Protocol-Based With Feature Selection in Intrusion Detection

游坤明,Ming-Feng Wu
Computer Science & Information Engineering
Computer Science and Informatics
yu@chu.edu.tw

Abstract

A lightweight network intrusion detection system is more efficient and effective for real world requirements. Higher performance may result if insignificant and/or useless features are eliminated, so choice a well feature selection method is important. Logistic Regression is one of powerful feature selection method. In this study, protocol type and Logistic Regression were used to pick up the feature sets and build different protocol detection model which can get surmount performance than the full feature using a Support Vector Machine. Evaluation was done over a benchmark dataset used KDD CUP'99. In terms of time efficiency,the proposed method performs more than seven times better than other feature selection methods.

Keyword：Intrusion detection, Logistic Regression, Protocol, Support Vector Machine