15th GENI Engineering Conference, Houston, TX, October 23th-25th, 2012

Performance Analysis of DDoS Detection Methods on GENI

Ilker Ozcelik and Richard Brooks*
Clemson University

Abstract

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.

In this study, we obtain the Internet traffic signature from our campus network to use as background traffic in DDoS detection experiments. By using the operational Internet traffic we investigate the effectiveness of theoretical DDoS Attack detection techniques on GENI.

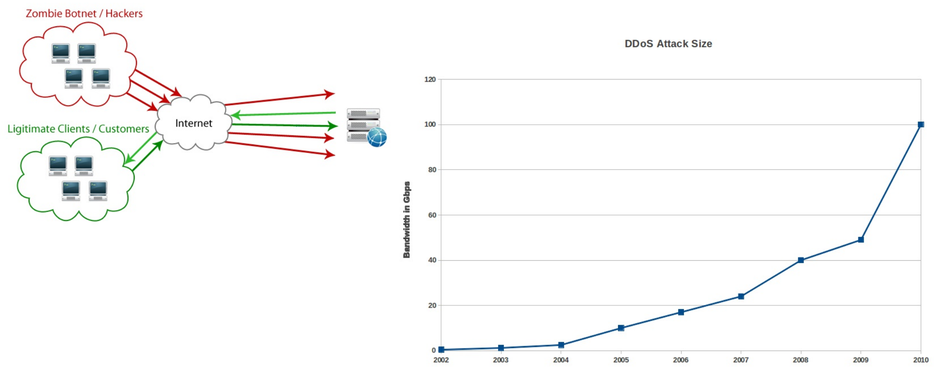

Fig 1. DDoS attack and attack volume increase trend

Experiment Design

The fundamental steps of our experiment design can be listed as;

- Replicating the operational system.
  - Consider negative effects
  - Discuss with local IT and test bed administrators
  - Run small test runs to verify lack of impact
- Using operational system data.
  - Verify need for IRB, (if necessary) get approval
- Data collection.
  - Consider data storage/archival/privacy issues

Experiment Setup & Objectives

In our experiments we use Openflow enabled switches to manage the network traffic and Clemson University Condor computer cluster to generate DDoS attack traffic. We collect experiment observations using our Openflow controller..

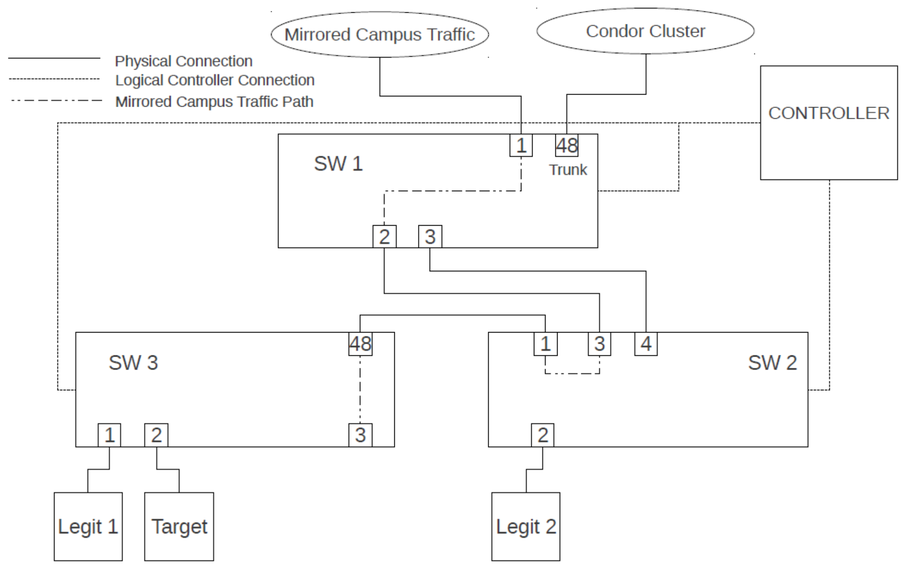

Fig 2. Experiment setup

Our experiments has two goals;

- Obtaining time series from operational Internet traffic.
- Testing DoS detection schemes using operational Internet traffic on GENI.

Data Collection

DDoS detection methods detect anomalies on observed Internet traffic. Due to our current inability to statistically explain Internet traffic; current generation network simulators are unable to mimic it adequately. Therefore, it is important to use real Internet data while verifying a DDoS detection method. We collect time-series from the operational Internet traffic, and test the effectiveness of the theoretical DDoS detection algorithms by using it as background traffic.

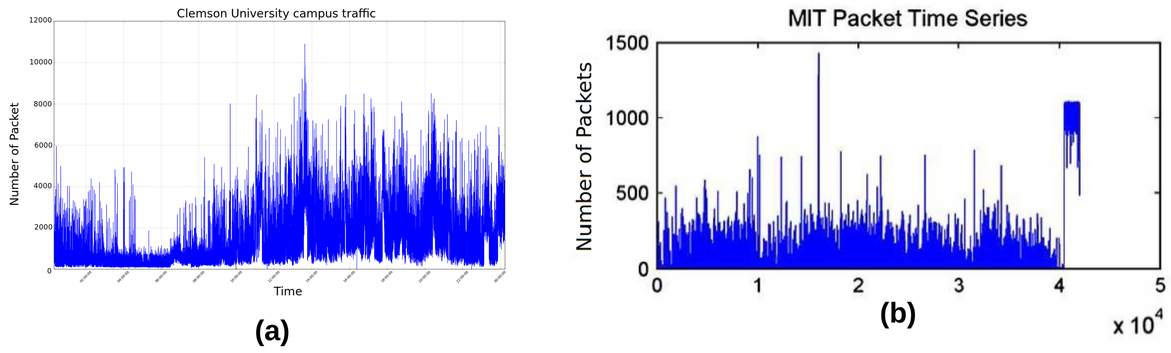

Fig 3. (a) Clemson University campus traffic without attack (b) Artificial network traffic generated MIT lab with attack

Verifying DDoS Detection Methods

Currently we are testing two DDoS detection method

- **Cusum** : calculates the difference between the current and estimated average of observations
- **Wavelet** : is used to quickly detect the changes on cusum coefficient.

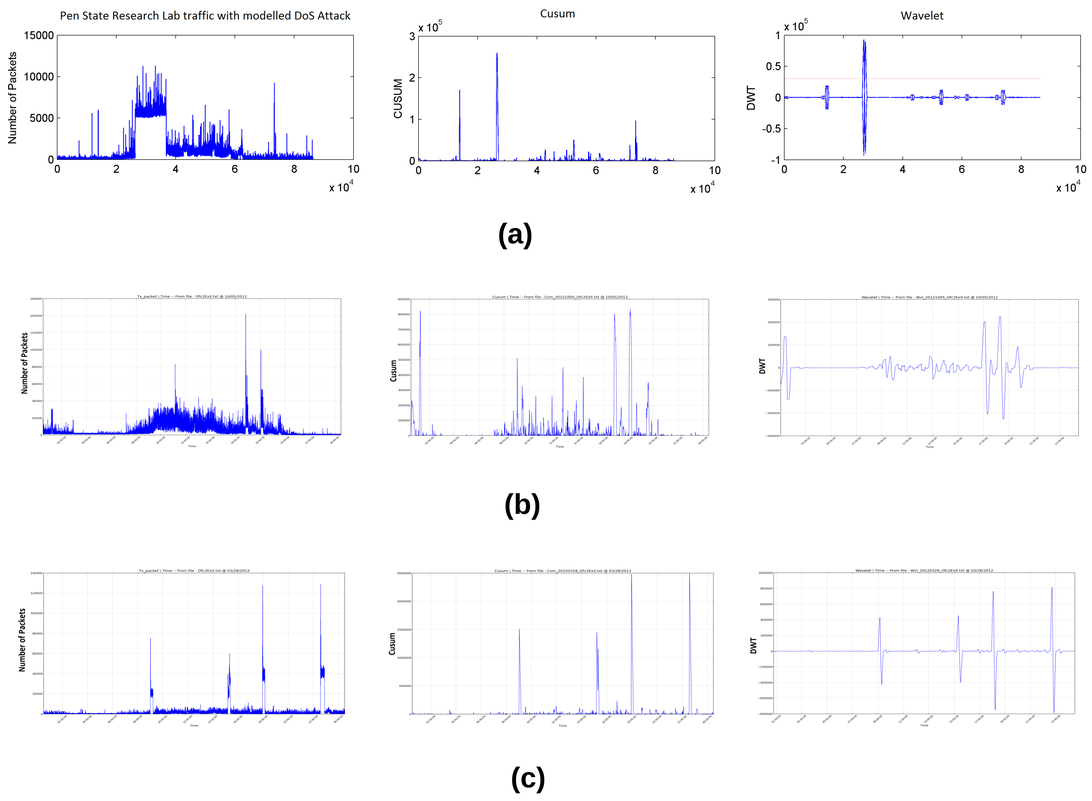

Fig 4. Detection results (a) Pen State firewall data with modeled attack, its cusum and wavelet (b) Clemson Uni. Network traffic with DDoS attack , its cusum and wavelet – port speed 100Mbps (c) Clemson Uni. Network traffic with DDoS attack, its cusum and wavelet – port speed 1000Mbps

Publications

I. I. Ozcelik and R. R. Brooks, “Operational system testing for designed in security,” in Proceedings of the Eighth Annual Workshop on Cyber Security and Information Intelligence Research, CSIIRW ’12, (New York, NY, USA), ACM, 2012(Accepted).

II. I. Ozcelik and R. Brooks, “Performance Analysis of DDoS Detection Methods on Real Network,” in 1th GENI research and educational experiment workshop, Los Angeles, CA, March 2012.

III. I. Ozcelik and R. Brooks, “Security experimentation using operational systems,” in 7th Annual Cyber Security and Information Intelligence Research Workshop, Oakridge,TN, October 2011

geni Exploring Networks of the Future
National Science Foundation WHERE DISCOVERIES BEGIN