ABSTRAK

Penelitian ini bertujuan untuk menyelidiki serangan *DDoS* di *SDN* menggunakan Shannon entropi dan metodologi *PPDIOO* serta konsekuensinya. Hal ini dimaksudkan untuk menentukan apakah *SDN* rentan terhadap serangan *DDoS* dan apakah entropi Shannon terbukti efektif dalam mengidentifikasi bentuk serangan tersebut. Penelitian ini berimplikasi lebih luas pada dinamika keamanan dan kinerja jaringan berlapis dalam menghadapi serangan *DDoS* dan beberapa skenario yang dilakukan pada jaringan *SDN* menunjukkan korelasi *DDoS* dan nilai entropi pada berbagai lintas data anomali. Kerangka *PPDIOO* memastikan bahwa model mengikuti urutan logis dalam mengidentifikasi tujuan, merencanakan dan merancang skenario serangan yang diikuti dengan penerapannya untuk memastikan konsistensi dalam pengumpulan data. Parameternya dapat dibagi lagi menjadi empat bagian dan akan merangkum keseluruhan kerangka serangan Studi ini menyoroti bagaimana serangan *DDoS* dapat dengan mudah menyusupi infrastruktur *SDN* sekaligus menyoroti bagaimana *Shannon entropy* dapat digunakan secara akurat untuk mengidentifikasi jenis serangan ini. Studi ini memberikan saran praktis untuk merancang mekanisme keamanan yang lebih kuat guna melindungi *SDN* dari serangan *DDoS* di masa depan.

Kata Kunci: *SDN*, *DDoS*, *Shannon Entropy*, POX *Controller*, *PPDIOO*.