A Testbed for GRMP Protocol

(draft-wang-forces-grmp-01.txt)

Ligang Dong (presenter), Lei Shi, and Weiming Wang,

(donglg@mail.hzic.edu.cn)

College of Information & Electronic Engineering

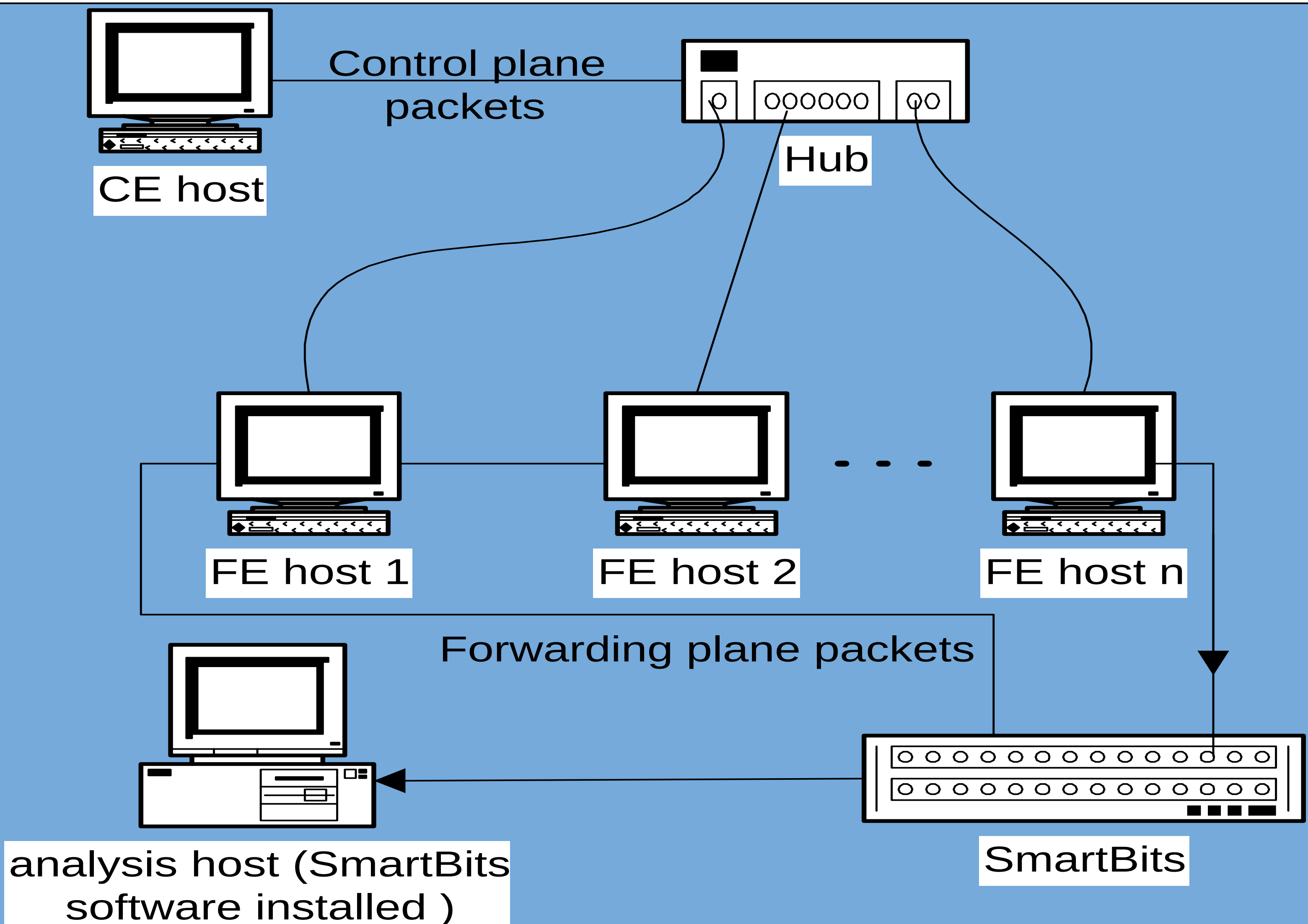
Hangzhou University of Commerce, P.R.China

March 2 2004

Content

- Introduction to Testbed
- Experiments on Testbed

Introduction to Testbed – Deployment



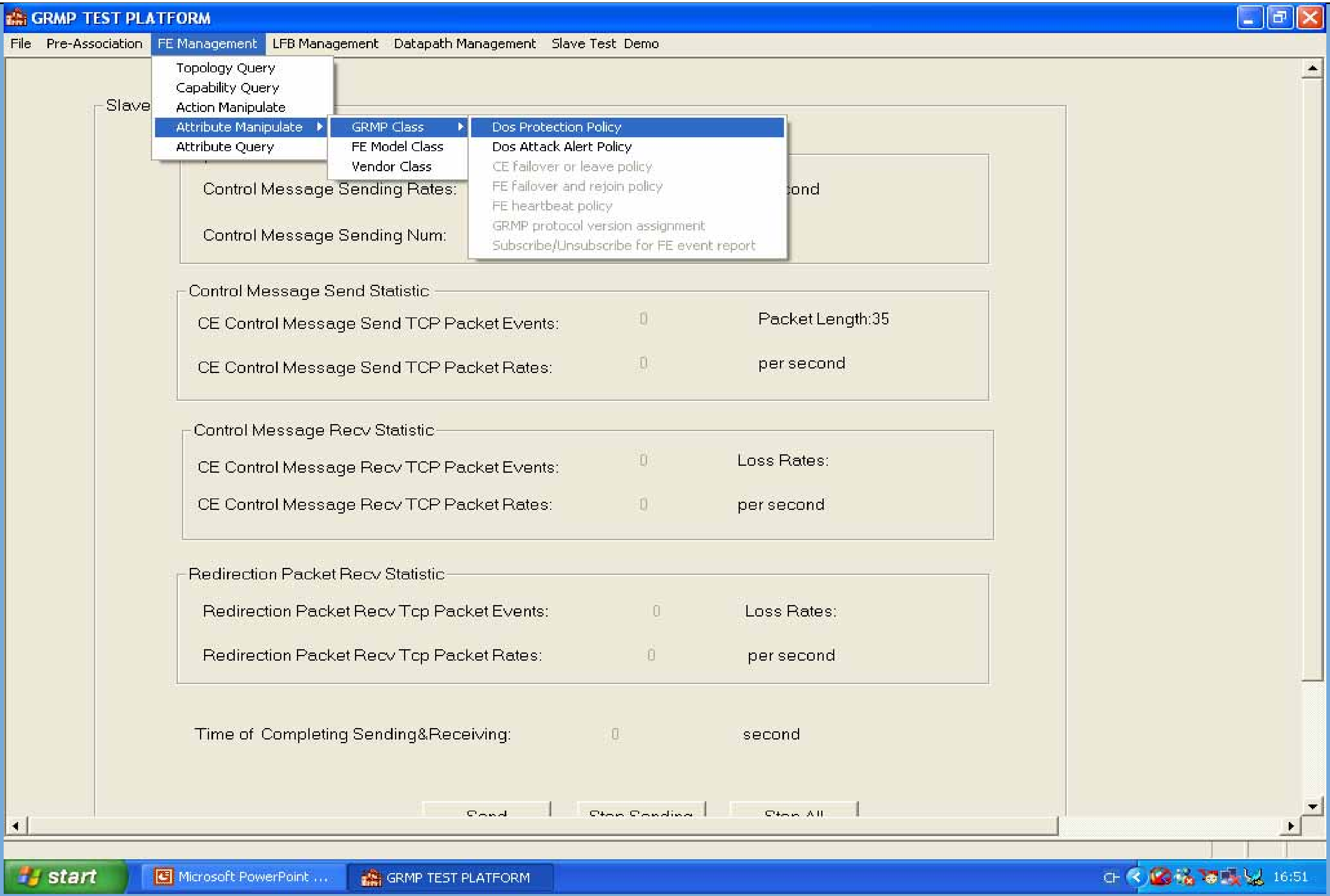
Introduction to Testbed – CE and FE

- The CE located in the CE host takes the responsibility to control FEs.
- The messaging system between the CE and the FEs follows GRMP
- Control plane packets can be sent between CE and FEs via TCP, UDP, or IP socket connection.

Introduction to Testbed - CE

- The CE is realized using a VC++ software that runs in Windows OS. (software)
- The CE can send various kinds of messages, whose parameters can be specified via dialog boxes.

Introduction to Testbed – CE software



Introduction to Testbed – FE

- The FE is realized using an adapted Linux kernel, which can forward packets and communicate with the CE.

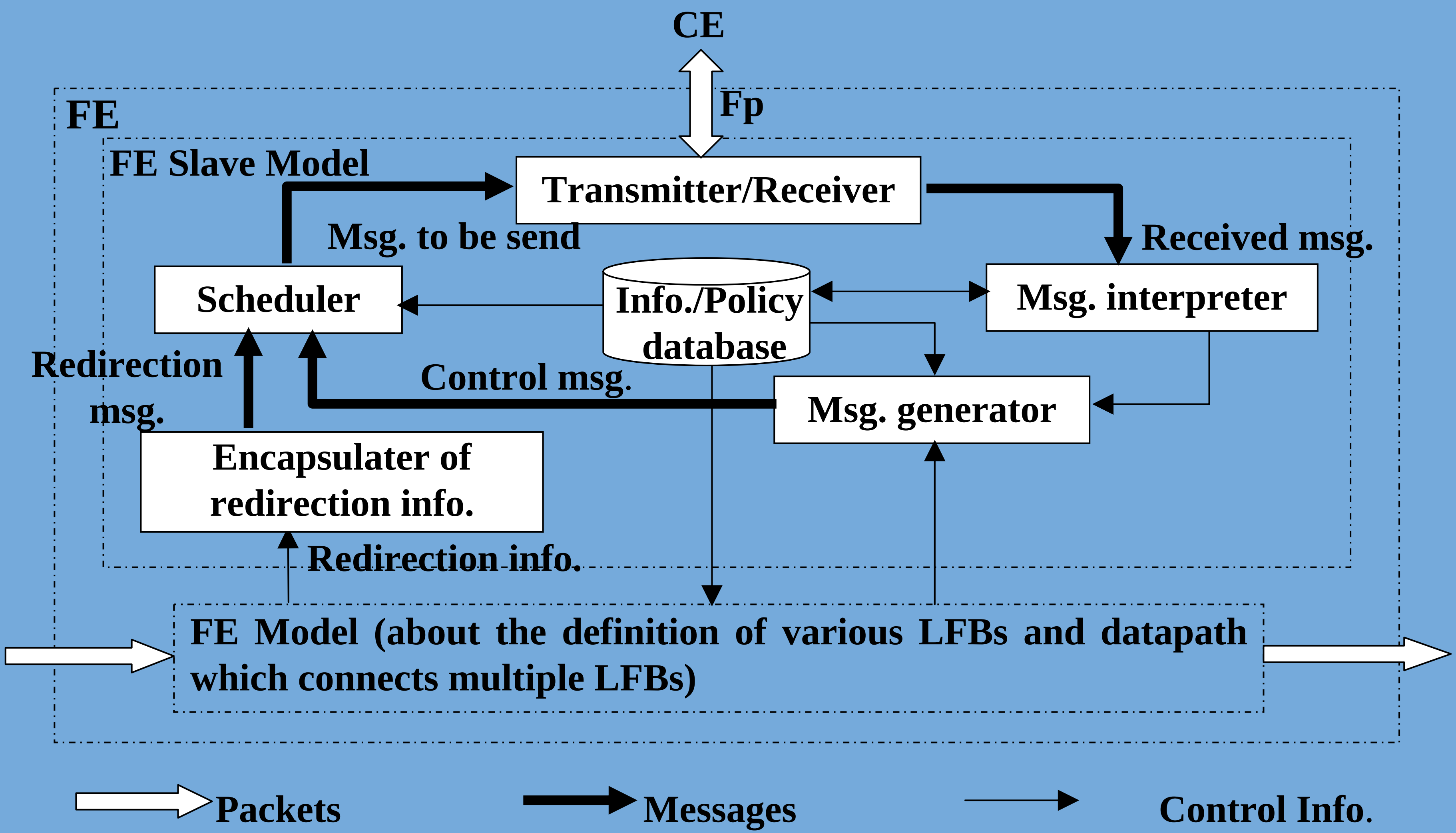
Introduction to Testbed – Smartbits

- The smartbits is used to generate various rates of packets and measure the rates of received packets.

Experiments on Testbed - Purpose

- Check the implementation feasibility of GRMP
- Currently testify the strategies for DoS attack protection policy

GRMP: FE architecture



Experiments on Testbed - Setting

- The smartbits generates and sends common data packets and redirection data packets to FEs.
- The CE generates and sends pseudo control packets to FEs.
    - As the rate of pseudo control packets can be controlled, we use pseudo control packets instead of “real" control packets for performance comparison.

Experiments on Testbed – Setting (cont.)

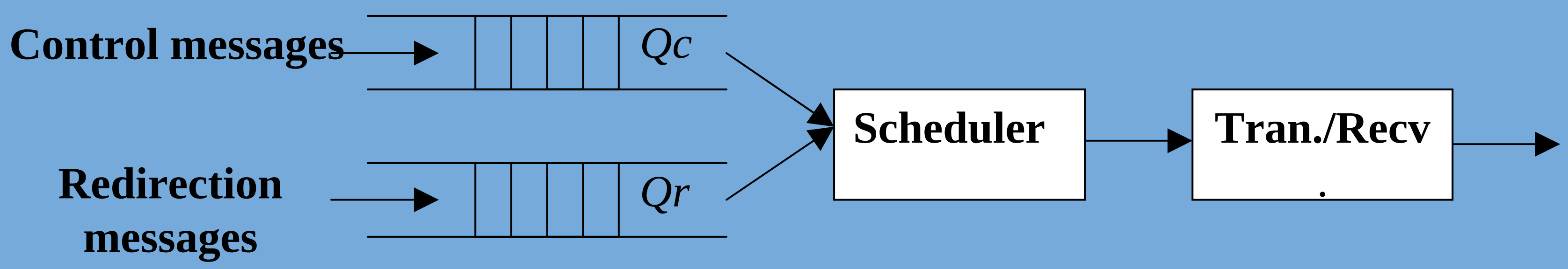
- When the FE receives packets from the CE, the FE sends back reply packets according to the test demand.
- When the FE receives packets from the smartbits, the FE forwards or redirects received packets to the smartbits or CE respectively according to the setting status of the classifier LFB.

Experiments on Testbed – Experiment I

- **Content**
  - **Before uploading a classifier LFB, All the packets sent by the smartbits are received by smartbits. (screen record)**
  - **The CE sends control messages to the FE and inform a FE host to upload the classifier LFB. (screen record)**
  - **After uploading, the redirection data packets are received by the CE while the common data packets are still received by the smartbits. (screen record)**
- **Result**
  - **It testifies that we implemented the messaging system and dynamic loading of the classifier LFB.**

Experiments on Testbed – Experiment II

- **Content**



- **We change the scheduling strategy (for DoS Protection Policy) in the FE in terms of the control from the CE according to GRMP**
  - **FCFS strategy**
  - **Priority-Based strategy**
  - **Rate-Based strategy**

Experiments on Testbed - Metrics

- DoS attack from the redirection packets may **congest** the communication channel
- Currently used performance metric: the **loss rate** of packets.
    - Packets may be **lost in the waiting queues** when congestion happens. The more the packets lost, the more serious the congestion is.

Experiments on Testbed – Experiment II

- **Table 1: Loss rate of Control and Redirection packets in the case of one TCP (when the rate of redirection packets varies)**

Packet Rates (% of 10Mbs)		r_c=50% r_r=20%	r_c=50% r_r=50%	r_c=50% r_r=80%	r_c=50% r_r=150%
FCFS	control	0.3%	0.3%	21%	49%
	redirect.	0.3%	0.3%	21%	49%
Priority-Based	control (H)	0.3%	0.4%	21%	21%
	redirect. (L)	0.2%	0.4%	22%	67%
Rate-Based (with RR)	Control (no rate limit)	0.3%	0.2%	0.1%	0.1%
	redirect. (50% rate limit)	0.3%	0.2%	38%	67%

Experiments on Testbed – Experiment II

- **Analysis of Table 1:**
  - **FCFS scheduling strategy cannot prevent the DoS attack**
  - **Priority-Based strategy can prevent the DoS to some extent.**
  - **Rate-Based (with Round Robin) strategy can prevent the DoS attack quite well.**

Experiments on Testbed – Experiment II

- **Table 2: Loss rate of Control/Redirection packets in the case of one TCP (when the rate of control packets varies)**

Packet Rates (percentage of 10Mbs)		r_c=20% r_r=50%	r_c=50% r_r=50%	r_c=80% r_r=50%	r_c=150% r_r=50%
Priority-Based	control	0.2%	0.4%	13%	32%
	redirect.	0.2%	0.4%	52%	100%

It shows that the control packet may congest the redirection packet too. In particular when we use priority-based strategy, it is possible that all of redirection packets can be congested.

Experiments on Testbed – Experiment II

- **Table 3: Loss rate of C and R packets in the case of TCP channel for C packets and UDP channel for R packets**

Packet Rates (percentage of 10Mbs)		$r_c=50\%$ $r_r=20\%$	$r_c=50\%$ $r_r=50\%$	$r_c=50\%$ $r_r=80\%$	$r_c=50\%$ $r_r=150\%$
Scheduling strategy from Linux kernel	Control (TCP channel)	0.3%	2.4%	67%	76%
	Redirect. (UDP channel)	0.2%	0.3%	0.3%	44%

It shows that control packets in the TCP channel will be affected by redirection packets in the UDP channel,
— meaning a DoS attack cannot be prevented purely by such separation.

Experiments on Testbed - Conclusion

- Current experiments testify the following facts
  - GRMP is feasible for implementation of
    - messaging, LFB uploading, …
  - Scheduling at the ForCES protocol level is effective for DoS attack protection.
    - Moreover, in this case, the scheduling strategies can be flexibly selected.
  - DoS attack cannot be avoided ONLY by separating Control packets and Redirection packets to different channels.
  - It is possible that Control packets may congest Redirection packets in some cases.

The End