Proceedings of the 2017 Winter Simulation Conference
W. K. V. Chan, A. D'Ambrogio, G. Zacharewicz, N. Mustafee, G. Wainer, and E. Page, eds.

SIMULATING DDOS ATTACKS ON THE US FIBER-OPTICS INTERNET INFRASTRUCTURE

Sumeet Kumar
School of Computer Science
Carnegie Mellon University
5000 Forbes Ave
Pittsburgh, PA 15213, USA

ABSTRACT

In November of 2017, a DDoS attack tried to bring down the Internet connectivity of the African nation of Liberia. It was reported that the attacks consumed over 500 Gbps bandwidth of the Africa Coast to Europe (ACE) fiber cables that provide the Internet to Europe and Africa. The incident highlights the vulnerabilities that exist in the Internet infrastructure. We need a simulation testbed that can reflect the complexity of the Internet, yet allows to swiftly test attacks, providing insights that can apply to real-world attack scenarios. In this research, we try to identify such vulnerable points using a simulation. This work summarizes our original work on 'Simulating DDoS Attacks on the US Fiber-Optics Internet Infrastructure' accepted as a full paper at the Winter Simulation Conference, 2017.

1 INTRODUCTION

Though network based cyber-attacks like DDoS appear to be a growing phenomenon, there is no clear understanding of where the attacks are coming from, how the attacks are organized, and how the attack targets are identified. Also, the precise impact and maximum possible damage of such attacks are usually not known. However, one thing is clear that the bandwidth used in these attacks are increasing with time. In a recent example of the cyber-attack on the African nation of Liberia in Nov 2016, when thousands of bots targeted the fiber-optic cable exchange point (IXP), attempted to bring down the Internet connectivity of the entire country. Another example is the 2007 attack on Estonia, which crippled the Estonia's government web-services for a few weeks. These incidents highlight the serious nature of such attacks and call for policies to counter them, and ways to understand and control them (Kumar and Carley 2016). In this research, we propose a simulation test-bed to estimate the impact of such attacks.

The important contributions of this research are: a) We design a simulation testbed mirroring the fiber-optics Internet architecture of the US. To the best of our knowledge, this is the first work that simulates DDoS attacks on a realistic US cyber infrastructure. b) We present a model to estimate the degradation in the quality-of-service and the number of users impacted in different attack scenarios. To make our simulation more realistic, we use a dynamic packet flow algorithm that changes the Internet traffic flow pattern with congestion. c) Our model enables to find cyber installations that are more vulnerable to attacks.

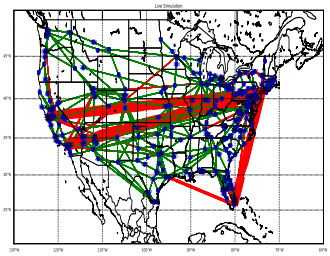
2 METHODOLOGY AND EXPERIMENTS

We use an agent-based network simulation approach to simulate cyber-attacks. Our simulation environment comprises of a network of connected Internet Exchange Points (IXPs) as nodes and Internet packet traffic as flow. The simulation is modeled as a dynamic network flow problem. On the Internet, the movement of packets change path as a portion of the Internet gets congested, and hence we use a dynamic network flow approach that uses Dijkstra algorithm to find paths of network flow. To test the simulation, we

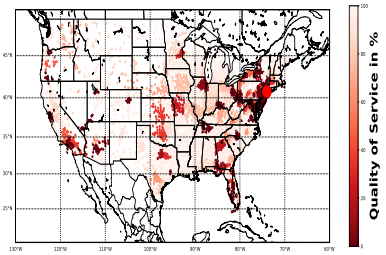
tried to simulate two different DDoS attacks. Please check Kumar and Carley (2017) for more details on methodology and algorithm used.

3 RESULTS AND DISCUSSIONS

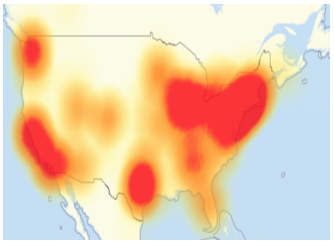
In one of the simulations, we selected the New York city IXP as the target of attack. This attack tries to simulate the DYN server attack that happened on Oct 21, 2016. In Fig. 1a, the width of edges indicate the network flow through the optical fibers, and the color indicates the congestion level. As the bandwidth of attack is increased in each iteration, more and more edges (optical-fibers) showed congestion. This is as expected in an attack. However, the edges that got more congested were not always close to the target. In fact, two of the most congested links are actually connecting the west coast areas, and one of the links is connecting the southern part of the US. This is a result of the dynamic nature of simulation. Figure 1b shows the result of the final stage of simulation (max bandwidth of attack). Figure 1c shows the actual impact as reported by downdetector website for comparison.



(a) Simulation Scenario 1: Visualizing the congestion in the network while an attack on the DNC INC New York city service.



(b) Simulation result for attack. The color bar indicates the relative impact in different areas.



(c) Actual impact as reported by DownDetector website. The red areas are most adversely impacted.

Figure 1: DYN attack Simulation: For DYN outage on 21th Oct, we compare the result of simulation to actual impact as reported by DownDetector website.

In this research, we designed and implemented a network simulation model to understand the Internet traffic flow pattern in a DDoS attack situation. The traffic flow visualization enabled us to find the edges (fiber-optic cables) that are more prone to congestion in case of an attack. We also used real data from downdetector.com website to compare both simulation results and found a reasonably good similarity.

4 ACKNOWLEDGMENTS

This work was supported in part by the ARL under Award No. W911NF1610049, DTRA Award No. HDTRA11010102, MURI Award No. N000140811186.. The views and conclusions contained in this document are those of the authors only.

REFERENCES

Kumar, S., and K. Carley. 2017. “Simulating Attacks on the US Fiber Optics Internet Infrastructure”. In *Proceedings of the 2017 Winter Simulation Conference*. Las Vegas.: Institute of Electrical and Electronics Engineers, Inc.

Kumar, S., and K. M. Carley. 2016. “Approaches to Understanding the Motivations behind Cyber Attacks”. In *Intelligence and Security Informatics (ISI), 2016 IEEE Conference on*, 307–309. IEEE.