1st DFG/GENI Doctoral Consortium, San Juan, PR
March 13th-15th, 2011

DDoS Attack on GENI

Ilker Ozcelik and Richard Brooks*
Clemson University

Abstract

In today's world the Internet is an environment where people not only communicate but also share knowledge, do business, attend school, and even socialize. As a result of growing dependence on the Internet, one of the biggest concerns of Internet users is security. Unfortunately, the number of security incidents increases exponentially every year.

A Distributed Denial-of-Service attack (DDoS attack) disables network services to legitimate users by flooding them. The recent attacks on trusted financial websites, Mastercard and PayPal, are an example of the need for security against DDoS attacks. One of the major problems with Distributed Denial of Service attacks is how difficult it is to detect the source of the attack, because of the many components involved.

In this study, we will obtain the Internet traffic signature to use as background traffic in future experiments. By using the real background traffic we will investigate the effectiveness of theoretical DDoS Attack detection techniques on GENI. We will also evaluate the equation of Necessary Traffic for DDoS Attack proposed by Dingankar and Brooks.

Research Objectives

Our study has four goals;

- Obtaining time series from real Internet data for future experiments.
- Testing Openflow slice isolation.
- Testing detection schemes using real background traffic.
- Verifying necessary DDoS attack traffic equation.

Experiments

In our experiments we will use two openflow enabled switches to manage the network traffic and two NetFPGA to collect data. In the first step of the experiment we will collect the number of packet and volume information from campus internet traffic to use as background traffic in future experiments.

Researchers have been using the synthetic network traffic to justify their detection algorithms. In the second step of our experiment, we will use the realistic background traffic, and test the effectiveness of the theoretical DDoS detection algorithms.

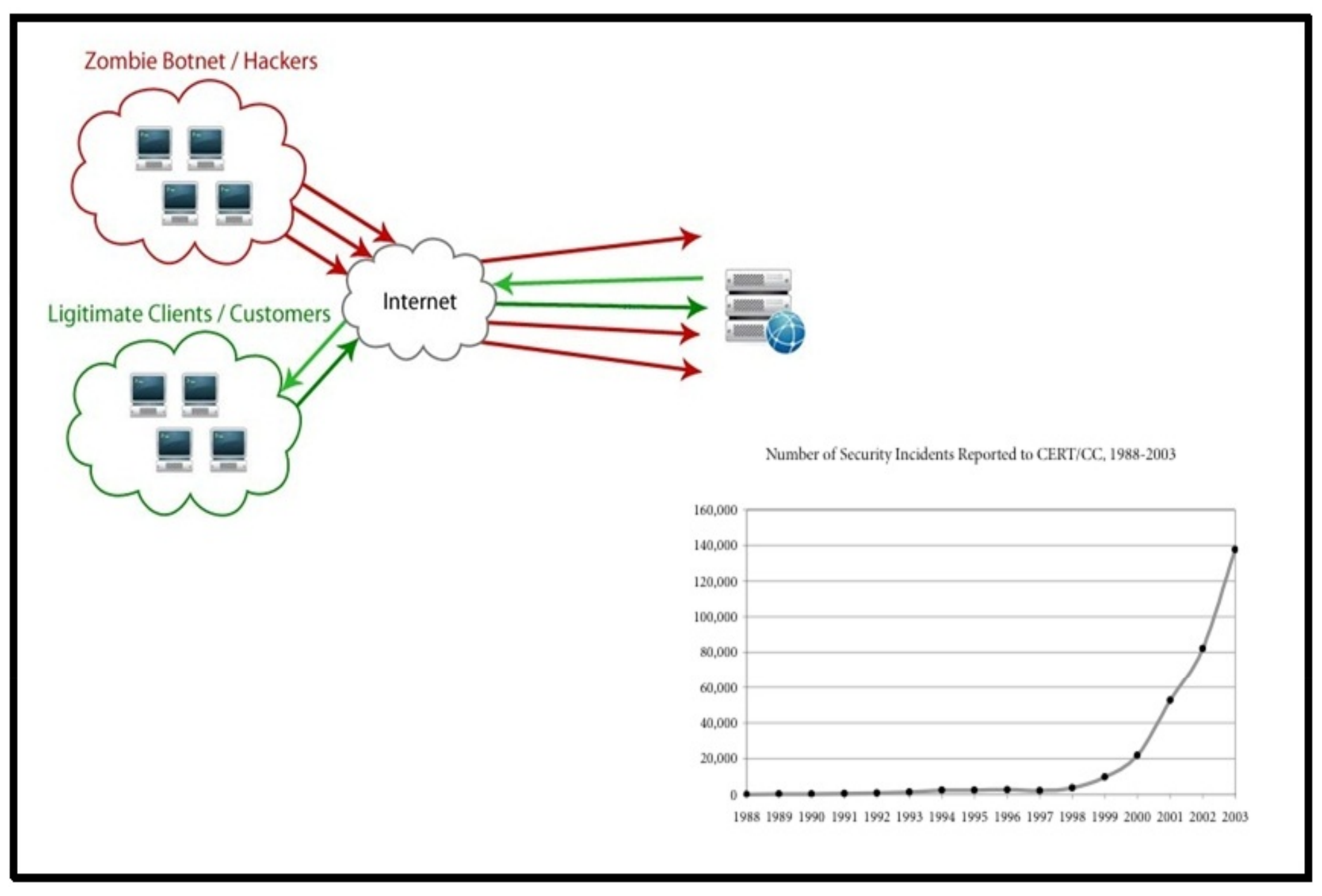

Fig 1. DDoS Attack

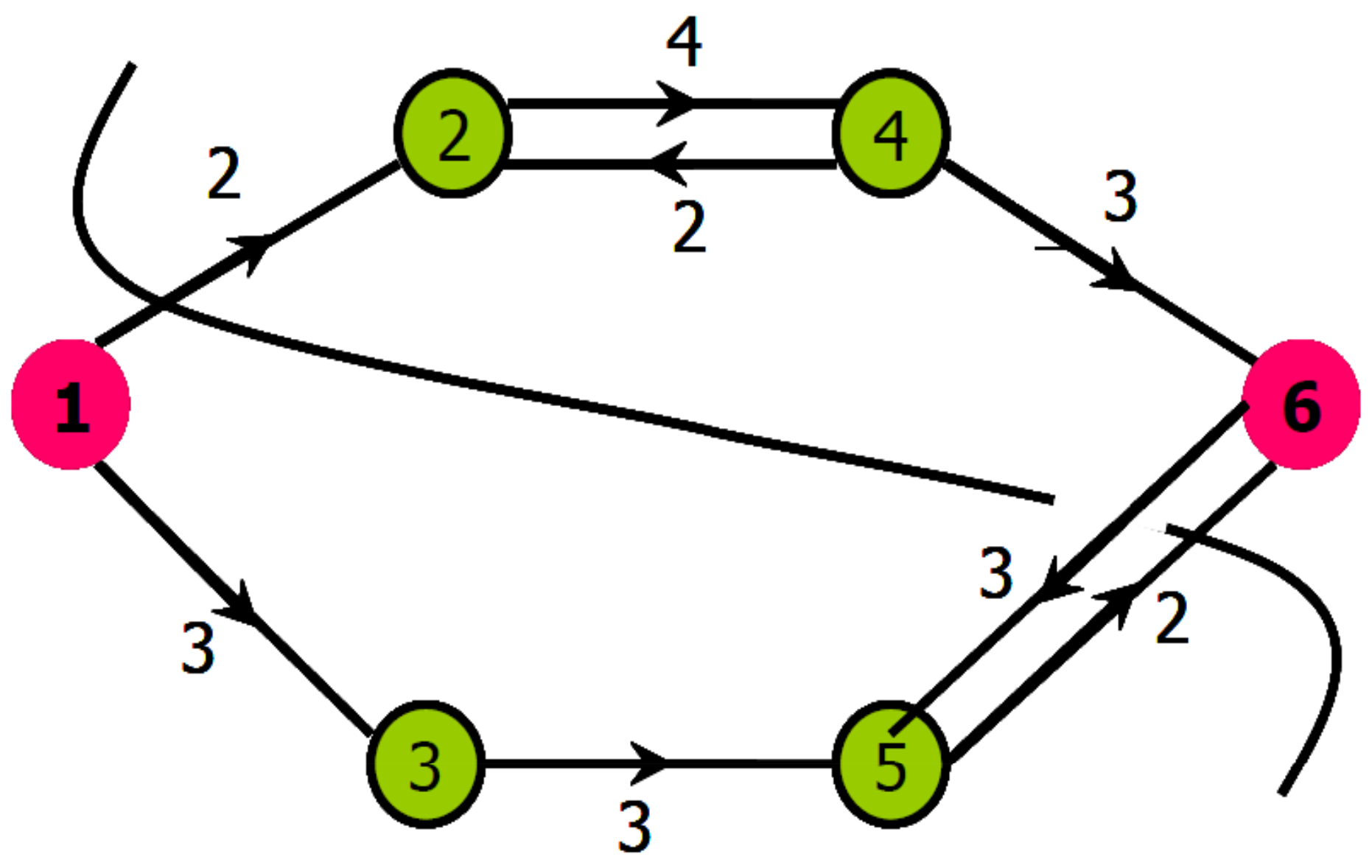

Fig 2. Max-flow and min-cut for directed graph

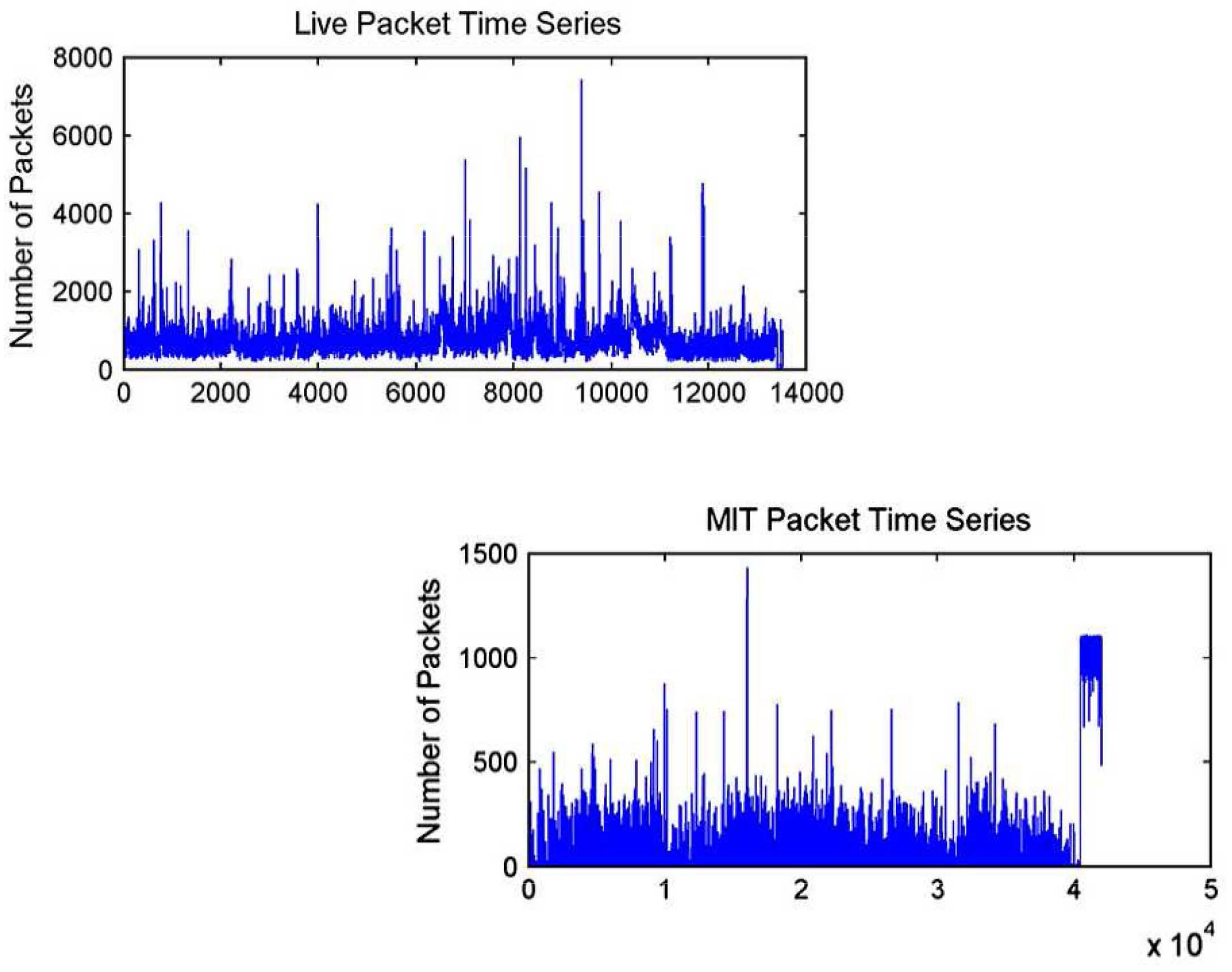

Fig 3. Live and Synthetic Packet Time Series

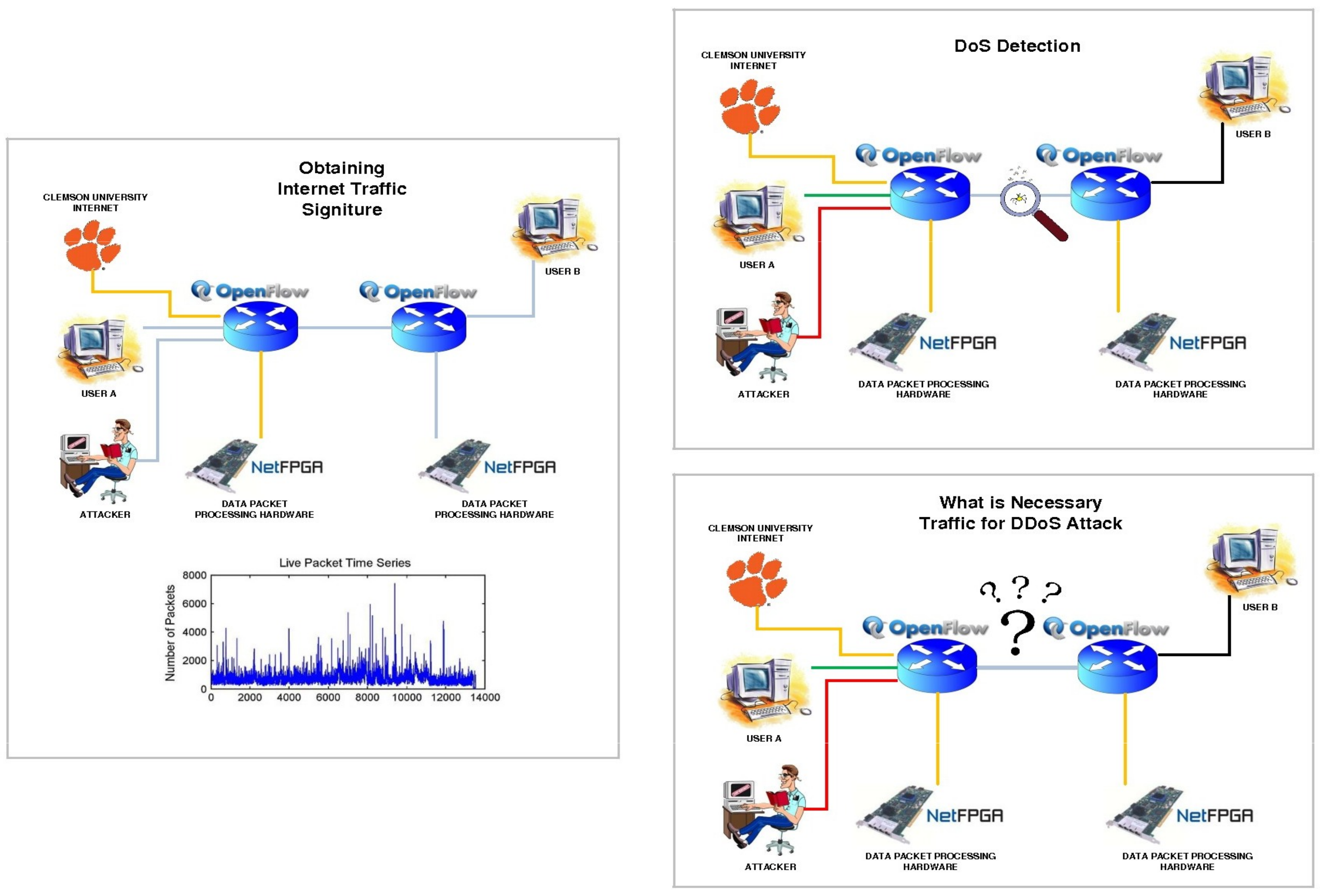
Obtaining Internet Traffic Signiture
CLEMSON UNIVERSITY INTERNET
OpenFlow
OpenFlow
USER A
USER B
ATTACKER
NetFPGA
DATA PACKET PROCESSING HARDWARE
NetFPGA
DATA PACKET PROCESSING HARDWARE
Live Packet Time Series
Number of Packets
8000
6000
4000
2000
0
0 2000 4000 6000 8000 10000 12000 14000
DoS Detection
CLEMSON UNIVERSITY INTERNET
OpenFlow
OpenFlow
USER A
USER B
ATTACKER
NetFPGA
DATA PACKET PROCESSING HARDWARE
NetFPGA
DATA PACKET PROCESSING HARDWARE
What is Necessary Traffic for DDoS Attack
CLEMSON UNIVERSITY INTERNET
OpenFlow
OpenFlow
? ? ?
?
USER A
USER B
ATTACKER
NetFPGA
DATA PACKET PROCESSING HARDWARE
NetFPGA
DATA PACKET PROCESSING HARDWARE

Fig 4. Experiment Sets

It is important to understand the requirements of a DoS attack in order to come up with effective countermeasure methods. It is evident that sending more packets than min-cut of the network can handle, cripples the network. Based on this idea, in the final step of our experiment, we will evaluate the equation of the Necessary Traffic for DDoS Attack proposed by Dingankar and Brooks.

Future Work

Detecting a DDoS Attack is not the solution for Internet security. After gaining better knowledge of DDoS Attacks, and detection methods, we will look for ways to develop countermeasures to eventually make networks immune to DDoS Attacks.

Use of Glab/GENI Infrastructure

In our experiments we will use openflow switches, end nodes and NetFPGAs on Clemson University Network. After getting results from our initial tests on campus we are planning to scale the experiments on GENI.