ABSTRAK

Improving DDoS Detection using Entropy in SDN

Oleh Dani Prasetiawan

Dosen Pembimbing: Dr. Maman Abdurohman, M.T.

SDN (Software Designed Network) merupakan teknologi baru dalam konsep jaringan, dimana memisahkan data plane (hardware) dan control plane (software) yang bertugas sebagai otak yang mengatur forwarding suatu paket jaringan. Konsep baru ini mampu meningkatkan flexibilitas bagi administrator jaringan dalam perancangan dan pengoperasionalan suatu jaringan.

Selama beberapa dekade terakhir, serangan Distributed denial-of-service (DDoS) merupakan salah satu masalah keamanan jaringan. Secara umum, mekanisme deteksi serangan DDoS dapat dikenali, meskipun demikian pendeteksian merupakan hal yang sangat sulit karena kesamaan antara trafik normal dan trafik anomali yang dikirim oleh host yang telah dikompromikan untuk menyerang korbannya. Banyak metodologi untuk mendeteksi serangan DDoS yang ada pada jaringan tradisional, tapi untuk jaringan SDN masih jarang tersedia. Metode pendeteksian DDoS di SDN yang ada mendeteksi serangan DDoS dengan memanfaatkan *threshold* dari trafik yang lewat dengan rata-rata ukuran trafik dibandingkan dengan tiga kali nilai standar deviasi. Kelemahan dari metode ini adalah jika ada lonjakan traffik akan dideteksi sebagai serangan meskipun sebenarnya trafik normal sehinggan meningkatkan *false positive*.

Tujuan dari thesis ini adalah memanfaatkan controller (*OpenFlow controller*) dari SDN untuk mendeteksi serangan DDoS berdasar metode sebelumnya dengan menambah mekanisme pengecekan tingkat keacakan trafik. Setelag terdeteksi sebagai serangan oleh metode sebelumnya, maka akan dicek apakah *entropy threshold*-nya lebih tinggi dari parameter yang ditentukan maka dideteksi sebagai serangan DDoS. Dalam penelitian ini, terbukti bahwa metode baru dapat mengurangi *false positive*, ketika terjadi lonjakan temporer pada trafik normal maka tidak terdeteksi sebagai serangan DDoS

Keywords: SDN, Software Defined Network, DDoS Detection, Network Security