ABSTRACT

For a decade Denial of Service attack (DoS) or Distributed DoS (DDoS) is still a scourge for the world's major sites and government's sites. For years of study related to different types of DoS attack is conducted, several variants known as a SYN Flood, Ping Flood / Ping of Dead, UDP Flood, ICMP Flood, etc.

In this study the author research on a new variant called Low-Rate TCP-Targeted Denial of Service or "Shrew Attack" which took advantage of the weakness of Retransmission Tiome Out (RTO)mechanism on TCP (New Reno and Vegas in particular). This is important because this type of DoS detection is difficult. It has rare frequency of attack flow and also perform synchronization based on the value of RTO. The method used to minimize the impact of attacks carried out on the end – point is RTO randomization. One objective of this research to prove the efficacy of this method to anticipate the attacks of low-rate TCP-targeted denial of service.

This simulation uses FTP as TCP's traffic data and CBR as UDP's traffic to create attack pulse. As a measure for the TCP policy against attack, is by comparing the value of Quality of Service in the form of end to end delay, jitter, packet loss and throughput both in normal circumstances without the attacks, with the attacks, and in a state of randomized RTO for each TCPs.

From the simulation results using NS-2:27 RTO was found that the use of randomization can reduce the adverse effect of the attack. Judging from the results of throughput, delay, packet loss, and jitter obtained behavior of each TCP flow control is different on different network models, as well as variations in the value of alpha and beta can influence the stability of TCP Vegas link utilization.

Keyword : *Denial of Sevice,low rate TCP-targeted DoS* (*Shrew Attack*), *Retransmission Time Out*