



A HYBRID METHOD FOR INTRUSION DETECTION WITH GA-BASED FEATURE SELECTION

ZHI-XIAN CHEN^{1,2} AND HAO HUANG¹

¹*State Key Lab for Novel Software Technology*

Nanjing University

Nanjing, Jiangsu, China, 210093

{czx_leo@126.com, hhuang@nju.edu.cn}

²*College of Electronics and Information Engineering*

Nanjing University of Technology

Nanjing, Jiangsu, China, 210009

ABSTRACT—Traditional intrusion detection techniques examine all features to detect intrusion or misuse patterns. But all features are not relevant and some of them may be redundant and contribute little to the detection process. Irrelevant and redundant features may lead to complex intrusion detection model as well as poor detection accuracy. In this paper, we propose and investigate a novel hybrid feature selection method to intrusion detection based on fusion of Extension Matrix (EM) and Genetic Algorithm (GA), which employs a combination of EM and GA through genetic operation, and it is capable of building an optimal detection model with only selected important features and their specific values. Experiment results show the achievement of high correct detection rates and tolerable low false positive rates based on benchmark KDD Cup 99 data sets.

Key Words: Intrusion detection; Genetic algorithm; Extension matrix; Feature selection; Network security