DDoS Attacks on Plant/Controller Networks

Kyle Marlin – Youngstown State University
Mentors: Dr. Suzanna Schmeelk, Blaine Nelson, and Saurabh Amin

Introduction

In my research, I designed an internal attack on a network using the DETERlab Testbed (1). The team emulated a scaled version of the Abilene backbone topology, as well as the background traffic associated with it and designed a remote power plant/controller setup. The team broke into three groups of scientists: the infrastructure group, software development group, and my group, the attack group. Our group developed the attacks and set up ways of monitoring their progress. These attacks were based on a Distributed Denial of Service attack (DDoS) (2) from the inside of the topology.

The Abilene Topology

The Abilene Topology is an Internet2 high-performance backbone network which enables development of several advanced network applications and enables the deployment of leading-edge network services by the Internet2 universities and research laboratories. (3)

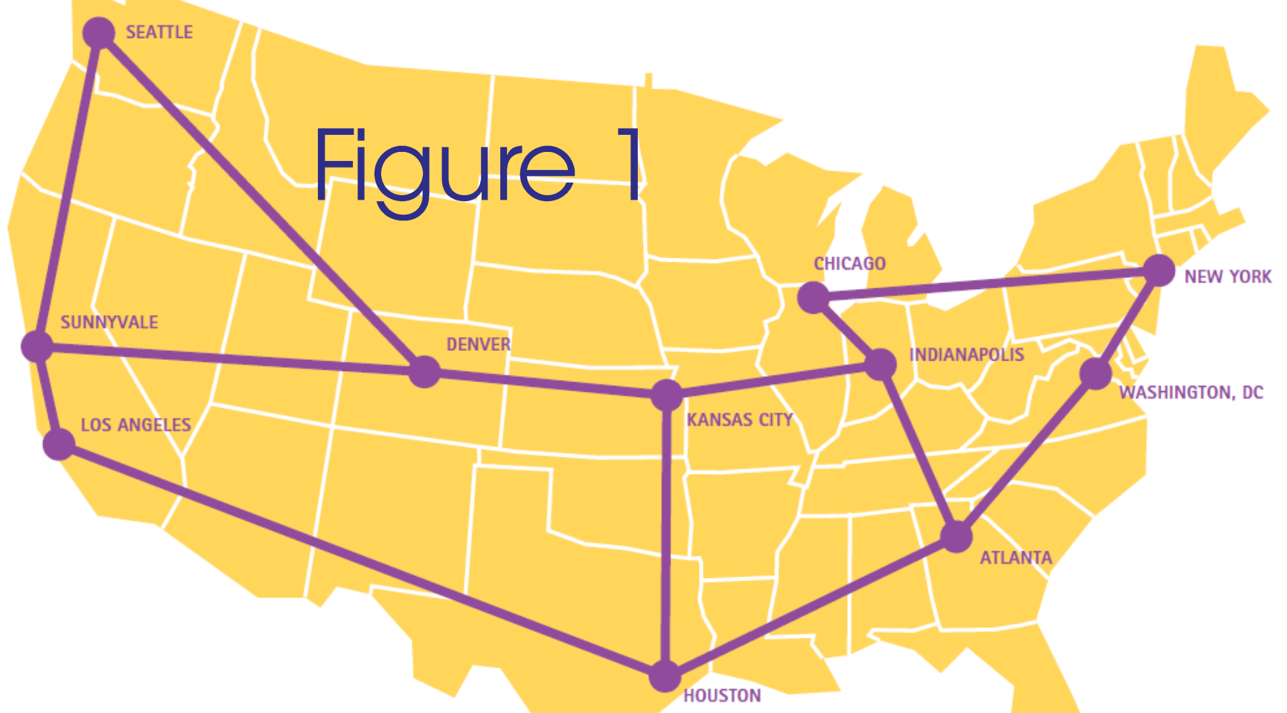


Figure 1 (left) shows a map of The Abilene Topology, according to Internet2 (3). Figure 2 (below) shows the network topology with backbone and external nodes.

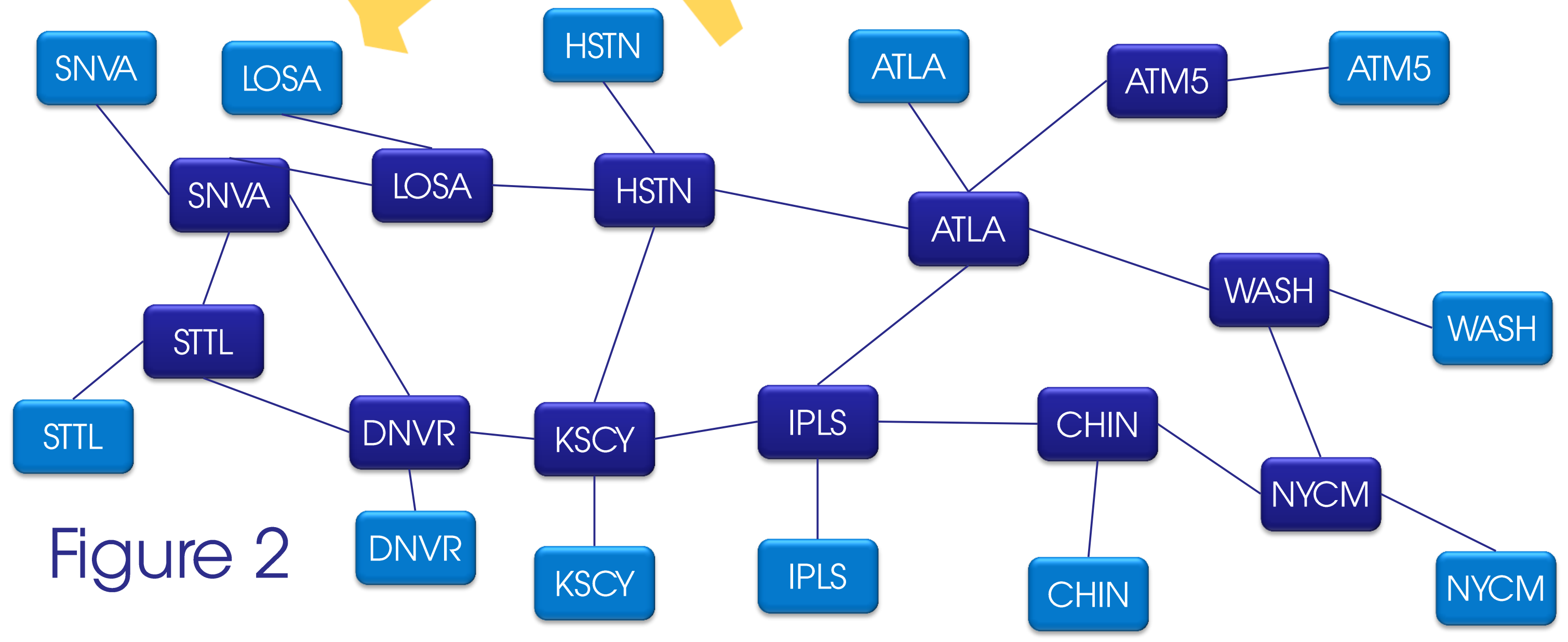


Figure 2

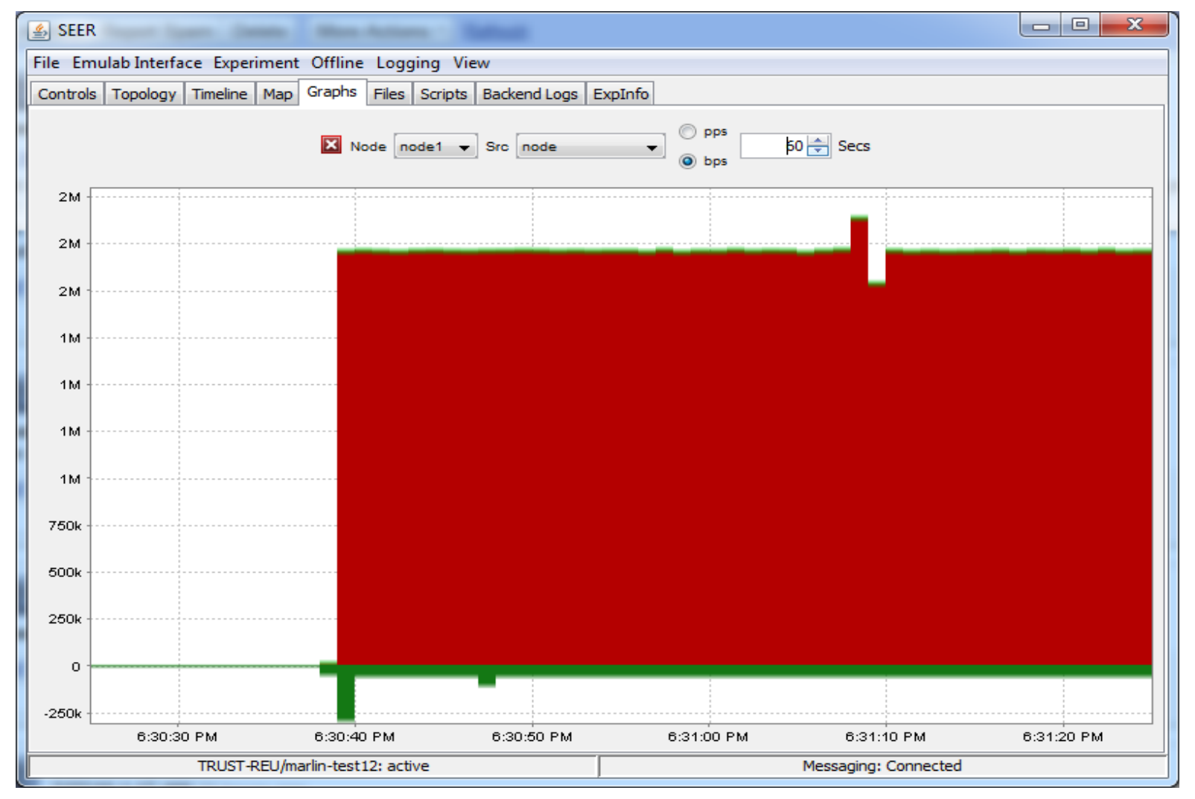


Figure 3: Flood

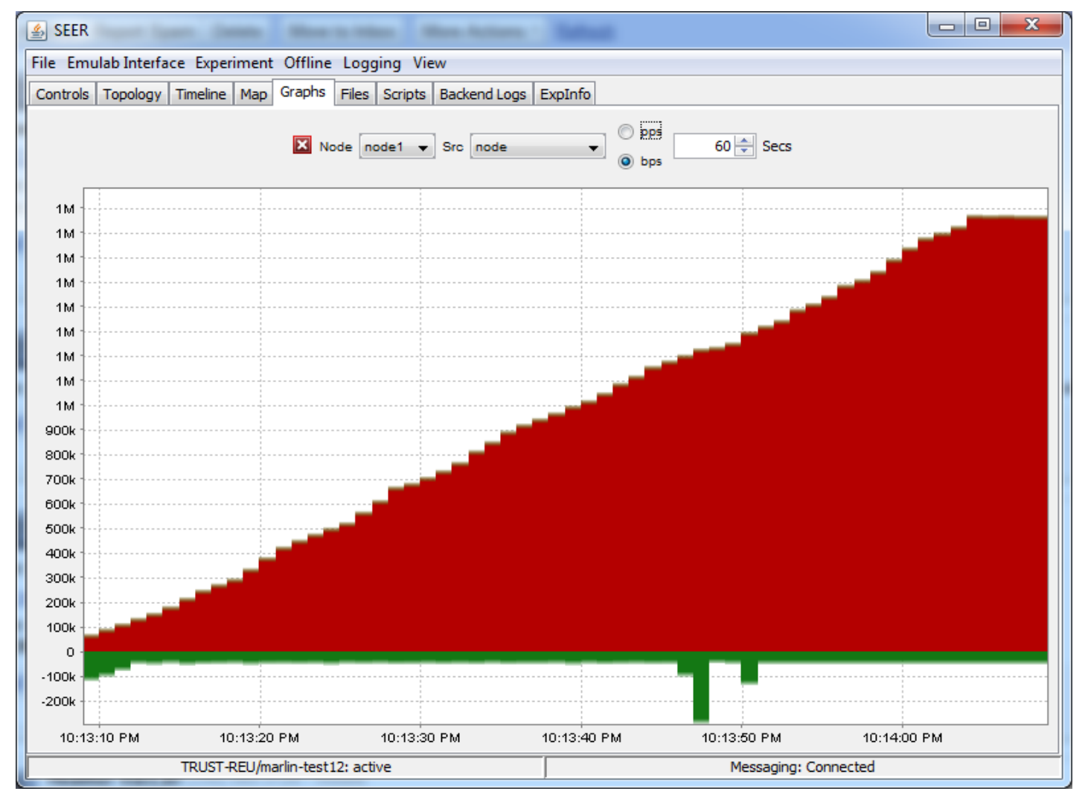
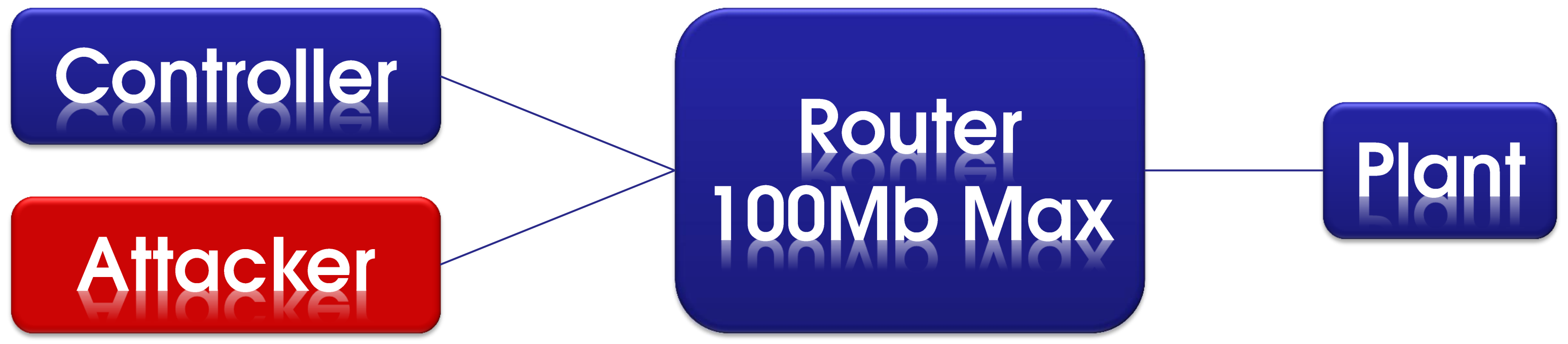


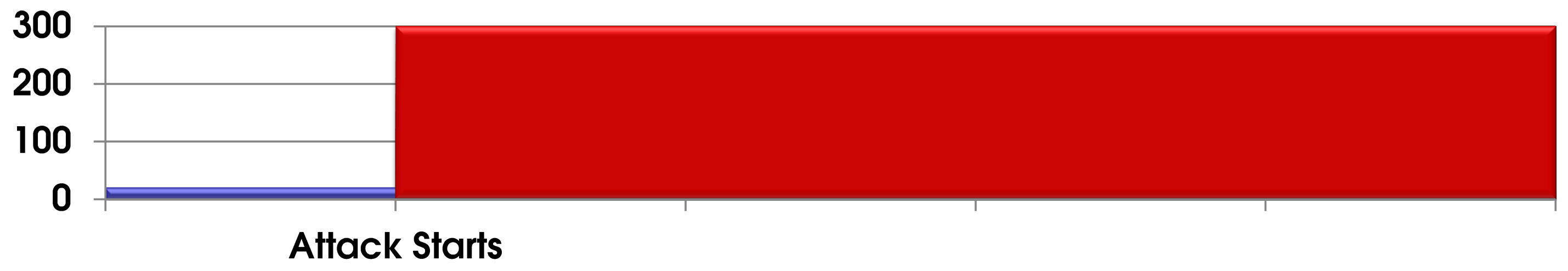
Figure 4: Ramp-up

Types of Attacks



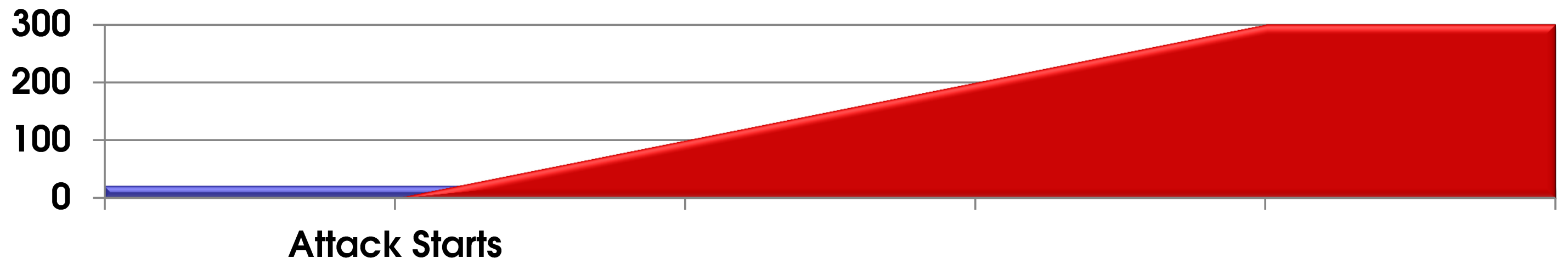
Legend for graphs below:
🟦 Plant/Controller Communication 🟥 Attack Traffic

Flood Attack: An attacker attacks with 300Mb of traffic. This overwhelms the 100Mb max router and it cannot process data from the controller. See Figure 3 for more information.



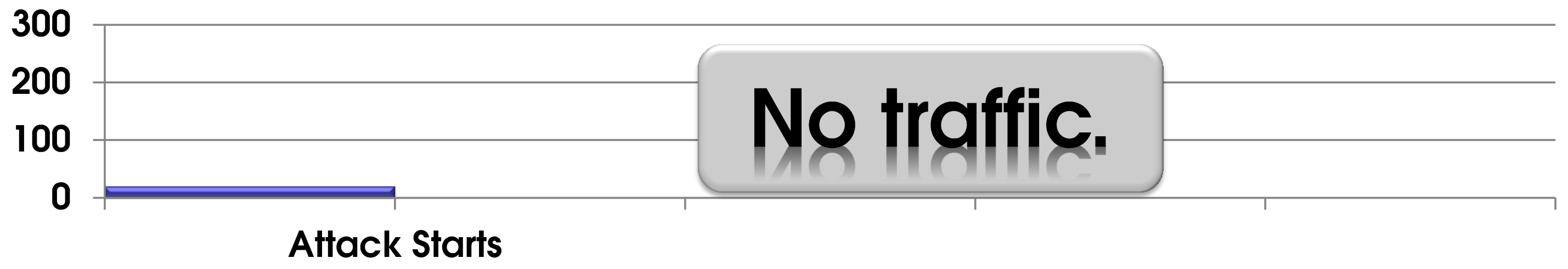
```
TCL Code: $cbr1 set packetSize_ 500
          $cbr1 set rate_ 300Mb        #Flood here
          $cbr1 attach-agent $tcp0
```

Ramp-up Attack: An attacker attacks with a small, steadily increasing flow of traffic, until this is above the router's limit, in which case, it cannot process data from the controller. See Figure 4 for more information.



```
TCL Code: $cbr1 set packetSize_ 500
          $cbr1 set interval_ 0.9   #Ramp-up Here
          $cbr1 attach-agent $tcp0
```

Cut-link Attack: An attacker attacks the link between the controller and plant, and severs the link between these nodes.



```
TCL Code: $ns at 60.0 "$link0 down"
```

All of these attacks resulted in a successful destruction of the plant. Without the control data from the controller, the plant will become unstable and fail every time.

Methodology

The network communication and attack occurs when:

1. Plant sends information to controller.
2. Controller responds with data.
3. Attacker attacks using one of currently three methods.

Conclusion

Attack experiments conducted on the scaled version of the Abilene Topology reflected expected results. In the plant/controller setup, attacks managed to destroy the plant every time. The project was to create plant and controller software and to apply that to the Abilene Topology. Background traffic was also successfully generated by analyzing several weeks' worth of archived data dumps.

Future Work

The next phase of my project would include perfecting the plant and controller software by allowing it to return actual variables, similar to an actual plant/controller scenario. Additionally, I would like to have varying attacks, so attacks can vary in nature. Proposed attacks would include worms, viruses, trojan horses, and other types of malware.

References

(1) University of Southern California USC Viterbi School of Engineering Information Sciences Institute. (2010, August 24). *DETERlab Testbed* (Online). Available: http://www.isi.edu/deter/

(2) CERT. (2001, June 4). *Denial of Service Attacks* (3rd ed.) (Online). Available: http://www.cert.org/tech_tips/denial_of_service.html

(3) Internet2. (2005, February). *Abilene Network* (Online). Available: http://www.internet2.edu/pubs/200502-IS-AN.pdf

Acknowledgements

I would like to thank the Team for Research in Ubiquitous Secure Technology (TRUST), Dr. Kristen Gates, Sally Alcala, Larry Rohrbough, Ted Faber, Jelena Mirkovic, the DETERlab team, The University of California, Berkeley, as well as the National Science Foundation (NSF) for funding the program. Additionally, I would like to thank my mentors: Dr. Suzanna Schmeelk, Blaine Nelson, and Saurabh Amin. Special thanks also to my groupmates: Katherine Gabales, Ricardo Estrada, and Darrel Brower.

This work was supported by the TRUST Center (NSF award number CCF-0424422)