Abstract

Software Defined Network (SDN) is a concept that allows the administrator to manage network devices via a controller software that can make configuration process via control plane easier. However, the security factor is considered in building a network. Basically there is no checking mechanism for malicious data packet on SDN network. Securing the network can be done by inspecting every packet of data over the network using Intrusion Detection System (IDS). However, it should be sought about how effective IDS to detect cyber attacks and its effect on SDN network's performance.

In this final project, integration of IDN on SDN network and measurement of its effect on performance has been done. Performance parameters that has been tested is the delay, throughput, jitter, and packet loss ratio. In addition, the network has been tested to detect specific cyber attacks.

From the results of tests, SDN network that has been integrated with IDS has the ability to detect cyber attacks in accordance with the applied rule so it has better security. However, SDN network after integrated with IDS has decreased in terms of performance compared to the network before integrated with IDS generally. This is because each data packet that passess will be checked according to the existing rule.

.

Keywords : *Software Defined Network*, *Intrusion Detection System*, performance, *cyber* attacks, *rule.*