Application of NetFPGA in Network Security

Hao Chen
2/25/2011
Introduction to Shrew DDoS Attacks

- DDoS attacks: Distributed Denial of Service attacks
- Shrew DDoS Attacks: Low rate TCP targeted DDoS Attacks
Power Spectral Density (PSD) Based Analysis

- Performing PSD analysis is computing intensive
- Adopt hardware implementation
  - NetFPGA based shrew DDoS attack detector
A NetFPGA Board

- Network + FPGA (Field Programmable Gate Arrays)

- Fits into standard PCI or PCI-X slot
  - Standard Bus: 32 bits, 33 MHz

- Provides interfaces for processing network packets
  - 4 Gigabit Ethernet Ports

- Allows hardware-accelerated processing
  - Implemented with FPGA Logic
The Block Diagram of NetFPGA

Your hardware specified in Verilog source code connected to components of the Reference Router circuits and cores.
A NetFPGA System

Networking Software Running on a standard PC

A hardware accelerator built with FPGA driving Gigabit network links

PC with NetFPGA

NetFPGA Board
Our Rackmount NetFPGA Server

2U Server (Dell 2950)

NetFPGA inserts in PCI or PCI-X slot
A NetFPGA Based Router
Architecture of Reference Router

- Five stages
  - Input
  - Input arbitration
  - Routing decision and packet modification
  - Output queuing
  - Output

- Packet-based module interface

- Pluggable design
Inter-Module Communication

Module i

data

ctrl

wr

rdy

Module i+1
Modifying Reference Router Pipeline
Modifying Reference Router Pipeline

Power Spectral Density (PSD) Based Shrew DDoS Attack Detector
Overall Shrew DDoS Attack Detection
Development Environment

NetFPGA Box 1
Producer

NetFPGA w
Custom DDoS Shrew
Traffic Generator

NetFPGA Box 2
Reference Router w
Shrew DDoS Detector

NetFPGA w
Custom DDoS Shrew
Detector

NetFPGA Box 3
Consumer

NetFPGA w
Reference NIC

Shrew Packet
Counter IF

1 msec TCP Count samples

Debug Interface

Autocorrelation

DFT

Threshold Detector

Shrew DDoS
Attack Detected
Questions?