Conceptual Framework for Soft Computing based Intrusion Detection to Reduce False Positive Rate

Dharmendra G. Bhatti  
Associate Professor,  
Shrimad Rajchandra Institute of Management and Computer Application,  
Bardoli, Gujarat, India

P. V. Virparia  
Associate Professor,  
Department of Computer Science and Technology,  
Sardar Patel University, Vallabh Vidyanagar, Gujarat, India

Bankim Patel  
Director,  
Shrimad Rajchandra Institute of Management and Computer Application,  
Bardoli, Gujarat, India

ABSTRACT
As the popularity and usage of Internet increases security concerns are also become important. Everyone want to be connected to the world through Internet protecting own resources. Intrusion Detection System is one of lucrative area for researchers since long. Numbers of researchers have worked for increasing efficiency of Intrusion Detection Systems. But still many challenges are present in modern Intrusion Detection Systems. One of the major challenges is controlling false positive rate. In this paper we have proposed Soft Computing based Intrusion Detection. We have suggested Genetic Algorithm based solution for Intrusion Detection. In place of standalone Genetic Algorithm we have proposed ensemble soft computing techniques for better results.

Keywords
Conceptual Framework, Intrusion Detection, Soft Computing

1. INTRODUCTION
Intrusion Detection System is front raw warrior in the fight against security threats. This front warrior need to overcome few challenges to carry out its responsibility successfully. Like old story if Intrusion Detection System shouts “wolf-wolf” frequently and incorrectly no one is going to believe it. Security staff needs to analyze alerts generated by Intrusion Detection System. Each alert generated by Intrusion Detection System demands resources like time and efforts from security staff. Large number of false positive alerts makes life of security staff horrifying. False positive alert can be defined as benign traffic identified as attack by Intrusion Detection System and raised alert. To overcome problem of false positive we need to understand causes which leads to it. Intrusion Detection System identifies attack by differentiating from benign traffic. The problem with signature based approach is creation of precise signature. If signature is too specific it cannot identify slightly modified attack. Attacker performs minor change in attack pattern and attack goes unnoticed. On the other hand if we design too generic signature then it can detect attacks variation but it increases possibility of false positive. Such generic signature identifies benign traffic as attack because of similar pattern. Context sensitivity is also one of the reasons for generating false positive alerts. Windows can use NetBIOS in LAN environment but such traffic cannot present on Internet. So depending on the context same network traffic can be normal or an attack. Intrusion Detection Systems come with their default configuration. In many cases, default configuration results in number of false positive alerts. Understandings of network topology and host vulnerabilities are essential for efficient configuration of Intrusion Detection.

2. RELATED WORK
Sandhya [16] have proposed ensemble architecture for Intrusion Detection System. They have suggested hybrid system based on Support Vector Machine and Decision Tree. Using hybrid approach they have tried to maximize detection accuracy and minimize computational complexity. Witcha [23] have proposed Rough-Fuzzy hybrid algorithm for computer intrusion detection. They have applied rough set based methods to identify subset of features and fuzzy c-means for intrusion detection.

Huy Anh [7] have suggested classifier selection model which uses data mining techniques. They have evaluated performance of comprehensive set of classifier algorithms using KDD99 dataset. From the evaluation results they have proposed two classifier algorithm selection models. Prasad [6] have proposed Intrusion Detection using Data Mining and Genetic Algorithm based on Fuzzy Logic. Their model uses anomaly detection based on fuzzy association rules which use genetic programming.

Jing Xiao-Pei [9] have proposed Immunity Intrusion Detection Model based on Genetic Algorithm and Vaccine Mechanism. Other researchers [8][24] have also used Genetic Algorithm for Intrusion Detection.

3. PROPOSED ARCHITECTURE
In our proposed model we are suggesting Genetic Algorithm and Neural Network based solution for reducing false positive rate. The basic idea is to get benefit of these two prominent soft computing techniques. The major components in our solution are as under:

3.1
Network traffic is handled by preprocessing component. This module is responsible for clean input data as well as handles missing and incomplete data. It collects network packet and generates records required for further processing. Initially one can start with default configuration but it is highly recommended to modify configuration according to network topology, hosts exists, services running, and other parameters. Vulnerability scanner tool recommended to collect such data and configuration should be modified by Intrusion Detection Analyst or Security Staff. Properly configured preprocessing unit will help in reducing false positive rate generated due to network topology and context sensitivity.
3.2 Detection engine collects records from preprocessing unit. This part is heart of the solution. We can divide attacks in four major classes: denial of service, remote to local, user to root, and probe. Genetic Algorithm and Neural Network both generates minimum false positive for certain attack classes while generates significant false positive for other classes. So we have assigned weight for each attack class to both classifiers. Analysis engine pass on the records to Genetic Algorithm for Intrusion Detection. Optimized Genetic Algorithm classifies records in various classes like normal record, suspicious record, and possible attack record for each attack class. Based to record type and attack type weight is calculated for suspicious records and possible attack records. Normal record identified by Genetic Algorithm is excluded from further processing. Suspicous record and possible attack record pass on to Neural Network for further processing. Neural Network also classifies record in to normal record, suspicious record, and possible attack record for each attack class. Combiner component is responsible for combining results produced by Genetic Algorithm and Neural Network. It passes on these processed results to response unit.

3.3 Response unit pass on results to Alert Monitoring System. It also transfers conflicting results to Intrusion Detection Analyst for verification. Intrusion Detection Analyst may send manual response to Alert Monitoring System. If required Intrusion Detection Analyst can adjust configuration file and/or database.

In our proposed model we have tried to reduce false positive rate in three different stages. In first stage preprocessing mechanism reduces false positive. In the second stage Genetic Algorithm and Neural Network identifies attacks and reduce false positive by further processing. In the third stage Intrusion Detection Analyst identifies false positive and adjust system accordingly.

4. CONCLUSION
Intrusion Detection System is one of the critical components in computer network security. But it requires addressing challenges like false positive to achieve the desired goal. Here, we have proposed three stage solution for reduction of false positive rate. Preprocessing stage reduces topological and context sensitive false positives. We suggest Genetic Algorithm and Neural Network for Intrusion Detection. Collectively these two techniques significantly reduces false positive rate. Finally Intrusion Detection Analyst helps to reduce false positive. So, proposed three stage solution helps to reduce false positive rate significantly.

Fig 1: Proposed Architecture
REFERENCES


[8] Brian Eugene Lavender, Implementation of Genetic Algorithms into a Network Intrusion Detection System (netGA), and Integration into nProbe, M.S. Project, CALIFORNIA STATE UNIVERSITY, SACRAMENTO, 2010


