ABSTRACT

Internet has become an integral part of Life as provide up to date information, entertainment as well as facilitating communication, but if the user does not have the ability in operating computer and internet, it shall lead the threat on computer and server in the network, example anomaly traffic. There are many type of traffic anomaly, one of them is robot network (Botnet). Botnet is a collection of infected Program computer designed by botmaster. The purpose of botnet attacks usually stealing important data from internet users such as passwords, credit card information and so on.

In this study, author using hybrid algorithm (combining two methods), which are the self-similarity method and CUSUM algorithm. The Self-similarity method is used to review whether a traffic detect anomaly or normal. While the CUSUM algorithm is used to review the classification from botnet attacks. In the method of self-similarity, it needs Hurst Exponent value takes from R/S method. The estimation value help the author to hypothesized either the entry traffic is anomaly or normal by monitoring the H value. then the author analyzes the traffic graphic movement by using agregat process in self similarity parameter. CUSUM algorithm clasify the attack by finding the CUSUM value.

The results of final project is analyzing the natural characteristics of self-similarity method performance, in which the hurst exponent estimated value between 0.5 to 1 means normal dataset test and if the value outside the range means anomaly traffic. meanwhile CUSUM algorithm showed that the good performance in clasify the attacks based on accuracy, detection rate and false positive rate.

Keywords : BOTNET, CUSUM, Self Similarity, Hurst Exponent