Abstract

In today's world, increasing number of networks connected to the Internet poses a great challenge on security issues. Many defensive mechanisms exist and one such higher level mechanism is network intrusion detection system. Intrusion detection system is a process of intelligently monitoring the events in an individual system or network, analysing them for signs of violation of security policy. Two major classifications of intrusion detection systems are misuse and anomaly intrusion detection systems. Misuse detection system refers to detection of intrusions that follow well defined intrusion patterns. Anomaly detection model refers to detection performed by detecting changes in the behaviour of the system. Many data mining techniques like k-Nearest Neighbour (kNN), Association Rule Mining etc., have been applied to intrusion detection. This paper aims at application of kNN to a subset of records from the KDD Cup 1999 dataset for classification of connection records into normal or attacked data. The paper also applies kNN to the subset of records with the selected features proposed by Kok-Chin-Khor et al [5] to compare the classifications.
Application of k-Nearest Neighbour Classification Method for Intrusion Detection in Network Data

- Victor-Valeriu Patriciu, Liviu Rusu, Iustin Priescu, ”Data mining approaches for Intrusion Detection in Email system Internet-Based”, Military Technical Academy, 144-147, 2003.

Index Terms

Computer Science

Security

Keywords

Attacks  connection records  normal  testing dataset  training dataset
Application of k-Nearest Neighbour Classification Method for Intrusion Detection in Network Data