

Topic of interest:

DDoS

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or persons to prevent an internet site or service from functioning efficiently. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even rootname servers.

I have decided to submit a **research paper** on the topic of tracing back the DDoS attacks using a probabilistic marking algorithm, as a research paper is an individual work and would give me more exposure to explore the topic in detail.

Tracing Back The DDoS Attacks Using A Probabilistic Marking Algorithm

There is currently an urgent need for effective solutions against distributed denial-of-service (DDoS) attacks directed at many well-known Web sites. Because of increased sophistication and severity of these attacks, the system administrator of a victim site needs to quickly and accurately identify the probable attackers and eliminate the attack traffic. This work is based on a probabilistic marking algorithm in which an attack graph can be constructed by a victim site. We extend the basic concept such that one can quickly and efficiently deduce the intensity of the “local traffic” generated at each router in the attack graph based on the volume of received marked packets at the victim site. Given the intensities of these local traffic rates, we can rank the local traffic and identify the network domains generating most of the attack traffic. We study the traceback and attacker identification algorithms. We also provide a theoretical framework to determine the minimum stable time t_{min} , which is the minimum time needed to accurately determine the locations of attackers and local traffic rates of participating routers in the attack graph. Extensive experiments are carried out to illustrate that one can accurately determine the minimum stable time t_{min} and, at the same time, determine the location of attackers under various threshold parameters, network diameters, attack traffic distributions, on/off patterns, and network traffic conditions.