ABSTRACT

This is an extraordinary challenge to trace back the source of Distributed Denial-of-Service (DDoS) attacks in the Internet. In DDoS attacks, attackers generate a huge amount of requests to victims through zombies with the aim of denying normal service or degrading of the quality of services. It has been a major threat to the Internet since year 2000. It was found that the peak of 40-gigabit DDoS attacks nearly doubled in the recent time as compared to the year 2000. However, the memory-less feature of the Internet routing mechanisms makes it extremely hard to trace back to the source of these attacks. As a result, there is no effective and efficient method to deal with this issue so far. Two of the major DDoS attack traceback methods(PPM and DPM) in use have many disadvanages and limitations such as high memory resource usage, vulnerability to hacking (through packet pollution) and requirement for frequent updating of routers. In a project a novel traceback method for DDoS attacks is proposed, that is based on entropy variations between normal and DDoS attack traffic, which is fundamentally different from commonly used packet marking techniques. DDos attack traceback by entropy variation method is designed and implemented using information entropy theory concepts. Victim and routers use packet flow variations to compute local variations during non attack periods. Huge entropy variations can be detected in DDoS attack period which can be traced back through successive upward communication till the router next to the attacker identifies the attack flow and it's IP. In comparison to existing DDoS traceback methods, the proposed strategy possesses a number of advantages - it is memory non-intensive, efficiently scalable, robust against packet pollution and independent of attack traffic patterns. The results of extensive experimental and simulation studies are presented to demonstrate the effectiveness and efficiency of the proposed method .DDos attacker IP address is traced back with in 30-45 seconds of attack under the experimental conditions used. This method is flexible to reduce false positive and false negative detection errors.

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompanies the successful completion of any task would be incomplete without the mention of the people who made it possible. Many are responsible for the knowledge and experience that we have gained during our project and throughout the course. Hence, we feel that expressing our deepest gratitude is just not formality but a part and parcel of the project.

We would also like to express our gratitude towards our honourable principal **Dr. M.K. Venkatesha** for facilitating all of us to pursue a project as per our choice and giving us all the inspiration and support.

We are highly indebted to **Dr. G T Raju ,** Professor and Head, Dept. of CS & E, for his consent and wholehearted cooperation in providing all the facilities and resources that we had required for successful implementation of this project.

We would first like to express our earnest thanks towards our project guide, **Mrs. Suneetha H. Angadi ,** Asst. Professor, Dept of CS & E. She is the motivator, guide and constant source of knowledge and inspiration for us towards the preparation of this project. We would also like to thank **Mr. Devaraju B. M.,** Asst. Professor, Dept. of CS & E for his encouragement and support throughout this project work.

Last but not the least, we thank all our friends who helped us directly or indirectly during this project and made it successful. At the same time, we thank all our faculty and lab assistants of the Computer Science and Engineering Dept., for their kind co-operation.

Gautam Prakash
M. Harish Rao
Pratik Dixit