Abstract

The Internet has become the platform of daily activities as a result of which threat of network attack has become more serious. Network Intrusion Detection Systems (NIDSs) are among the most widely-deployed security tools for detecting cyber-attacks and activities conducted by intruders for observing network traffics.

In this project we used flow based system to detect anomalous activity like scan and flood. Holt-Winters Prediction method and Entropy based method use the Extracted and Selected Feature and detect the attack. The Entropy and Holt-Winter methods are implemented independently to detect the attacks. The Report starts with an introduction to Intrusion Detection System. It further covers details of approach system and system implementation. And conclude with tests performed and results. The result is a system which indicate instances of aberrant behaviour as they occurs. This information help network operator to deal the situation.