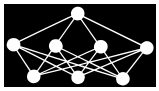

INTELLIGENT NETWORK-MISUSE-DETECTION-SYSTEM USING NEUROTREE CLASSIFIER

B. Muthukumar[*], *S.S. Sivatha Sindhu*[†], *S. Geetha*[‡], *A. Kannan*[§]

Abstract: Intrusion detection systems (IDSs) are designed to distinguish normal and intrusive activities. A critical part of the IDS design depends on the selection of informative features and the appropriate machine learning technique. In this paper, we investigated the problem of IDS from these two perspectives and constructed a misuse based neurotree classifier capable of detecting anomalies in networks. The major implications of this paper are a) Employing weighted sum genetic feature extraction process which provides better discrimination ability for detecting anomalies in network traffic; b) Realizing the system as a rule-based model using an ensemble efficient machine learning technique, neurotree which possesses better comprehensibility and generalization ability; c) Utilizing an activation function which is targeted at minimizing the error rates in the learning algorithm. An extensive experimental evaluation on a database containing normal and anomaly traffic patterns shows that the proposed scheme with the selected features and the chosen classifier is a state-of-the-art IDS that outperforms previous IDS methods.

Key words: *intrusion detection system, misuse detection, genetic algorithm, neural network, decision tree, neurotree*

Received: November 27, 2014 **DOI:** 10.14311/NNW.2015.25.027
Revised and accepted: June 6, 2015

1. Introduction

1.1 Motivation and misuse detection scenario

One of the biggest hurdles to having a secure and safe network is the large amount of human expertise and domain knowledge required to manage and at the same time non-availability of suitable personnel to man them. A mechanism that partially automates the network security management procedures, thus reducing the

[*]Balasubramaniam Muthukumar, Department of Information Technology, Syed Ammal Engineering College, Ramanathapuram, India

[†]Siva S. Sivatha Sindhu, Security Associate, Shan Systems, New Jersey, USA

[‡]Subbiah Geetha – Corresponding author, School of Computing Science and Engineering, VIT Campus Chennai, India, E-mail: geethabaalan@gmail.com

[§]Arputharaj Kannan, School of Information Science and Technology, Anna University, Chennai, India

