WUJNS
Wuhan University Journal of Natural Sciences

Vol.12 No.1 2007 147-150

Article ID: 1007-1202(2007)01-0147-04
DOI 10.1007/s11859-006-0258-z

# Learning Vector Quantization Neural Network Method for Network Intrusion Detection

☐ **YANG Degang[1,2], CHEN Guo[3], WANG Hui[4], LIAO Xiaofeng[1†]**

1. Department of Computer Science and Engineering, Chongqing University, Chongqing 400044, China;

2. Department of Mathematics and Computer Science, Chongqing Normal University, Chongqing 400047, China;

3. Department of Modern Educational Technology, Chongqing Normal University, Chongqing 400047, China;

4. Department of Mathematics, Leshan Normal College, Leshan 610043, Sichuan , China

**Abstract:** A new intrusion detection method based on learning vector quantization (LVQ) with low overhead and high efficiency is presented. The computer vision system employs LVQ neural networks as classifier to recognize intrusion. The recognition process includes three stages: ① feature selection and data normalization processing; ② learning the training data selected from the feature data set; ③ identifying the intrusion and generating the result report of machine condition classification. Experimental results show that the proposed method is promising in terms of detection accuracy, computational expense and implementation for intrusion detection.

**Key words:** intrusion detection; learning vector quantization; neural network; feature extraction

**CLC number:** TP 393

**Received date:** 2006-04-20

**Foundation item:** Supported by the National Natural Science Foundation of China (60573047), Natural Science Foundation of the Science and Technology Committee of Chongqing (8503) and the Applying Basic Research of the Education Committee of Chongqing (KJ060804)

**Biography:** YANG Degang (1976-), male, Ph.D. candidate, Associate professor of Chongqing Normal University, research direction: information security. E-mail:ydg42@163.com

† To whom correspondence should be addressed. E-mail:xfliao@cqu.edu.cn

## 0 Introduction

IDS is a system of monitoring and detecting data trace or user behavior to identify intruders. These are classified into two types: misuse detection and anomaly detection. Misuse detection is a method which intrusion pattern is hand-coded using expert knowledge for well-known attacks or weak spots of the system, then through matching and identifying these known intrusion, patterns or signatures to detect intrusion. Misuse detection has low false alarm because of its nature. But the main shortcomings of misuse detection are: known intrusion patterns have to be hand-coded; it is unable to detect any new or unknown attack that has no matched pattern stored in the system. Anomaly detection assumes that an attack will always reflect some deviation from normal patterns, which is designed to capture any deviations from the established profiles of the system normal behavior. Anomaly detection can detect new and unknown intrusion, but it has the shortcoming of false alarm rate.

The basic task of intrusion detection is to audit the log data of a computer, which includes network-based data and host-based