ABSTRACT

Denial of Service (DoS) attack is the process of limiting the service provided by a particular server in a working environment to its valuable user. There are number of daemons available for performing the above task. Daemons are the compromised systems used in the process of prevention of the service. Eventhough many researches are in progress in order to identify the Denial of Service process, there exist some of the user promoting the attack steps. The service interruption is carried out by those users are identified with the help of any technique. The main objective is to detect the attack and make the system into a secure one. The attack process comprises of the steps such as, attack initiator who plays the role of attack process initialization followed by the daemons who helps the initiator to progress the attack process. The compromised daemons then follow the commands issued by the initiator to block the service provided to the intended user.

Jammers are the devices used to block the signals which are all in the category of the attack process. Jammer helps to prevent the entry of large volume of signals into the system and allow certain signals which are under through investigations. The Birth-Death process in the random process is taken into account for the detection and counting of the incoming and outgoing signal from and to a particular network. The usage of the network resources and its measure are calculated by using the total number of signals present in the current environment.

The jammer plays the role of decision making whether the particular signal from a particular sender is supposed to allow or deny in the working environment. The new entry of the signal into the system is considered as birth of the signal and the signal which drops below certain level is termed as death signal. The birth and death signals are arrived randomly in the system environment. Based on the arrival, the birth and death

process happens. This thesis proposes a Denial of Service attack detection method by combining the mathematical concepts and using the technological term called jammers. The Birth-Death Random Analysis for Denial of Service Attack in Distributer Wireless Networks by Distributed Jammer Network is presented. Here the number of incoming and outgoing signals are identified by Birth-Death Random Process. Also the Position occurrence or presence of the jammer is detected using the random variable. The jammers are placed in the network to monitor the distributed traffic flow. The system performance is analyzed based on the assumption that the birth and death rate are randomly varied in the system. Here the assumption is made such that the possible rates are equally distributed. The performance of the system is measured by using the simulator and identifies the protocols involved in the denial process. Hence the resultant system is free from the external hackers and intruders.