Abstract

The increase in Internet-based transactions and communications offers new opportunities for hackers to disrupt business operations with DDoS attacks. Organizations that are not adequately protected risk losing customers, revenue, and their good reputations. This thesis discusses the challenges of identifying, countering, and avoiding crippling DDoS attacks. With the proposed comprehensive Self-Defending Network, organizations can deploy layers of defense to detect and mitigate the effects of DDoS attacks. The convenience, efficiency, and global reach of e-business benefit both consumers and businesses. But the accessibility of today’s business operations brings increased security challenges. Legions of malicious hackers target e-commerce sites, online banks, partner networks, and Internet or e-mail servers seeking revenge or profit.
DDoS attack quickly overwhelms a company's server, router, firewall or network link with traffic, if successful, the attack floods the network or its resources so completely that legitimate traffic cannot be processed, and the company cannot function. The results are disastrous frustrated customers place orders elsewhere, service-level agreements are violated, and corporate reputations are damaged. Meanwhile, all IT and security resources focus on responding to the attack. Unfortunately, their efforts are usually too late and only partially effective. A security strategy must instantly identify and respond to DDoS threats, while maintaining the availability of critical network resources for custoers, partners, and employees.

The proposed model develops counter mechanism to mitigate the potency of the resource attacks and evaluate the efficacy. The proposed access matrix captures the spatial-temporal patterns of a normal flash crowd. The anomaly detector based on hidden Markov model (HMM) is proposed to describe the dynamics of Access Matrix (AM) and to detect the attacks. Numerical results based on real Web traffic data are presented to demonstrate the effectiveness of the proposed method. Asymmetric attack overwhelms the server resources, by increasing the response time of legitimate clients from 0.1 seconds to 10 Seconds. Under the same attack scenario, HMM model limits the effects of false-negatives and false-positives and improves the victims' performance to 0.8 seconds.

Reference


**Index Terms**

Computer Science  
Security

**Key words**

Traffic Ddos  
Am  
Hmmm  
Self-Defending Network