Abstract

Security attack is the most import issue that is always the focus among professionals and practical engineers, going with the fast development of Internet in the past two decades. And Denial of Service (DoS) has been the prevalent attack that causes serious threats to Internet and information security. It tries to disrupt the normal operations of targeted system with numerous deliberate requests and packets which will consume the limited basic resources, like progress control blocks, pending network connections, and network bandwidth. The aim of this thesis is to provide a deep insight for the performance of system under DoS attacks.

Usually, it is hard to apply the mathematical models in analysis of DoS attacks. Either it is too complicated to set up a mathematical model, or it is impossible to obtain the analytical solution. On the other hand, it is time consuming and costs us much to observe and analyze the real performance of the victim server in the real case, or in the test bed. It motivates us to adopt simulation method to simulate the real situation.

In this thesis, we propose a queueing model to specify the system performance under the most prevalent SYN-flooding attack, with reference different parameters and different situations, such as arrival rate, traffic rate, the length of timeout, the maximum capacity of system, the standard deviation and the distribution of the service time. We obtain some effective quantitative measurements (e.g. loss probability of regular request, utility for regular request or attack, and utility for whole server) and analyze the performances of the server under various conditions.