Plant-Controller Attacks via Cut-Link and Flooding Attacks

Katherine R. Gabales
Computer Science – Math and Science Option
California State University, Chico
kgabales@mail.csuchico.edu

Graduate Mentors: Mr. Saurabh Amin, Mr. Blaine Nelson, and Dr. Suzanna Schmeelk
Research Supervisor: Dr. Kristen Gates
Faculty Mentor: Dr. Larry Rohrbough

July 30, 2010

TRUST Research Experiences for Undergraduates (TRUST-REU)
In Cyber Security and Trusthworthy Systems 2010

Department of Electrical Engineering and Computer Sciences
College of Engineering
University of California, Berkeley

Simple-Topology Attacks via Cut-Link and Flooding Attacks

Katherine Gabales

ABSTRACT

In an emulated environment, learning the basic interaction and strategies for attack and defense of control systems and detection systems are vital in building a stronger infrastructure for it can minimize the possible number of intrusions. Emulating routing and traffic on a large-scale network, in this case the Abilene Network Topology, will provide insights of possible effects caused by sample attacks placed within the system. DDOS attacks concerning cut-link attack and flooding attack were implemented to test the strength of the provided nodes, which are the plant and controller. The DETER research was divided into three phases to perform the following task: build infrastructure of the network, deploy the learning based DoS detection algorithm and test for attacks, and explore defenses that will allow for the learning system to be more resilient to attacks. The main purpose of the attacks is to record the amount of time when a plant/controller node stops connecting to other to which nodes it is connected.

KEYWORDS: DoS Attack, DDoS Attack, Cut-link, Flooding, network traffic, DETER, SEER, Abilene, Plant, Controller

I. INTRODUCTION

A. Cyber Threats and Issues

Cyber-threats occurring in cyber-network urge advancement in security. Rapid advances are urgently needed to defend against network attacks such as distributed denial of service, worms, and viruses [1]. The complexity of new attacks develops accordingly to technological advancement. As dependence on IT and the Internet grow, governments should make proportional investments in network security, incident response, technical training, and international collaboration [7]. It is only a matter of time when one can develop an improved attack before one can ever think of how to counter such attack. Thus, to avoid any kind of network loss, further research relating cyber-security is needed to maximize protection against growing cyber-attacks and minimize the impacts of successful attacks.

B. DETER Testbed, Abilene Network Topology Emulation, and SEER

The cyber-DEfense Technology Experimental Research network (DETER network) provides an infrastructure network, tools, and supporting processes for large-scale experimentation on merging security research and advanced development technologies [4]. Via DETER, an emulation of the Abilene network topology was created and tested using Distributed Denial-of-Service (DDoS) attacks. The DETER testbed was used in tandem with the Security Experimentation EnviRonment (SEER), a set of tools and agents for helping an experimenter setup, script and perform experiments in the DETER environment [8]. It was through SEER that the actual graphic representations of the attacks were accessible and examined. Agents for traffic generation, attack generation, traffic collection and analysis were also available through SEER allowing a thorough observation of the normal traffic compare to the traffic that was modified and affected by an attack [8].

C. DoS and DDoS Attacks

A denial-of-Service (DoS) attack is when a malicious user exploits the connectivity of the Internet to cripple the services offered by a victim site, often simply by flooding a victim with many requests [9]. A DoS attack is a single source attack, while the multiple source attack is called the Distributed Denial-of-Service attacks (DDoS).

Two types of DoS attacks, Cut-link Attack and ICMP Flood Attack, were constructed to test the strength of the Abilene network topology and to later determine the appropriate kind of defenses needed to sustain the health of the network. Cut-link Attack merely cuts the connection between the client and the server, while the ICMP Flood Attack [flooding attack] overwhelms the internet connection by sending the victim packets faster than it can manage [10].

II. BACKGROUND

A. Abilene Network Topology

Abilene is an Internet2 high-performance backbone network that enables the development of advanced Internet applications and the deployment of leading-edge network services by Internet2 universities and research laboratories across the country [5]. The emulation of the Abilene network topology is composed of 12 nodes, each representing a router that has only a few highs bandwidth connection [6].

Figure 1. shows the backbone topology of the Abilene Network. The nodes [cities] are as follows: Seattle, Sunnyvale, Los Angeles, Denver, Kansas City, Houston, Chicago, New York, Washington, DC, Indianapolis, and 2 nodes in Atlanta. The emulation of the Abilene network via DETER testbed included external nodes of each of the stated cities.

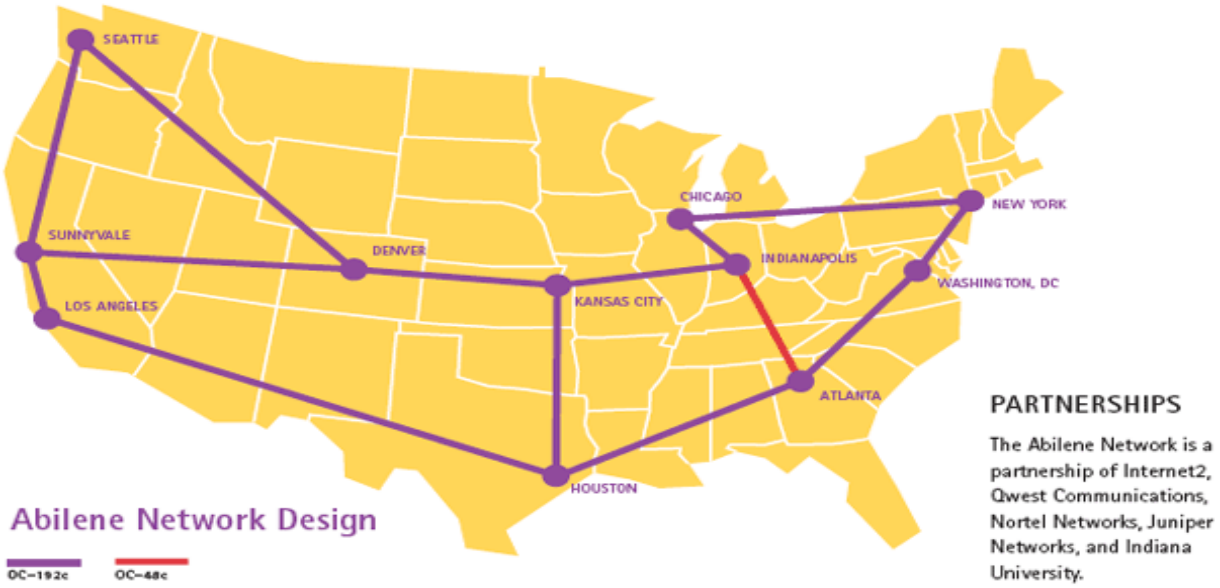

Figure 1. Abilene Network Backbone by www.ixbt.com

III. METHODS

A. Construction of Simple Plant-Controller Topology

Attacking the Abilene topology appeared highly impractical which lead to the construction of a simpler topology. Several created topologies simpler than the Abilene topology were created, each composed of nodes ranged from three up to six numbers of nodes. For each experiment, there is at least a Plant node [or client node], a Controller

node [or server node], and an attacker node; the number of Plant nodes varied by experiment. The Plant nodes are the victims of attacks, while the Attack nodes are the sources of the attacks.

The connections between the nodes were either a duplex-link or a make-lan through a switch. Duplex-link permits two nodes to simultaneously talk to each other—like a regular phone call. Alternatively, switch is a connection device in which multiple nodes can communicate to each other—like a conference call.

B. DDoS Attacks on Simple Plant-Controller Topology via SEER tool

Organizing attacks on a simpler and smaller topology reduced the observation complexity since there were fewer nodes to monitor simultaneously. Attacking via SEER illustrated events that can be expected once the actual attack-coding started. SEER provided graphical presentation of the topologies showing graphs of normal and under attack traffic.

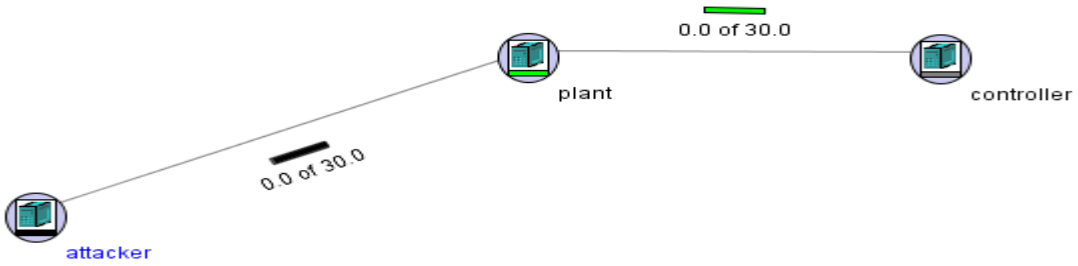

Figure 2. Simple Plant-Controller Topology. Plant node pinging Controller

Figure2 shows the basic part of a simple topology that has a Plant node, a Controller node, and an attacker node attached via duplex-link. The green bar underneath the Plant node indicates that it is alive and well. The green bar on the link connecting the Plant and the Controller signify a healthy connection between the two nodes.

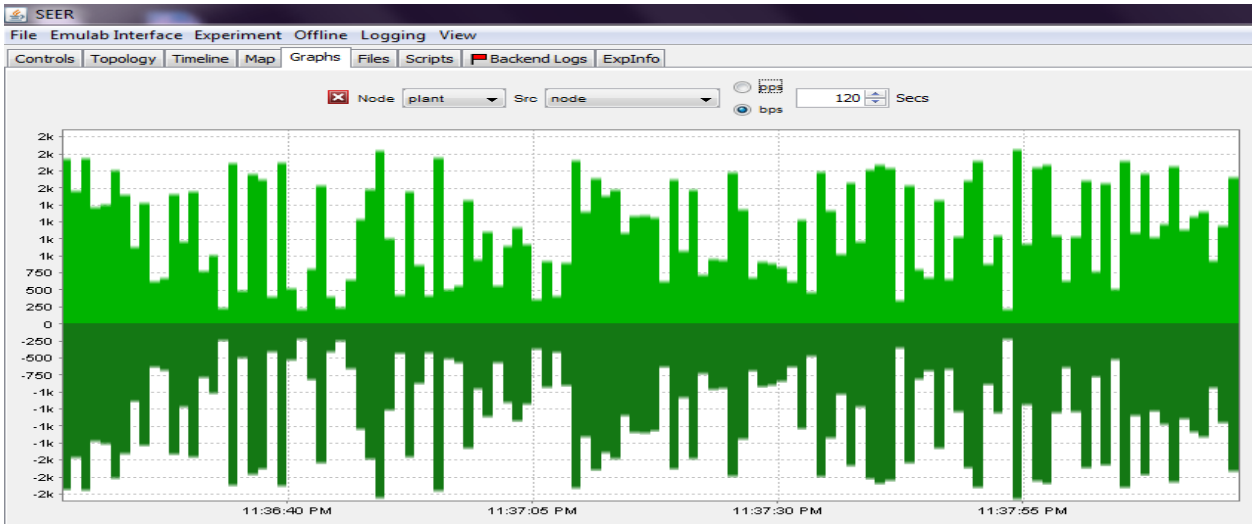

Figure 3. Graph of Plant-Controller Topology. Plant node pinging Controller node

Figure3 shows an undisturbed traffic between Plant and Controller node via green graphs as time elapsed; provided that the traffic remained uninterrupted, the graph shall remain green. The horizontal values [x-axis] represents elapsed time, while the vertical values [y-axis] represent the total number of bandwidth assigned; the positive values on y-axis represents the incoming traffic, while the negative values represents the outgoing traffic.

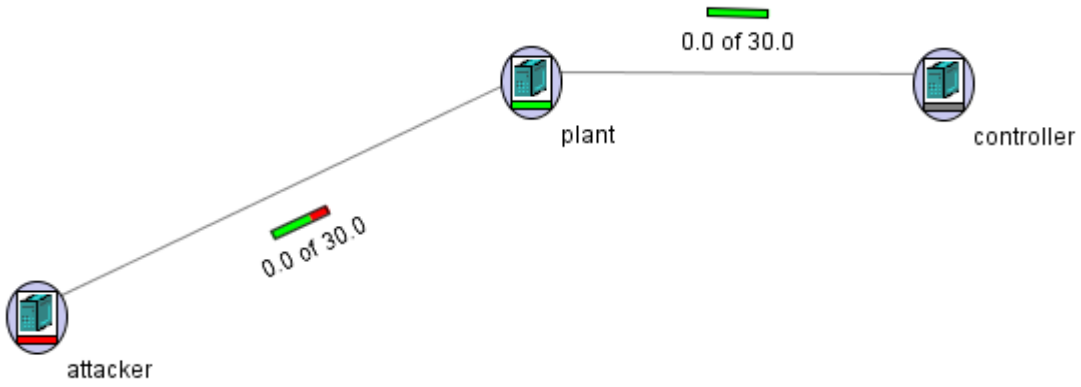

Figure 4. Simple Plant-Controller Topology. Attacker node attacking Plant node

Figure 4 is similar to **Figure 2** except that the Attacker node has been activated and that it is performing an attack to the Plant node. The colored [green and red] bar represents the ratio of the normal to attack traffic occurring between the Attacker and Plant node.

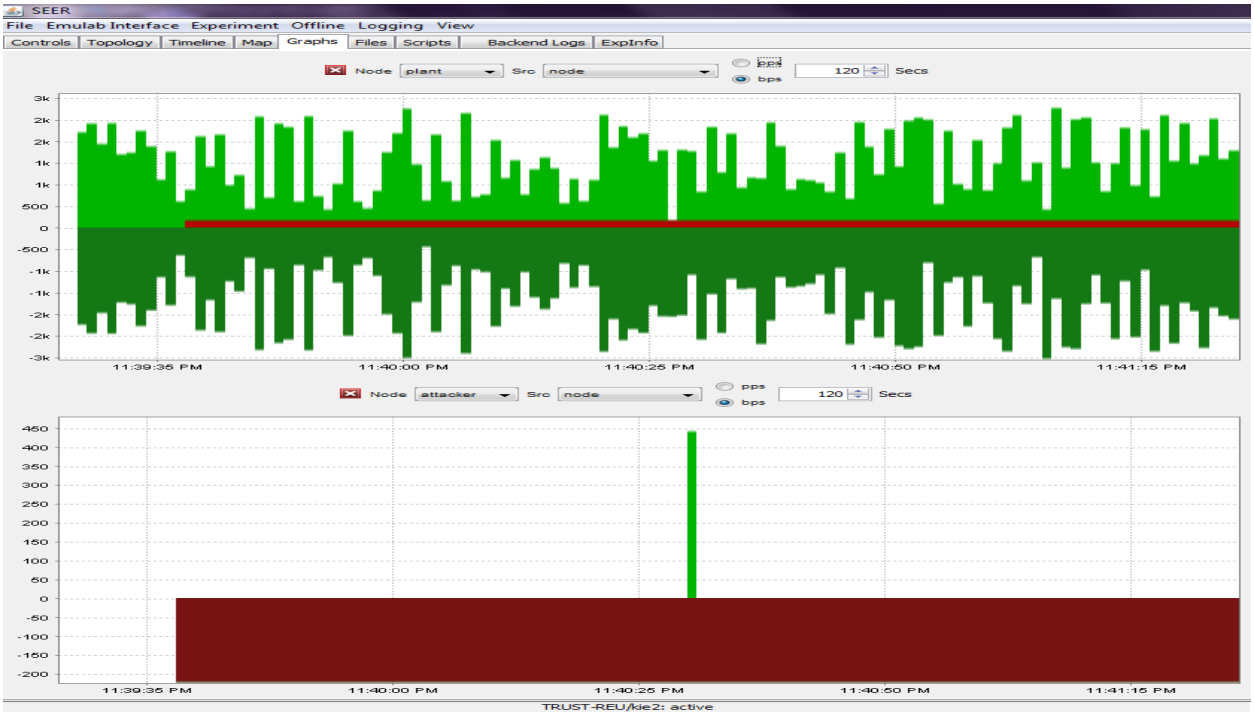

Figure 5. Graph of Simple Plant-Controller Topology. Attacker node attacking Plant node

Figure 5 displays a graphic representation of the traffic that is simultaneously shown over a period of time. The red graph illustrates that the normal traffic has been interrupted by an attack. Plant node has incoming [ingress] traffic of attacks, and outgoing [egress] traffic of interrupted traffic; it is interrupted since a gap is apparent between the green graphs. In addition, the Attacker node only has outgoing traffic of attacks since it is the source of the attack.

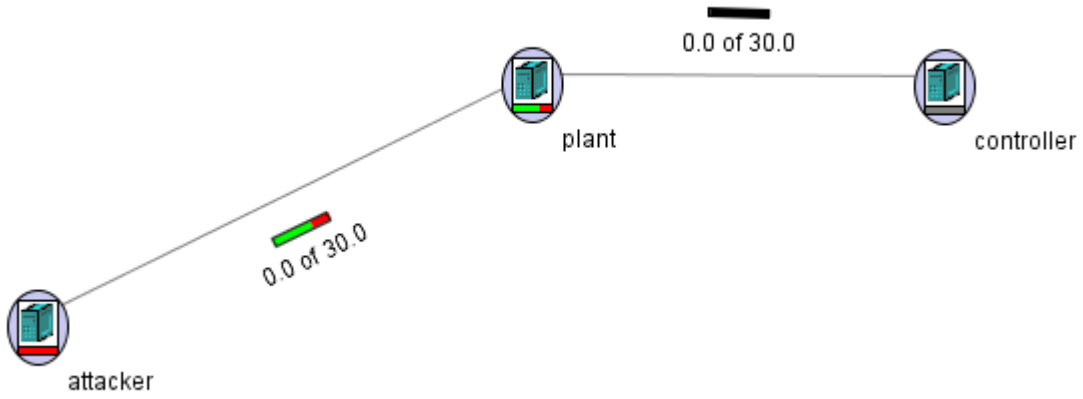

Figure 6. Simple Plant-Controller Topology. Attacker node attacking Plant node diminishing connection between the Plant and the Controller node

Figure 6 shows a black bar link on the Plant and the Controller node indicating loss of connection between the two nodes due to the flood attack that the Attacker performed.

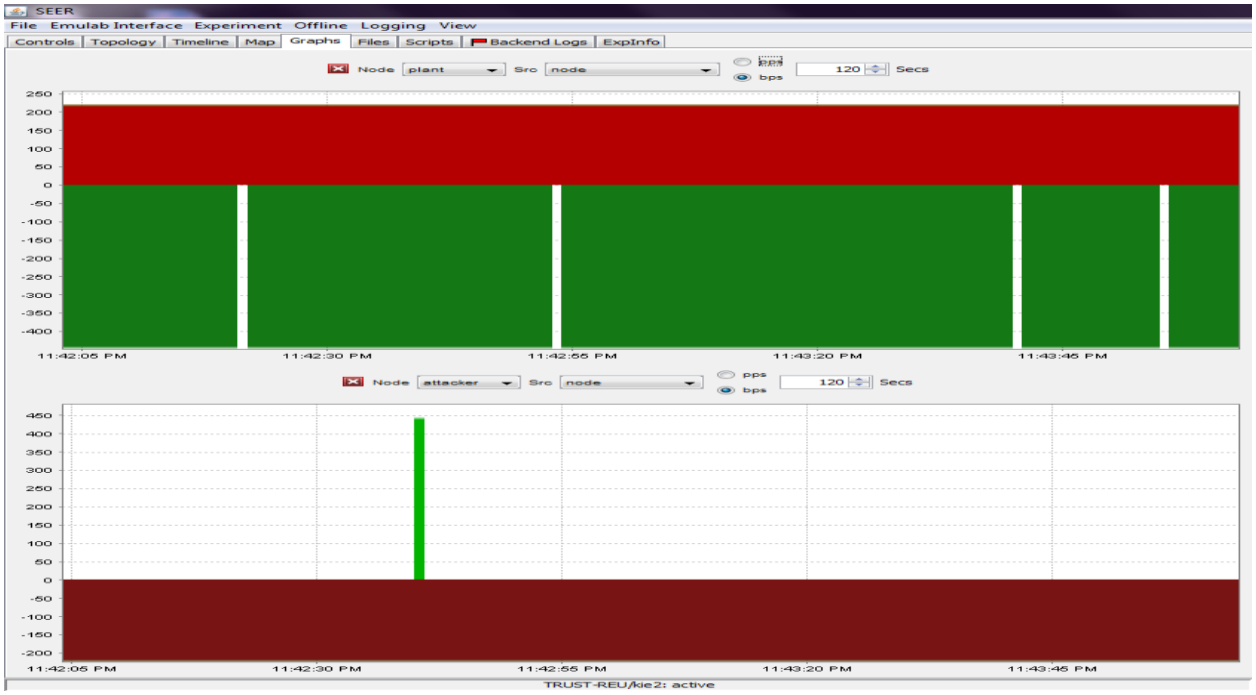

Figure 7. Graph of Simple Plant-Controller Topology. Attacker node overwhelmed Plant node.

Figure 7 demonstrates that the incoming traffic of the Plant node is flooded with attacks [red graph] and that no normal incoming traffic is visible.

In an experiment, there may be two additional colored graphs—excluding red and green. The colors are as follows: cyan graph color represents regular traffic that was not forwarded; and black graph color represents attack traffic that was not forwarded. Considering other experiments, there were multiple nodes serves as the sources of attacks, which in most cases were flooding attacks. The loss of connection between nodes depends on the speed of the bit rate. The higher the bit rate, the sooner a connection will diminish—and vise-versa for slower bit rate.

C. DDoS Attacks on Simple Plant-Controller Topology via Tcl

Tcl, pronounced tickle, is a scripting language available for free on a wide variety of platforms. It provides native "look and feel" GUI tools, and is a mature and stable technology [11]. Via Tcl, scripting a Cut-link attack took no more than three lines of code; and it operates upon the stated time for it to function. The Cut-link attack merely cuts the network connection of the victim prohibiting the victim node to function at a specified time. Once the specified time come the target node will simply loss connection to any network it was once connected. Additionally, Flooding attack took several lines of code since it ensures victims were overloaded with packets information. The Attacker node will send more packets than what a Plant node can handle. As time passes, the Attacker node will simply overwhelms the Plant node due to overloading packets until its connection dies.

IV. RESULTS

Cut-link and Flood attack scripts function efficiently via manual testing. The Controller node and Plant nodes were able to communicate with via Ping; also, packets were captured as **Figure 8** illustrates. After creating an attack, the traffic was interrupted and the connection between plants slowly diminished.

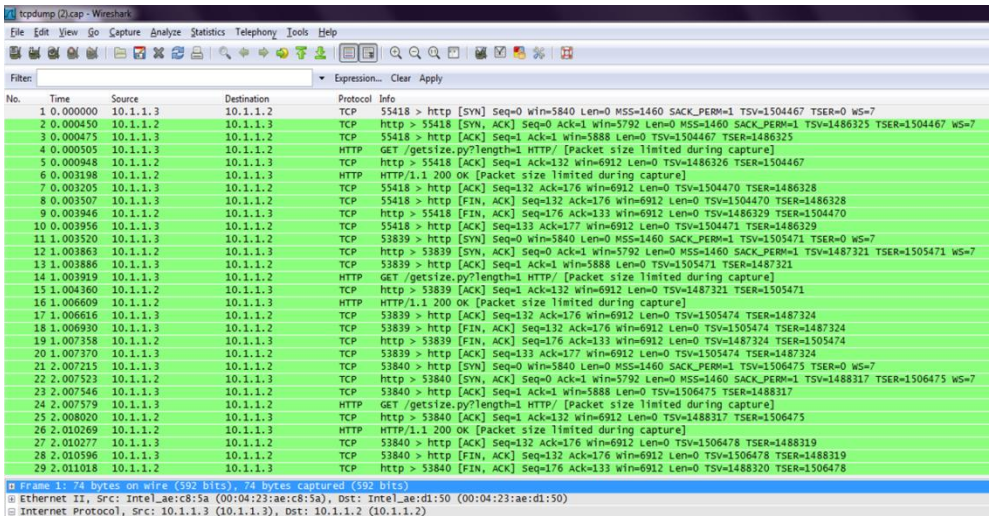

Figure 8. Captured packets between the Plant node and the Controller node

V. DISCUSSION

Upon making thorough research, new discoveries were accomplished. Learning Tcl and python were critical, as was learning the proper operation of the DETER testbed and the SEER tool. To assure that accurate findings were made, several experiments of different network topologies were created. For every topology, connections were checked via Ping to ensure that nodes were properly communicating to each other. Additionally, a collection of

packets was called via tcpdump viewed using Wireshark, which functions similarly to tcpdump, except it is known for its user-friendly graphical interface capabilities.

VI. FUTURE WORK

Automation of the Plant-Controller is a definite a must to do. Flooding attack must be polish to enable further complexity. Perhaps in the future, use it on Abilene network topology. To increase complexity use of the Abilene topology network, modification of the ns file is necessary to allow latter ease of use. An example is the modification of how each Abilene topology was individually created. Instead of manually assigning each node to a be connected to another node, consider using how a For Loop Statement to ease the connection of those who share the same characteristics. This indeed is a tough challenge since a careful study of how each is connected must be taken seriously.

VII. ACKNOWLEDGMENT

Thank you to those who made this research project a great learning and enjoyable summer experience. Thank you Dr. Kristen Gates, Dr. Larry Rohrbough, Dr. Suzanna Schmeelk, Saurabh Amin, Blaine Nelson, Ted Faber, Jelena Mirkovic, DETER cohort, TRUST-REU staff, TRUST-REU 2010 participants, University of California, Berkeley, and the National Science Foundation [award number: CCF-0424422].

VIII. LITERATURE CITED

[1] T. Benzel, R. Braden, D. Kim, C. Neuman, A. Joseph, K. Sklower, R. Ostrenga, S. Schwab. TridentCom2006. *Experience with DETER: A Testbed for Security Research". 2nd IEEE Conference on testbeds and Research infrastructures for the Development of Networks and Communities".*

[2] Cárdenas, Alvaro A., Ami,n Saurabh, and Sastry, Shankar. 2008. *Research Challenges for the Security of Control Systems*. In Proceedings of the 3rd. USENIX Workshop in Hot Topics in Security (HotSec)

[3] Marco Barreno, Blaine Nelson, Anthony D. Joseph, and J. D. Tygar. *The Security of Machine Learning. To appear in Machine Learning.* 2008

[4] R. Bajcsy, T. Benzel, M. Bishop, B. Braden, C. Brodley, S. Fahmy, S. Floyd, W. Hardaker, A. Joseph, G. Kesidis, K. Levitt, B. Lindell, P. Liu, D. Miller, R. Mundy, C. Neuman,R. Ostrenga, V. Paxson, P. Porras,C. Rosenberg, J. D. Tygar, S. Sastry, D. Sterne, S. F. Wu: Members of the DETER Projects and the EMIST Project. March 2008. *Cyber defense technology networking and evaluation*. Communications of the ACM, Vol 47, Issue 3. Pg. 58-61

[5] *Abilene Network*. Available at http://www.internet2.edu/pubs/200502-IS-AN.pdf

[6] Li Lun, David Alderson, Walter Willinger, John Doyle. 2004. *A First-Principles Approach to Understanding the Internet's Router-level Topology*

[7] Geers, K. 2009. The Cyber Threat to National Critical Infrastructures: Beyond Theory. Inf. Sec. J.: A Global Perspective 18, 1 (Jan. 2009), 1-7. DOI= http://dx.doi.org/10.1080/19393550802676097

[8] DETER SEER Wiki. 2010. http://seer.isi.deterlab.net/trac

[9] Alefiya Hussain, John Heidemann, Christos Papadopoulos. Feb 2003. A Framework for Classifying Denial of Service Attacks.

[10] Internet Relay Chat flood. May 2009. Available at http://en.wikipedia.org/wiki/Internet_Relay_Chat_flood

[11] Martin C. Calisle, Patrick Maes. 1998. *RAPID: A Free, Portable GUI Design Tool.* Proceedings of the 1998 annual ACM SIGAda international converence on Ada. Washington, D.C. Pp. 158-164