# ABSTRAK

Dalam dekade ini serangan berupa *Denial of Service* (DoS) atau *Distributed DoS* (DDoS) masih menjadi momok bagi situs – situs besar dunia dan juga situs – situs pemerintahan. Selama bertahun – tahun studi yang berkaitan dengan beragam tipe serangan virtual DoS dilakukan, sehingga saat ini dikenal beberapa variannya seperti *SYN Flood, Ping Flood / Ping of Dead, UDP Flood, ICMP Flood* dan lainnya.

Pada tugas akhir ini dilakukan studi dan penelitian mengenai varian baru serangan DoS yang dinamakan *low rate TCP-targeted Denial of Service* atau *Shrew Attack* yang mengambil keuntungan dari kelemahan mekanisme *Retransmission Time Out* (RTO) pada suatu TCP (khususnya New Reno dan Vegas). Hal ini penting dilakukan mengingat DoS jenis ini sulit terdeteksi karena memiliki frekuensi aliran serangan yang jarang dan juga melakukan sinkronisasi berdasarkan nilai RTO.

Metode yang dilakukan untuk meminimalisasi dampak serangan dilakukan pada sisi *end – point* dengan merandomisasi nilai RTO-nya. Salah satu tujuan tugas akhir ini dibuat untuk membuktikan keampuhan metode tersebut untuk mengantisipasi serangan *low-rate TCP-targeted denial of service*. Simulasi meggunakan paket data melalui FTP sebagai trafik dari TCP yang berfungsi untuk mengirim dan menerima paket informasi sebagaimana biasa dan trafik CBR dari UDP sebagai penyerang yang mengeksekusi *low-rate tcp-targeted denial of service.*

Sebagai tolak ukur kebijakan TCP terhadap serangan, ialah dengan cara membandingkan *Quality of Service* berupa *end to end delay, jitter, packet loss* dan *throughput* baik dalam keadaan berjalan normal tanpa serangan, dengan adanya serangan, dan dalam keadaan termodifikasi sesuai metode berdasarkan skenario yang ditentukan.

Dari hasil simulasi menggunakan NS-2.27 didapatkan bahwa penggunaan randomisasi RTO dapat mengurangi dampak buruk dari serangan. Dilihat dari hasil *throughput, delay, packet loss,*dan *jitter* didapatkan tingkah laku *flow control* tiap TCP berbeda pada model jaringan yang berbeda, serta variasi nilai alpha dan beta pada TCP Vegas dapat mempengaruhi stabilitas utilisasi link.



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