

Hybrid of fuzzy clustering neural network over NSL dataset for intrusion detection system

ABSTRACT

Intrusion Detection System (IDS) is one of the component that take part in the system defence, to identify abnormal activities happening in the computer system. Nowadays, IDS facing composite demands to defeat modern attack activities from damaging the computer systems. Anomaly-Based IDS examines ongoing traffic, activity, transactions and behavior in order to identify intrusions by detecting anomalies. These technique identifies activities which degenerates from the normal behaviours. In recent years, data mining approach for intrusion detection have been advised and used. The approach such as Genetic Algorithms , Support Vector Machines, Neural Networks as well as clustering has resulted in high accuracy and good detection rates but with moderate false alarm on novel attacks. Many researchers also have proposed hybrid data mining techniques. The previous researchers has introduced the combination of Fuzzy Clustering and Artificial Neural network. However, it was tested only on random selection of KDDCup 1999 dataset. In this study the framework experiment introduced, has been used over the NSL dataset to test the stability and reliability of the technique. The result of precision, recall and f-value rate is compared with previous experiment. Both dataset covers four types of main attacks, which are Denial of Services (DoS), User to Root (U2R), Remote to Local (R2L) and Probe. Results had guaranteed that the hybrid approach performed better detection especially for low frequent over NSL dataset compared to original KDD dataset, due to the removal of redundancy and uncomplete elements in the original dataset. This electronic document is a “live” template. The various components of your paper [title, text, tables, figures and references] are already defined on the style sheet, as illustrated by the portions given in this document.

Keyword: Artificial neural network; Fuzzy clustering; Intrusion detection system; KDDCup 1999; NSL KDDCup; Data mining