Improved Evolutionary Algorithm based Fuzzy Adaptive Resonance Theory Map (IEA-FARTM) Classifier for Intrusion Detection System

R. Karthik, Assistant Professor, Department of Information Technology, Kongunadu Arts and Science College, Coimbatore.

Dr.S. Veni, Professor & Head, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, India.

Dr.B.L. Shivakumar, Principal, Sri Ramakrishna Polytechnic College, Coimbatore, India.

Abstract--- This investigation effort aims in planning and growth of an improved Evolutionary Algorithm based Fuzzy Adaptive Resonance Theory Map (IEA-FARTM) classifier for the Intrusion Detection System. IEA-FARTM is a double-stage data grouping and rule mining form build on a trimmed FARTM form and the EA. FARTM is proposed in the first stage. Then the rules are pruned using EA. EA is a section of evolutionary calculation, a distracted population-based metaheuristic optimization algorithm. KDD cup'99 dataset that contains four main types of attacks in the system is selected for performing the IEA-FARTM classification. Performance metrics detection rate and false alarm rate are selected. Imitation outcome shows that the proposed IEA-FARTM classifier out performs regarding better detection rate and decreased the false alarm rate.

I. Introduction

Intrusion Detection Systems (IDSs) is the improvement in ensuring the safety in the middle of PC and information networks. For instance, previously denial-of-service (DoS) attack expressions bear with reference to actual calamity, though these times, creative DoS attacks can fetch the overpowering principal associated hard luck to associations. The function of intrusion detection frameworks is to make the distinction anomalous or mistreatment behavior of framework and report to system administrators concerning the movements. Abundant intrusion detection setups have a safety boundaries, for instance, neglecting to encrypt the record credentials, overlooking the access control, and neglecting to act upon responsibility checks, and so on. An IDS is extra sheltered than other safety gadgets, for instance, firewalls [1]. Preceding investigation works falls majorly in two noteworthy ideas known as anomaly detection and signature detection enchanting into consideration, anomalous conducts the framework [2]. At first IDS comprises of addition of inspection records from the watched framework. At that position this records is moreover preprocessed or purposely linked to the pointer to produce an alarm. The primary position of IDS is to develop the detection rate and to diminish the false alarm rate in recognizing attacks. As of late, the investigator for the most part centered on anomaly detection in vision of the projected procedures, for instance, data mining, neural system, etc.

The Intrusion detection forms could be classified into a couple of main types: misuse-based and anomaly-based [3, 4]. Signature-based or Pattern-based, are the other terms used for misuse-based, the detection is based on the attacks in the information stored in a database. Despite of the fact that this type of ID is professionalized in detecting the past or existing intrusions, it has been bluffed by any minute alteration in the primitive. Both known and unknown intrusions can be detected using the Anomaly-based forms, it can also detect the deviations from the usual connections [5]. The main disputes in the present anomaly IDS are their stumpy detection rates, which illustrates that they can initially fail to find out the serious attacks and the drastic 'false alarm' rates, by which usual connection can be incorrectly classified as an attack. In common, attacks can be divided into four categories [6]:

Denial of Service (DoS): Attackers struggle to put off genuine clients from using a service, workstation or source. Examples include SYN Flood, Ping of Death, Back, Smurf, Land, Apache2 and Teardrop [7].

Remote to User (R2L): Attackers seeks admission to the prey mechanism. Examples include Send mail, Dictionary, Named, Guest, Imap, and Ftp_write.

User to Root (U2R): Attackers with limited access to the loser mechanism and struggle to achieve super client privileges. Examples include Perl, Xterm, Loadmodule, Eject, Fdformat.

Probing (Probe): Attackers struggle to get the information about the end host. Examples include Saint, Nmap, Mscan, Satan, Ipsweep.