**PROJECT PROPOSAL**

COURSE: MGS 655: Distributed Computing, Professor: Dr. Haimonti Dutta

**TITLE: DDOS (Distributed Denial of Service)**

TEAM: **Suvir Singh** (50161742)

**Potuluri Reddy** Ganta (Raj) (50166764)

DATE: September 22, 2015

Motivation: Why is this an interesting problem?

DDOS attacks are not something new. They have been bothering almost every organization regardless of its size, regardless of its awareness towards security protocols. This attack has evolved with time and till date there is no full proof solution for these kind of attacks. Hence the motivation is to understand it, simulate it and try to find a solution to prevent it in our controlled simulated setup.

During the course, we would like to form clear answers to the following questions:

Question 1: What are the different types of DDOS attacks? How much is the threat involved in each of them?

Question 2: What are the prevention mechanisms that are currently in place and how far they have been able to mitigate DDOS?

Question 3: How is DDOS carried in a peer to peer network? How does it takes the advantage of the vulnerabilities of the local nodes and what does it do with it?

Question 4: How is DDOS carried in cloud, or any other network topology?

General Approach:

We will try to use the peer to peer simulator present in the lab and try to create a cluster to nodes and then we will try to create a botnet in that cluster, controlled by a master node. Using this botnet we may force the remaining nodes to leave the cluster by flooding them. Going forward the outgoing innocent nodes may be allowed to add into the botnet and hence thereby increasing the infected cluster.

Sources:

<http://www.cs.bham.ac.uk/~tpc/cwi/Teaching/MASPPapers/BittorrentDoS.pdf>

<https://www.cloudflare.com/ddos>

<http://ddos-protection-services-review.toptenreviews.com/>

<http://www.arbornetworks.com/attack-ddos>

<http://www.cisco.com/c/en/us/products/collateral/security/traffic-anomaly-detector-xt-5600a/prod_white_paper0900aecd8011e927.html>

<http://www.rroij.com/open-access/analysis-of-ddos-attacks-in-distributed-peer-to-peer-networks-10-16.pdf?aid=37554>

<http://publications.lib.chalmers.se/records/fulltext/122264.pdf>

Tentative Schedule:

DDOS attacks study, feasibility analysis:

R&D on Peer to Peer Simulator, Cloud Networks:

Intermediate report:

Implementation of DDOS on a cluster:

Proposing defense mechanism:

Final Project: