



Contribution ID: 7

Type: **Research Paper**

Improving the Performance of Network Intrusion Detection Based on Hybrid Feature Selection Model

Improving the Performance of Network Intrusion Detection Based on Hybrid Feature Selection Model

Abstract

Due to the high dimensionality of the network traffic data, it is not realistic for an Intrusion Detection System (IDS) to detect intrusions quickly and accurately. Feature selection is an essential component in designing intrusion detection system to eliminate the associated shortcoming and enhance its performance through the reduction of its complexity and acceleration of the detection process. It eliminates irrelevant and repetitive features from the dataset to make robust, efficient, accurate and lightweight intrusion detection system to be certain timelines for real time. In this paper, a novel feature selection model is proposed based on hybridising feature selection techniques (information gain, correlation feature selection and chi square). In this experiment the performance of the proposed feature selection model is tested with different evaluation metrics which includes: True Positive rate (TR), Precision (Pr), false positive rate (FPR), on NSL KDD dataset with four different classification techniques i.e. random forest, Bayes, J48, Parts. The experimental results showed that the proposed model improves the detection rates and also speed up the detection process.

Key words Intrusion detection, Performance, hybrid, feature selection, classifier.

Primary author: CHAHIRA, joseph (university)

Co-authors: THIGA, Moses (Kabarak University); Mr SIROR, joseph

Session Classification: Artificial Intelligence

Track Classification: Artificial Intelligence