ABSTRACT

The topic of this thesis is about the construction of algorithms for application of anomaly detection methods in Software Defined Networking (SDN) aimed at detecting bots from botnet. Unlike in traditional networks, SDN monitors all status and network flow centrally by SDN controller. This feature can be utilized to facilitate detection of botnet attacks by separating traffic information based on source and destination address.

There are several detection methods for securing botnet attacks in traditional networks that cannot be directly applied to SDN that has different architectures with traditional networks. In general, network security research on SDN against botnet attacks focuses on detection frameworks alone without discussing detection algorithms and their detection results. Therefore, the author tries to build algorithms for detection of botnet attacks on the SDN.

Detection methods based on botnet behavior in this thesis, refers to the pattern and data flow of C&C communication traffic. The botnet traffic pattern is obtained based on botnet C&C traffic communication. By utilizing the hamming distance method, the traffic pattern can be described by labeling the lowest traffic with bit 0 and other traffic with bit 1. There is a possibility of error detection when normal traffic pattern resembles C&C communication traffic, this problem can be solved by applying detection based on data flow consisting of APR (Average Packet Rate) and APS (Average Packet Size).

As an experimental result, the detection performance based on anomaly behavior is able to detect above 90% of the presence of botnets in the SDN. On the other hand, Botnet attack detection algorithm has a weakness when facing background traffic that has high traffic variations with low average throughput and low number of packages.

Keywords: *SDN, Botnet, Anomaly Detection, Hamming Distance, APR, APS*