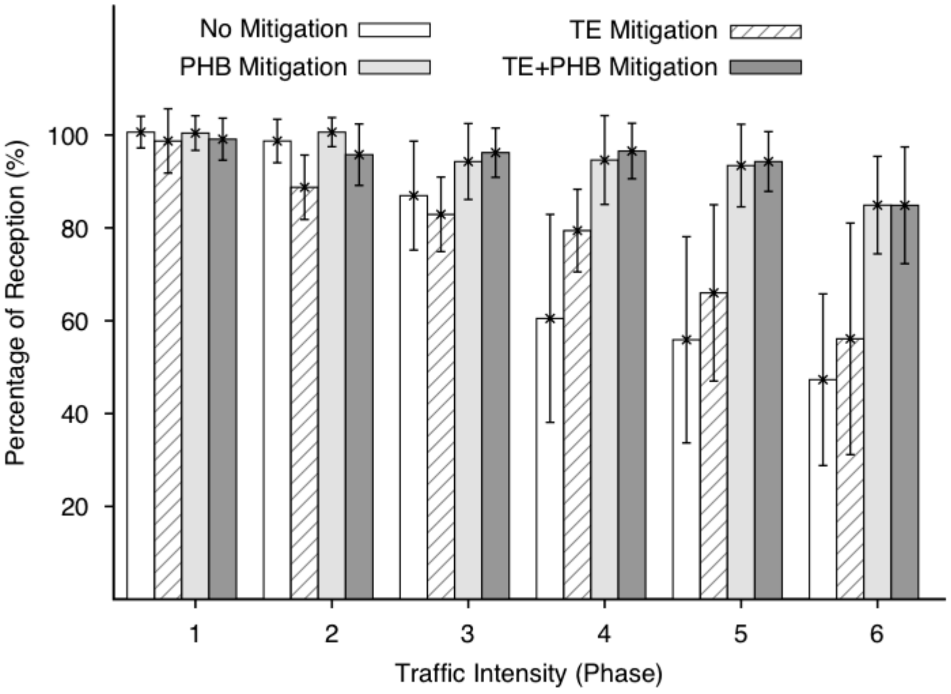
(a) Legitimate flows



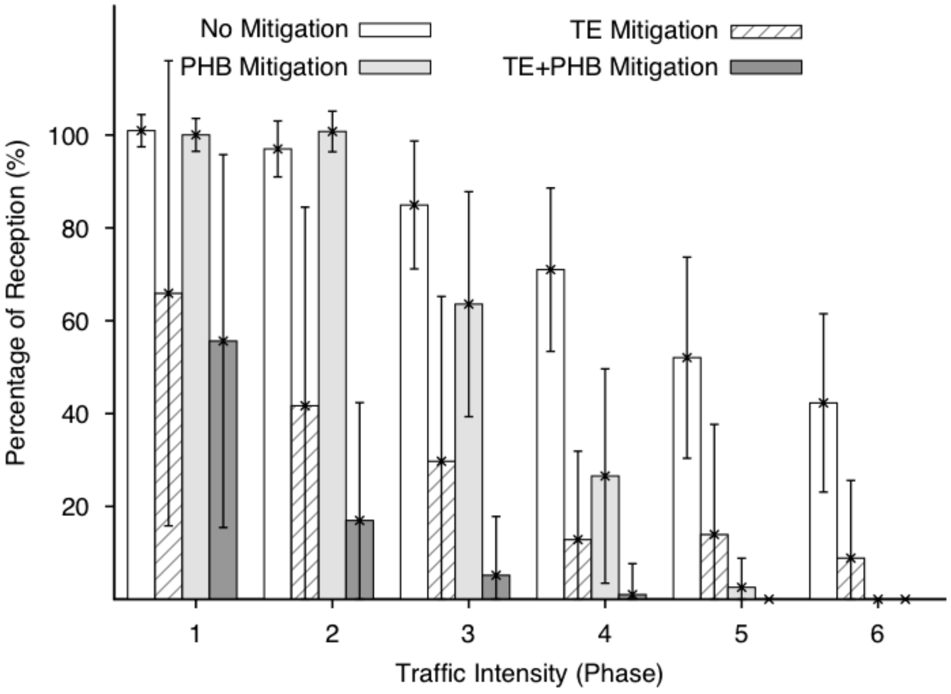
(d) High suspicious flows

End-to-end & Per-hop

- No Mitigation: flows equally balanced & FIFO queuing/scheduling on every router
- TE+PHB Mitigation: combine mitigation based on two previous approaches



(a) Legitimate flows



(d) High suspicious flows

Outline

- Motivation
- Background on MPLS
- MPLS-based mitigation
- **Conclusion & perspectives**

Conclusion & Perspectives

- Problem addressed today:
  - Enable adaptive mitigation of suspiciousflows
- Provided solution:
  - Complement to existing equipment, by tuning parameters
  - Guarantee best QoS for legitimate flows
  - Possibility to reroute suspicious flows for further inspection
    - goal: reduction of false detection rate
- Future (on-going work):
  - Complement evaluation (PoR + Delay, ...)
  - Comparison to current techniques (e.g., Blackholing)
  - From intra-domain to inter-domain