Network Intrusion Detection Based on Neuro-Fuzzy Classification

Adel Nadjaran Toosi  
Communication and Computer Research Laboratory, Faculty of Engineering, Ferdowsi University of Mashhad  
ad_na85@stu-mail.um.ac.ir

Mohsen Kahani  
Computer Department, Faculty of Engineering, Ferdowsi University of Mashhad  
kahani@um.ac.ir

Reza Monsefi  
Computer department, Faculty of Engineering, Ferdowsi University of Mashhad  
rmonsefi@um.ac.ir

Abstract—With rapid growth of computer networks during the past few years, network security has become a crucial issue. Among the various network security measures, intrusion detection systems (IDS) play a vital role to integrity, confidentiality and availability of resources. It seems that the presence of uncertainty and the imprecise nature of the intrusions make fuzzy systems suitable for such systems. Fuzzy systems are not normally adaptive and have not the ability to construct models solely based on the target system's sample data. One of the successful approaches which are incorporated fuzzy systems with adaptation and learning capabilities is the neural fuzzy method. The main objective of this work is to utilize ANFIS (Adaptive Neuro Fuzzy Inference System) as a classifier to detect intrusions in computer networks. This paper evaluates performance of ANFIS in the forms of binary and multi-classifier to categorize activities of a system into normal and suspicious or intrusive activities. Experiments for evaluation of the classifiers were performed with the KDD Cup 99 intrusion detection dataset. The Overall Results show that ANFIS can be effective in detecting various intrusions.

Keywords—Intrusion Detection, KDD dataset, Computer network Security, ANFIS, Neuro-Fuzzy classifier.

I. INTRODUCTION

During the past few years, the numbers of intrusions in computer networks have grown extensively, and many new hacking tools and intrusive methods have appeared. Using an intrusion detection system (IDS) is one way of dealing with suspicious activities within a network [1].

Soft computing and machine learning approaches have demonstrated their abilities in IDS, and there are continual interests in utilizing them in such systems [1] [2] [3] [4]. Fuzzy logic as a robust artificial intelligent method has been successfully employed for many IDSs [2] [3] [5] [6] [7].

Most Fuzzy systems make use of human expert knowledge to create their fuzzy rule base and hence, lack adaptation. However, elicitation of fuzzy rules from experts is usually difficult. Therefore, building fuzzy systems with learning and adaptation capabilities has recently gained much attention. Various methods have been suggested for automatic generation and adjustment of fuzzy rules without using aid of human experts; the neural fuzzy [8] [9] and genetic fuzzy [10] [11] are two most successful approaches in this regard.

From the classification point of view, the main work of building an IDS is to build a classifier which can categorize normal and intrusive event data from the original dataset. ANFIS can incorporate human expertise as well as adopt itself through repeated training. This ability among others qualifies ANFIS as a fuzzy classifier for IDS [8].

In order to promote the comparison of different works in IDS area, the Lincoln Laboratory at MIT, under the Defense Advanced Research Project Agency (DARPA) and Air Force Research Laboratory (AFRL/SNHS) sponsorship, constructed and distributed the first standard dataset for evaluation of computer network IDS [12].

The fifth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining collected and generated TCP dump data provided by the aforementioned DARPA in the form of train-and-test sets of features defined for the connection records (a connection is a sequence of TCP packets starting and ending at some well-defined times) which we name them as KDD cup 99 dataset [13] and will use it for our experiments.

Intrusion detection as a classifier mainly consists of two processes; training the classifier from a training dataset and using this classifier to categorize a test dataset. Hereby, we made use of neuro-fuzzy classifiers to detect intrusions in computer networks based on KDD cup 99 datasets.

The subsequent parts of this paper are organized as follows: Section 2 describes KDD Cup 99 dataset on which our experiments are conducted. Then the next section briefly outlines the basics of neuro-fuzzy concepts in general and ANFIS particularly. The proposed system and experimental results are discussed in sections 3 and 4, respectively. Finally, section 6 makes some concluding remarks and recommends areas for future research.

II. KDD CUP 99 DATA SET

The KDD cup 99 dataset includes a set of 41 features derived for each connection and a label which specifies the status of connection records as either normal or specific attack type. These features had all forms of continuous, discrete, and symbolic, with significantly varying ranges and fall in four categories [13]:

- The intrinsic features of a connection, which includes the basic features of individual TCP connections. For example, duration of the connection, the type of the protocol (tcp, udp, etc), network service (http, telnet, etc), etc.
- The content feature within a connection suggested by domain knowledge is used to assess the payload of the original TCP packets, such as number of failed login attempts.
- The same host features examine established connections in the past two seconds that have the same destination host as the current connection, and calculate statistics related to the protocol behavior, service, etc.

This work was partially supported by the Iran Telecommunication Research Center (ITRC).