# Protocol-Based classification for Intrusion Detection

游坤明,Ming-Feng Wu,Wai-Tak Wong
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. Logistic Regression is one feature selection method. In this study, protocol type and Logistic Regression were used to pick up
the feature sets which can get nearly the same performance as 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