2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)

Implementation of Anomaly Detection Algorithms for Detecting Transmission Control Protocol Synchronized Flooding Attacks

Nenekazi N. P. Mkuzangwe[1, 2], Andre McDonald[1] and Fulufhelo V. Nelwamondo[1, 2]

[1]Modelling and Digital Science, Council for Scientific and Industrial Research, Pretoria, South Africa
[2]Department of Electrical and Electronic Engineering, University of Johannesburg, Johannesburg, South Africa

Abstract

This work implements two anomaly detection algorithms for detecting Transmission Control Protocol Synchronized (TCP SYN) flooding attack. The two algorithms are an adaptive threshold algorithm and a cumulative sum (CUSUM) based algorithm. Furthermore, we fused the outcomes of the two algorithms using the logic OR operator at different thresholds of the two algorithms to obtain improved detection accuracy. Indeed, the results indicated that the OR operator performs better than the two algorithms in detecting SYN flooding attack and detection delay.