MPLS-based DDoS Mitigation

Pierre Edouard Fabre & Jouni Viinikka & Hervé Debar

pef@6cure.com & jvi@6cure.com & herve.debar@telecom-sudparis.eu

6cure & IMT

Objectives

- distribute DDoS mitigation upstream from the target
- maintain an *acceptable* level of Quality of Service during DDoS attacks by :
  - using *existing router capabilities*
  - efficiently load-balancing traffic, ie. restricting malicious traffic into a lower QoS trunc.
- proactive setup possible while avoiding allocating network resources (e.g. a FEC) for malicious traffic before and after the attack

Background

An MPLS FEC contains both malicious and legitimate traffic

Attack Characterization

Malicious traffic is discriminated on an IP basis.

- source IPs for unspoofed traffic
- destination IPs for spoofed traffic

Characteristics retained in a MPLS Label format as *Mitigation Label*

Mitigation Label

Goal: determine if an IP is involved in an attack

Pushed onto each packet FEC label stack. (Figure 1)

PPP or Ethernet Header	outer MPLS Header	FEC MPLS Header	Mitigation Label Header	Inner MPLS (e.g. IP) Header

Figure 1: Packet Datagram

Approach

Use of MultiPath

- before the attack: mutitple paths handle the FEC related traffic
- during the attack: available paths are segregated to handle legitimate and malicious traffic differently with use of load-balancing of IP and Mitigation Label. Different QoS can then be applied to the path with Traffic Engineering.

Mitigation Plan

1. push Mitigation Label that characterizes DDoS attacks at the Edges routers
2. advertise Mitigation Router (core router) of the FEC to protect and attack characteristic (source- or destination-based load-balancing)
3. traffic is split at the Mitigation Router side
   - positive traffic : traffic that match the Mitigation Label characterization is *shaped* to reach a maximal bandwidth constraint (Traffic Engineering)
   - negative traffic which does not match characterization

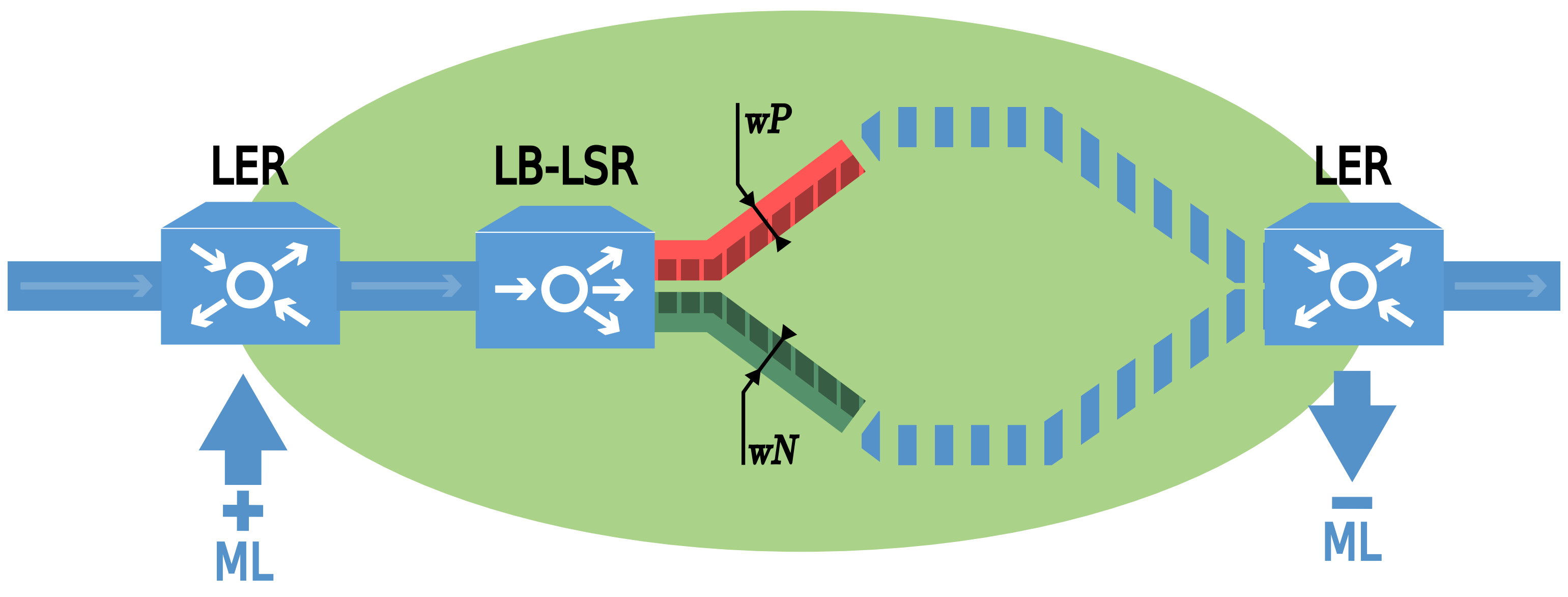

Figure 2: Traffic segregation

Results

Hypothesis

- 2 output interfaces used (up-to 16) on the Load-Balancing router $\forall idx \in [0, 15], OUTPUT[\,idx\,] =$ output interface
- Load-Balancing **[Comment:** *todo citation*]: $output = OUTPUT\,[\,CRC16\,(\,IP\,|\,MitigationLabel\,)\,\%\,16\,]$
- output path weight tuning capabilities (wP, wN in Figure 2)

Finding Mitigation Label that maximizes the number of True Positive IPs.

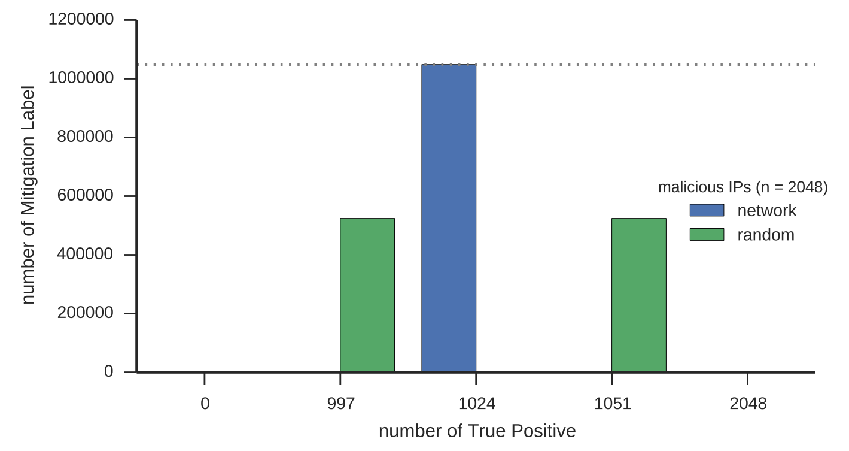

Figure 3: True Positive IPs Distribution

Figure 3 shows how the Load Balancing distributes the malicious IPs (represented by either a 2048 IPs subnet or 2048 random IPs) on the positive path. The standart deviation of network pool distribution curve is smaller than the random IP pool. Although both distribution have a small standard deviation ($< 1\%$). The second characteristic of the True Positive distribution is that the mean is equal to $\frac{wP}{wP+wN}$.
Several Load-Balancing simulations in varying number of malicious IPs, wN and wP validate that: $\forall$malicious IPs pool,

$$\exists ML \mid \begin{cases} nIPs_{TP} = LB\,(\,IP,\ ML\,) \\ max\,(\,nIPs_{TP}\,) \simeq \frac{wP}{wP+wN} \times nIPs_{malicious} \end{cases}$$

Conclusions

- as the load-balancing is a per IP basis, results do not reflect the real efficiency in terms of volume. For example in reflective volumetric attack, volume per malicious IP is much larger than per legitimate IP.
- legitimate traffic handled with a declared malicious IP (e.g. NATed traffic) are not recognised as collateral damage (ie. False Positive)
- in terms of number of IPs, the maximum of True Positive is no enough

Future Works

- Add the cappability to rank malicious IPs (e.g. according to their related volume)
- Increase the mean value of the True Positive IPs distribution. A variety of gutures can be envisaged, such as the use of another load-balancing function instead of CRC16.
- Compare these results with real from attack traffic captures.

Acknowledgement

This work has been supported in part by the European Seventh Framework Programme (FP7), and by the Japanese Ministry of Internal Affairs and Communication (MIC) during the project NECOMA under grant agreement N^{O} 608533.