Intrusion Detection Using Fuzzy Meta-Heuristic Approaches

Bachir Bahamida, Laboratory of Research in Artificial Intelligence, Alger, Algeria
Dalila Boughaci, Laboratory of Research in Artificial Intelligence, Alger, Algeria

ABSTRACT

Due to a growing number of intrusion events, organizations are increasingly implementing various intrusion detection systems that classify network traffic data as normal or anomaly. In this paper, three intrusion detection systems based fuzzy meta-heuristics are proposed. The first one is a fuzzy stochastic local search (FSLS). The second one is a fuzzy tabu search (FTS) and the third one is a fuzzy deferential evolution (FDE). These classifiers are built on a knowledge base modelled as a fuzzy rule “if-then”. The main purpose of these methods is to get the highest quality solutions by optimizing the fuzzy rules generation. The proposed classifiers FSLS, FTS and FDE are tested on the benchmark KDD’99 intrusion dataset and compared with some well-known existing techniques for intrusion detection. The results show the efficiency of the proposed approaches in the intrusion detection field.

Keywords: Deferential Evolution, Fuzzy Logic, Genetic Algorithm, Intrusion Detection, KDD’99 Dataset, Stochastic Local Search, Tabu Search

INTRODUCTION

These last years, the quantum of information is increasing exponentially on the internet, yet the massive growth of data should be protected and preserved.

In order to protect data and information exchange, several security tools were developed such as: firewalls, cryptographic systems, private virtual network, access control and secure protocols. However, all these strategies can’t insure a high level protection against intrusions attempts. This has led to the use of intrusion detection tools in order to get a monitoring permission.

The intrusion detection’s concept was first proposed by James Anderson in 1980 (J. P. Anderson, 1980). But, the works on this domain started effectively in 1987 with the publication of the model of intrusion detection (Denning, 1986).

An intrusion detection system can be a software application, hardware device or both of them designed to monitor all inbound and outbound network activity and identify any suspicious activities or policy violations that may indicate a network or system attack.

Intrusion detections methods can be divided into two main models: anomaly detection and misuse detection approaches.
The anomaly detection model is based on user’s profiles. It describes the usual behaviour of a user to detect his anomalous or unaccustomed action. Among these methods, we find: the statistical methods (Anderson et al., 1995), the expert systems (Vaccaro & Liepins, 1989) and the neural networks (Debar et al., 1992).

The misuse detection model is referred as signature based detection that analyzes susceptible data in order to detect any anomalous behaviour that can be attacks. Some well know works based on misuse detection are: the expert systems (Lunt & Jagannathan, 1988), the genetic algorithm (Ludovic, 1998) and the pattern matching method that recognizes attacks’ signatures. Various algorithms are used to localize these signatures in the audit trail (Kumar & Spafford, 1994).

In the last few years, various techniques have been applied extensively for intrusion detection such as the clustering techniques (Shah et al., 2003), neural networks (Ryan et al., 1998; Lee & Heinbuch, 2001), Bayesian approach (Amor et al., 2004; Kruegel et al., 2003; Mehdi et al., 2007), fuzzy genetic algorithms (Abadeh et al., 2007; Boughaci et al., 2012), fuzzy local search (Boughaci et al., 2011), the Mobile agent (Boughaci et al., 2006), and fuzzy stochastic local search (Bahamida & Boughaci, 2012). The idea of applying data mining for intrusion detection was introduced in 1998 (W. Lee, Stolfo, & Mok, 1998; Lee et al., 1999). Data clustering methods have also applied in intrusion detection with K-means (Portnoy et al., 2001), and fuzzy C-means (Shah et al., 2003), this techniques is based on calculating the numeric distance between features. Debar (Debar et al., 1992) and Zhang (Zhang et al., 2001) worked on the artificial neural networks for detection intrusion.

In this paper, we consider the intrusion detection as a pattern classification where a connection’s attributes constitutes a pattern that should be assigned to one of existing classes. The problem is How to identify a given connection as a normal event or attack?

More precisely, the classification problem in intrusion detection is based on the following pattern classification (Ishibuchi & Murata, 1999):

Let us consider a dimensional C-classes pattern classification problem in n-dimensional pattern space with n continuous attributes. Let M be a set of training patterns from the C-classes ($C << M$). Each pattern $X_p$ is a combination of n attributes $X_{pi}$, $X_{p2}$…$X_{pn}$, $p = 1, 2…M$. The problem is finding a set of rule permitting to classify the input patterns with high classification ability.

This work proposes three meta-heuristic based methods for intrusion detection which are: stochastic local search, tabu search and differential evolution. All the three methods work on fuzzy rules “if-then” which are improved by using the optimization meta-heuristic process.

This paper is organized as follows. The second section gives an overview of the KDD’99 dataset. The third section presents the three proposed approaches for intrusion detection. In the fourth section, an experimental evaluation and comparison results are discussed. Finally, the fifth section summarizes our approaches and presents some concluding remarks and future work direction.

DATASET

The Dataset considered in the current work is the KDD’99. This dataset is oriented intrusion. Each line represents a connection between the destination and the source. The connection includes 41 discrete or continuous attributes. The values of attributes are considered as normal connections or attacks.

The full KDD dataset contains 494019 lines of connections. Which consists of 19.65% Normal, 79.07% Dos, 0.23% R2L, 0.22% U2R and 0.83% probing. More precisely, the KDD99 data set consists of 22 attacks which are divided into four categories which are: Denial...
Related Content

Systematic Redaction for Neuroimage Data
[www.igi-global.com/article/systematic-redaction-neuroimage-data/72876?camid=4v1a](www.igi-global.com/article/systematic-redaction-neuroimage-data/72876?camid=4v1a)

Selection of Molybdenum-Filled Hip Implant Material Using Grey Relational Analysis Method
Hybrid Cuckoo Search Algorithm for Optimal Placement and Sizing of Static VAR Compensator
www.igi-global.com/chapter/hybrid-cuckoo-search-algorithm-for-optimal-placement-and-sizing-of-static-var-compensator/147519?camid=4v1a

Optimization Algorithms in Local and Global Positioning
www.igi-global.com/chapter/optimization-algorithms-in-local-and-global-positioning/147509?camid=4v1a