Rough Set Significant Reduction and Rules of Intrusion Detection System

Rohani Abu Bakar
Faculty of Computer System and Software Engineering, Universiti Malaysia Pahang

ABSTRACT
Intrusion Detection System deals with huge amount of data which contains irrelevant and redundant features causing slow training and testing process, also higher resource consumption as well as poor detection rate. It is not simply removing these irrelevant or redundant features due to deteriorate the performance of classifiers. Furthermore, by choosing the effective and important features, the classification mode and the classification performance will be improved. Rough Set is the most widely used as a baseline technique of single classifier approach on intrusion detection system. Typically, Rough Set is an efficient instrument in dealing with huge dataset in concert with missing values and granularing the features. However, large numbers of generated features reducts and rules must be chosen cautiously to reduce the processing power in dealing with massive parameters for classification. Hence, the primary objective of this study is to probe the significant reducts and rules prior to classification process of Intrusion Detection System. All embracing analyses are presented to eradicate the insignificant attributes, reduct and rules for better classification taxonomy. Reducts with core attributes and minimal cardinality are preferred to construct new decision table, and subsequently generate high classification rates. In addition, rules with highest support, fewer length, high Rule Importance Measure (RIM) and high coverage rule are favored since they reveal high quality performance. The results are compared in terms of the classification accuracy between the original decision table and a new decision table.

DOI: 10.3233/978-1-61499-637-8-65