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 warier in the fight against security threats. This front warier 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.

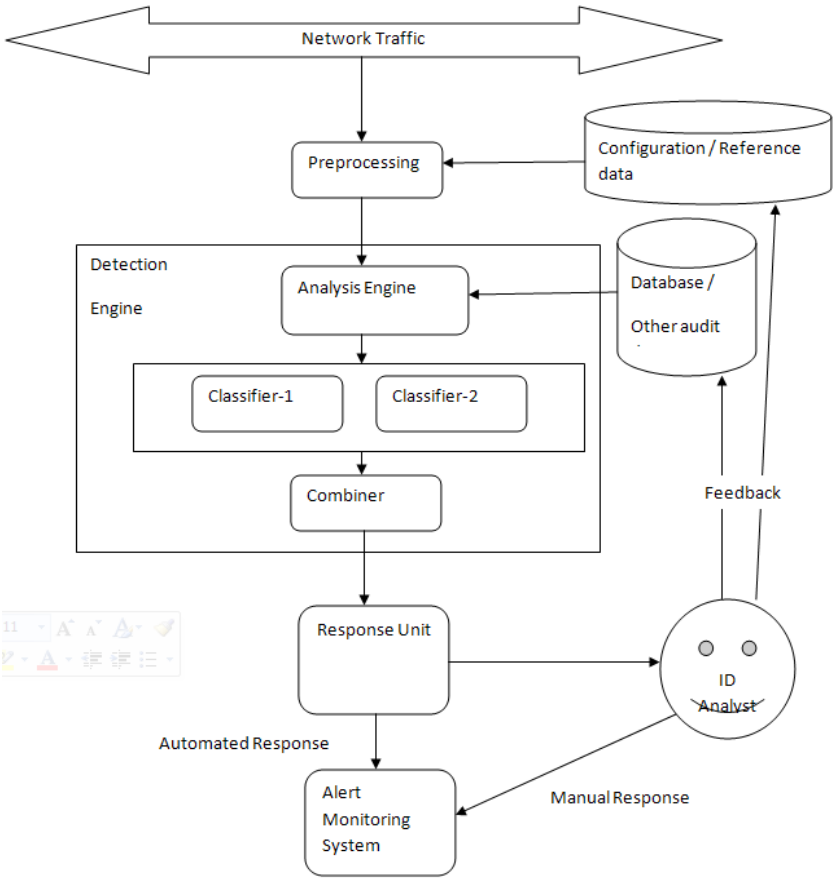

Fig 1: Proposed Architecture

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. Suspicious 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

.

5. REFERENCES

[1] Amir Azimi Alasti Ahrabi, Ahmad Habibizad Navin, Hadi Bahrbegi, Mir Kamal Mirnia, Mehdi Bahrbegi, Elnaz Safarzadeh, Ali Ebrahimi, A New System for Clustering and Classification of Intrusion Detection System Alerts Using Self-Organizing Maps, International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6), 2011

[2] Aung Htike Phyo, Steven Furnell, Emmanuel Ifeachor, A Framework for Monitoring Insider Misuse of IT Applications, Peer-reviewed Proceedings of the ISSA 2004 enabling tomorrow Conference, ISBN 1-86854-522-9, 2004

[3] D.A. Karras, V. Zorkadis, Neural Network Techniques for Improved Intrusion Detection in Communication Systems, Proceedings of the 5th WSES International Conference on Circuits, Systems, Communications and Computers (CSCC 2001) ISBN: 960-8052-33-5, 2001

[4] Damiano Bolzoni, Sandro Etalle, APHRODITE: an Anomaly-based Architecture for False Positive Reduction, Cornell University Library, Subjects: Cryptography and Security (cs.CR), Report number: TR-CTIT-06-13, arXiv:cs/0604026v1 [cs.CR], 2006

[5] Dan Gorton, Extending Intrusion Detection with Alert Correlation and Intrusion Tolerance, Thesis for the degree of licentiate of engineering, Chalmers University of Technology, Goteborg, Sweden, 2003

[6] G.V.S.N.R.V.Prasad, Y.Dhanalakshmi, Dr.V.Vijaya Kumar, Dr I.Ramesh Babu, Modeling An Intrusion Detection System Using Data Mining And Genetic Algorithms Based On Fuzzy Logic, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.7, July 2008

[7] Huy Anh Nguyen, Deokjai Choi, Application of Data Mining to Network Intrusion Detection: Classifier Selection Model, APNOMS '08 Proceedings of the 11th Asia-Pacific Symposium on Network Operations and Management: Challenges for Next Generation Network Operations and Service Management, ISBN: 978-3-540-88622-8, 2008

[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

[9] Jing Xiao-Pei, Wang Hou-Xiang, A new Immunity Intrusion Detection Model Based on Genetic Algorithm and Vaccine Mechanism, I.J.Computer Network and Information Security, 2010, 2, 33-39

[10] Mahmoud Jazzar, Aman Jantan, A Novel Soft Computing Inference Engine Model for Intrusion Detection, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.4, April 2008

[11] Mansour Sheikhan and Zahra Jadidi, Misuse Detection Using Hybrid of Association Rule Mining and Connectionist Modeling, World Applied Sciences Journal 7 (Special Issue of Computer & IT): 31-37, ISSN 1818-4952, 2009

[12] Muna Elsadig, Azween Abdullah, Biological Inspired Intrusion Prevention and Self-healing System for Network Security Based on Danger Theory, International Journal of Video & Image Processing and Network Security Vol: 9 No: 9, 2008

[13] Obbo Aggrey, An Intrusion Detection System For Academic Institutions, Master of Science Thesis, Makerere University, July 2007

[14] P. Kiran Sree, Exploring a Novel Approach for Providing Software Security Using Soft Computing Systems, International Journal of Security and its Applications, Vol. 2, No. 2, April 2008

[15] S. Elahi, A. Shayan, B. Abdi, Designing a Framework for Convergent Information Security Management among Federated Organizations, World Applied Sciences Journal 4 (Supple 2): 21-32, ISSN 1818-4952, 2008

[16] Sandhya Peddabachigaria, Ajith Abrahamb, Crina Grosanc, Johnson Thomasa, Modeling intrusion detection system using hybrid intelligent systems, Journal of Network and Computer Applications 30 (2007) 114–132, 2007

[17] Suhair Hafez Amer, Enhansing Host based Intrusion Detection Systems with Danger Theory of Artificial Immune Systems, Ph.D. Thesis, Auburn University, Alabama, May 2008

[18] Tadeusz Pietraszek, Alert Classification to Reduce False Positive in Intrusion Detection, Dissertation thesis submitted to Institut fur Informatik, Albert-Ludwigs-Universitat Freiburg, Germany, 2006

[19] Tao Wan, Intrudetector: A Software Platform for Testing Network Intrusion Detection Algorithm, Master of Science Thesis, University of Regina, Canada, 2000

[20] Te-Shun Chou, Cyber Security Threats Detection Using Ensemble Architecture, International Journal of Security and Its Applications Vol. 5 No. 2, April, 2011

[21] Thomas A, RAPID: Reputation based approach for improving intrusion detection effectiveness, Information Assurance and Security (IAS), 2010 Sixth International Conference, On page(s): 118 - 124, Print ISBN: 978-1-4244-7407-3, 23-25 Aug. 2010

[22] Wanli Ma, John Campbell, Dat Tran, and Dale Kleeman, A Conceptual Framework for Assessing Password Quality, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.1, January 2007

[23] Witcha Chimphlee, Abdul Hanan Abdullah, Mohd Noor Md Sap, Siriporn Chimphlee, Surat Srinoy, A Rough-Fuzzy Hybrid Algorithm for Computer Intrusion Detection, The Internaltional Arab Journal of Information Technology, Vol. 4, No. 3, July 2007

[24] Zorana Bankovic, Jose M. Moya, Alvaro Araujo, Slobodan Bojanic and Octavio Nieto-Taladriz, A Genetic Algorithm-based Solution for Intrusion Detection, Journal of Information Assurance and Security 4 (2009) 192-199, 2009