Analysis of Control, Data separation in ForCES protocol for protection against DoS attacks

Hormuzd Khosravi

Shashidhar Lakkavalli

Lily Yang

60th IETF Meeting, San Diego

Problem Statement

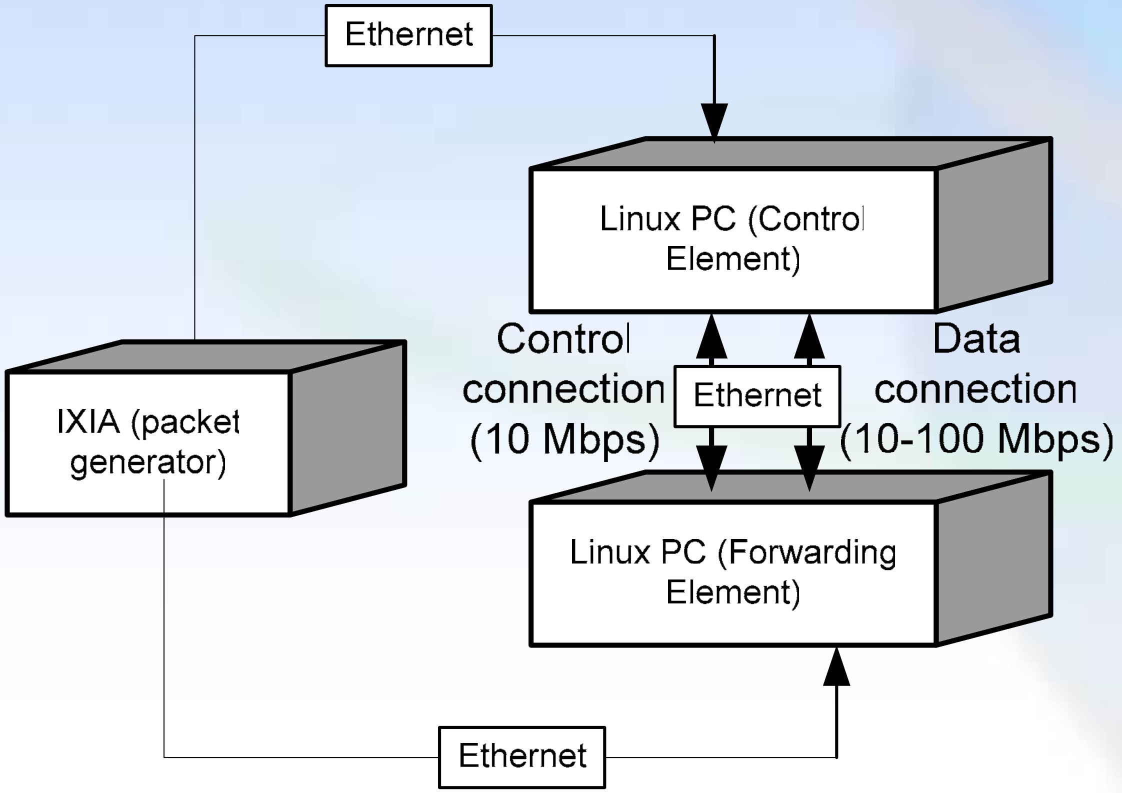
- **Requirements RFC 3654 – “Protection against Denial of Service Attacks (based on CPU overload or queue overflow) - Systems utilizing the ForCES protocol can be attacked using denial of service attacks based on CPU overload or queue overflow. The ForCES protocol could be exploited by such attacks to cause the CE to become unable to control the FE or appropriately communicate with other routers and systems. The ForCES protocol MUST therefore provide mechanisms for controlling FE capabilities that can be used to protect against such attacks. FE capabilities that MUST be manipulated via ForCES include the ability to install classifiers and filters to detect and drop attack packets, as well as to be able to install rate limiters that limit the rate of packets which appear to be valid but may be part of an attack (e.g., bogus BGP packets).”**

Possible Solutions

- **Basic Idea – Separation of data and control messages**
  - **Data messages are control protocol packets such as RIP, OSPF, BGP packets. All other messages considered control messages**
- **Solution 1 – Different Transport connections**
  - **Use different congestion aware transport protocol connections for data and control messages**
- **Solution 2 – Different Prioritization**
  - **Assign higher priority to control messages and use scheduling mechanisms in protocol to differentiate**

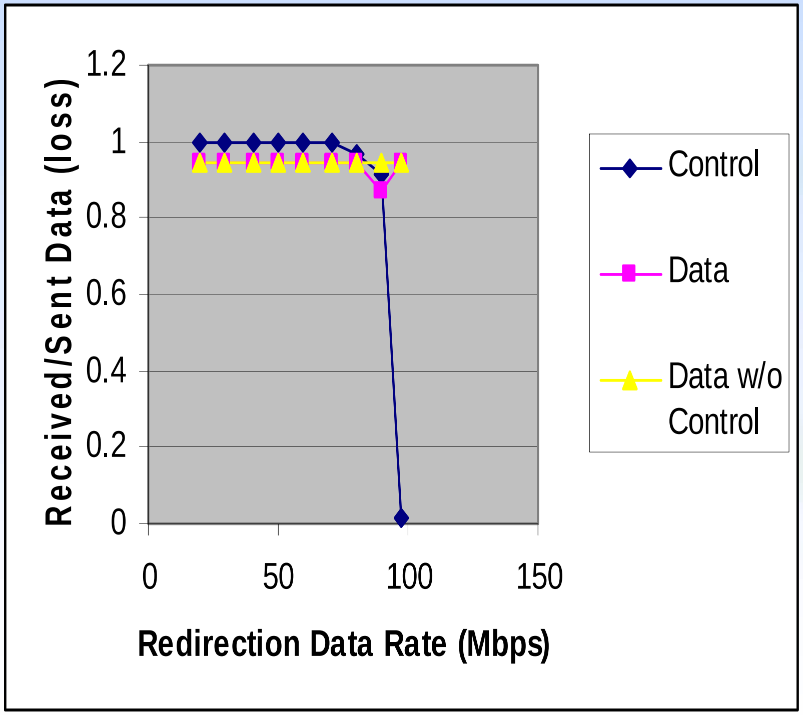
Experimental Setup

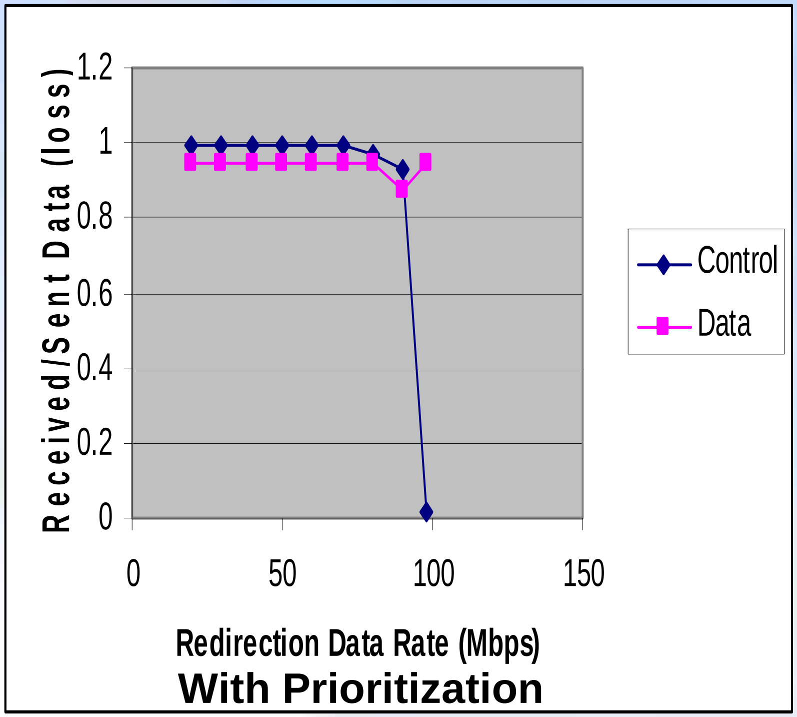
- Used IXIA box as packet generator and Linux PCs as CE, FE connected using 100 Mbps Ethernet links
- Basic implementation consisting of multi-threaded client/server on Linux using pthreads (RR scheduling for threads)
- Increased data connection rate to simulate DoS Attack


Ethernet
Linux PC (Control Element)
Control connection (10 Mbps)
Ethernet
Data connection (10-100 Mbps)
IXIA (packet generator)
Linux PC (Forwarding Element)
Ethernet

Experimental Results

- Using TCP for control and UDP for data messages (with and without prioritization for control)
- Results show UDP (data) overwhelms TCP (control) traffic during DoS attack, prioritization of No help

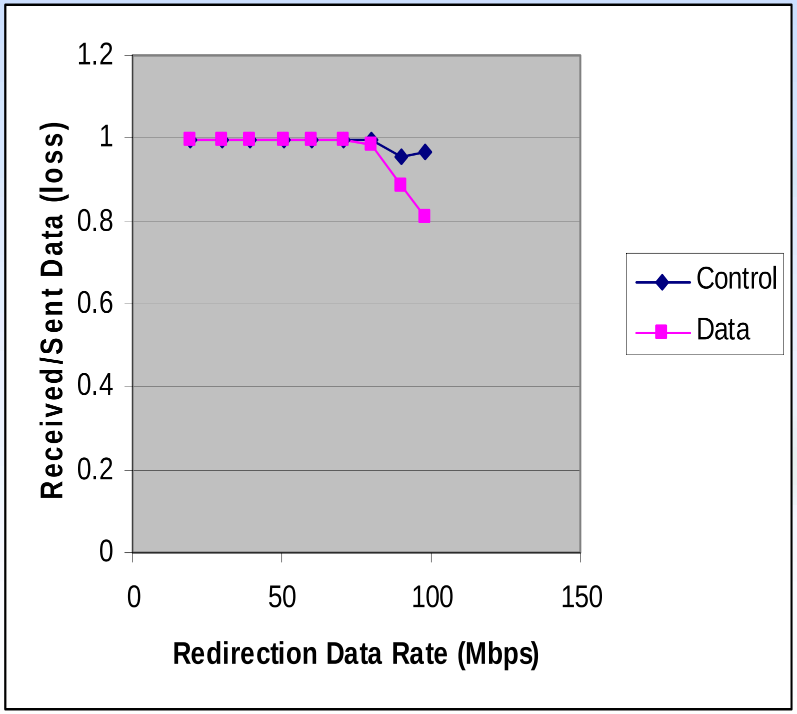


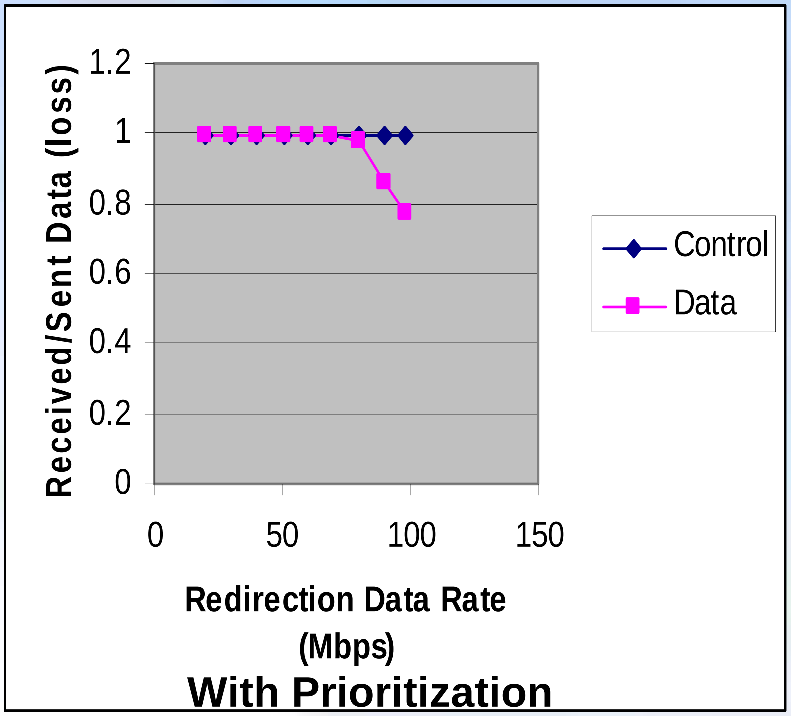


With Prioritization

Experimental Results (contd..)

- Using TCP for control and TCP for data messages (with and without prioritization for control
- Results show control traffic is not overwhelmed by data traffic during DoS attack, prioritization helps improve the performance (by 5%)





With Prioritization

-

Summary

- Protection against DoS attacks is a key requirement for the ForCES protocol
- Separation of Control and Data messages in the ForCES protocol is key to meet this requirement
- Separation scheme consisting of
  - separate congestion aware, control and data transport connections such as TCP connections
  - combined with higher priority for control gives best results
- References – http://www.sstanamera.com/~forces/, http://www.sstanamera.com/~forces/Ietf59/testbed_dong.pdf