ABSTRAK

Perkembangan teknologi jaringan modern, khususnya melalui penerapan *Software-Defined Network* (SDN), memberikan fleksibilitas tinggi dalam pengelolaan lalu lintas data melalui pengendalian terpusat. Namun, arsitektur ini juga membawa tantangan keamanan baru, terutama terhadap serangan volumetrik seperti *Internet Control Message Protocol* (ICMP) *Flood*, yang dapat membebani *controller* dan menurunkan performa jaringan secara signifikan. Penelitian ini bertujuan untuk menganalisis penerapan algoritma *Support Vector Machine* (SVM) sebagai deteksi lalu lintas anomali, serta implementasi teknik *rate limiting* sebagai upaya mitigasi untuk menekan dampak serangan ICMP *Flood* pada SDN berbasis *POX Controller*. Simulasi dilakukan menggunakan emulator *Mininet* dengan skenario lalu lintas normal dan serangan tanpa mitigasi maupun dengan mitigasi, serta pengukuran parameter performa meliputi *packet length*, ICMP *count*, *packet loss*, dan *round-trip time* (RTT). Simulasi dilakukan menggunakan emulator Mininet dengan lima skenario serangan (2 penyerang tanpa mitigasi, 3-5 penyerang dengan mitigasi) dan intensitas serangan hingga 100.000 paket ICMP berukuran 5.000 byte dengan interval 1–2,5 ms. Hasil penelitian menunjukkan bahwa tanpa mitigasi, durasi gangguan pada jalur komunikasi mencapai 1.323 detik dengan *False Positive* (FP) hingga 23.134, menandakan sistem tidak mampu membedakan lalu lintas sah dari *flood*. Sebaliknya, dengan penerapan *rate limiting*, durasi lonjakan *delay* dapat ditekan menjadi hanya 45–94 detik, dan nilai FP menurun drastis ke kisaran 1.396–2.589. Selain itu, *packet loss* tetap berada di bawah 72%, dan akurasi deteksi SVM berada pada rentang 93,48%–95,82%, menandakan sistem mampu menjaga kestabilan jalur normal meski berada di bawah tekanan *flood*. Penerapan *rate limiting* terbukti mampu menurunkan laju serangan dan menjaga *traffic* normal tetap berjalan meski tingkat *packet loss* mencapai 45–72%. Hasil ini membuktikan bahwa integrasi deteksi SVM dan mitigasi *rate limiting* pada POX *Controller* efektif dalam menekan dampak serangan ICMP *Flood* tanpa mengganggu lalu lintas normal.

Kata Kunci — ***Software-Defined Network*, ICMP *Flood*, DDoS, POX *Controller*, *Rate Limiting*, Keamanan Jaringan**