EXPLORATION OF HYBRID SOFT COMPUTING TECHNIQUES FOR INTRUSION DETECTION

S. Revathi [1], Dr. A. Malathi[2]

[1]*Ph.D. Research Scholar, Government Arts College, Coimbatore (India)*
[2]*Assistant Professor, Government Arts College, Coimbatore (India)*

ABSTRACT

Security is a vital role in information and communication technology where a lot of effort has been invested. Intrusion detection plays a prominent role in this field. Many researcher focused on this area mainly to increase detection rate and to reduce false alarm rate. Various methods has been used to detect intrusion, in earlier days data mining automates network intrusion detection with greater efficiency. This paper presents a depth survey on intrusion detection based on various soft computing methods. This paper presents a depth survey on intrusion detection based on various research paper published using hybrid soft computing methods such as Fuzzy-Genetic, Neuro-Fuzzy, Neuro-Fuzzy-Genetic and other evolutionary methods. The various dataset used for their research be KDD cup dataset and DARPA 98 dataset to test the effectiveness of their proposed method.

***Keywords*: *Anomaly detection, Misuse detection, Intrusion detection, soft computing*.**

I INTRODUCTION

The nature of network grows rapidly from few decades, which leads to development in the nature and requirement of network security. The major issues with network is to identify difference between normal and abnormal transactional activities. The ways to monitor network activity is to either prevent it or to detect intrusion, for prevention many techniques are available such as encryption, firewalls and authentication of system. But prevention cannot be a sufficient measure, so we need to detect intrusion. For detection various researcher used different methods to increase detection accuracy. Now-a-days Soft Computing becomes a promising solution to detect harmful and previously unseen intruders. The rest of this paper is sectioned as follows: Section 2 and 3 explains introduction to IDS and SC. Section 3 describes related work based on hybrid SC methods to detect intrusion. Section 4 deals with Discussion Analysis and section 5 indicates conclusion and future work.

II INTRUSION DETECTION SYSTEM

The origin of intrusion detection system was developed from 1980s [1] were proposed by Denning [2]. IDS is used to monitor network activities for detecting known or unknown attacks. The main objective of IDS is to generate alarm by system administrator if any suspicious activity happening. It tries to identify break in attempt from unauthorized user. Intrusion detection techniques are classified in two categories: anomaly detection and

signature detection or misuse detection. Anomaly detection refers to the identification of unknown pattern or any deviation from normal behavior, it is also referred to as outlier, change, deviation, surprise, aberrant, peculiarity, intrusion, etc. In misuse detection it identifies only known attacks that stores from large database of attack signature. IDS looks for a specific attacks that has been already documented. The major drawback of misuse detection is it cannot able to identify unknown attacks. IDS response in two ways [3]: Active- takes some action to intrusion (such shutting down services, connection, logging user). Passive - generates alarms or notification. Audit information analysis in intrusion detection system can be done in two ways: on the fly processing (real time) and interval based (periodical). Intrusion detection system runs continuously for intrusion detection and gives result in real time is called real-time intrusion detection system. The term real-time does not indicate more than a fact that IDS reacts to an intrusion quick enough. Intrusion detection system runs periodical for intrusion detection, Interval based are also called periodical intrusion detection system.

III SOFT COMPUTING

The term Soft Computing was first purposed by Zadeh [4] for constructing new generation computationally intelligent hybrid systems which consist of fuzzy logic (FC), artificial neural network (ANN), probabilistic reasoning (PR) and Genetic Computing (GC). Soft Computing is an intelligent systems, which provide human expertness such as specific knowledge for a particular domain, uncertain reasoning, and adaptation a time varying environment. All these features are used for solving practical computing problems. Conventional AI techniques deals only with precision, certainty but in contrast with soft computing it exploit the tolerance for imprecision, uncertainty and partial truth, low solution cost, achieve tractability, error free, and enhanced result with reality. It is used in conjunction with rule-based expert systems in the form of if-then rules. Despite different approaches have been proposed in recent years, for detecting intrusion. Various hybrid method such as neuro-fuzzy, neuro-genetic, fuzzy-genetic, and neuro-fuzzy- genetic are used as most popular techniques for building IDS.

IV RELATED WORK

Soft Computing Approaches is played a prominent role in the field of intrusion detection. This section briefly explains the literature survey of various soft computing methods used to detect intrusion. The analysis are carried based on both misuse and anomaly detection. The dataset used for evaluation of their proposed system be DARPA 98or KDD cup 99 dataset. Initially,

Siraj A et al. [5] (2004) Shows the working of intrusion detection decision engine based on fuzzy knowledge inference based cognitive maps (FCMs).

Abraham, R. Jain [6] (2004a): They compared various method such as fuzzy rule based classifier, SVM, Decision tree, Linear genetic programming and some ensemble method to detect intrusion. The result proves that soft computing methods shows higher efficiency in detecting intrusion.

Abraham et al. [7] (2004b): They proposed a light weight Soft Computing IDS (SIDS). Decision tree is to reduce attribute, further Fuzzy classifier and Linear genetic programming are used to identify intrusion. This work was expanded into a Distributed SCIDS (D-SCIDS).

Chen et al. [8] (2005a): The author used Genetic programming along with flexible neural tree to optimize the DARPA data and further PSO is used to fine tune the node weight and functional parameter. The process repeats until the result satisfies.

Chen et al. [9] (2006): The author analyzed two hybrid work based on DARPA dataset. Initially neural network with ANN are used to train the dataset based on distribution and evolutionary algorithms. Then they compared ANN with Estimation of distributed algorithm along with PSO.

Ajith Abraham et al. [10] (2007): In this paper the author evaluates three fuzzy rule generation based classifier to detect intrusion in a network and the result are compared with other machine learning techniques like decision trees, support vector machines and linear genetic programming.

Tsang C et al. [11] (2007a) has proposed Genetic-fuzzy rule mining approach and evaluation of feature selection techniques for anomaly intrusion detection. Performance of the proposed system has been evaluated on KDDCup99 dataset and shows highest detection accuracy for intrusion attacks and low false alarm rate for normal network traffic with minimized number of features.

Toosi et al [12] (2007b) has proposed a neuro fuzzy classifier based on Adaptive Neuro Fuzzy Inference system using genetic algorithm. In addition, subtractive clustering is used to group data from large database. No feature selection methods were used. The training, testing, cost per example of the proposed system shows better accuracy than other existing system.

Michailidis et al. [13] (2008): The authors explain in detail about various evolutionary neural networks methods. They trained IDs using ANN with PSO based on its weight training, architecture design, feature selection and connection weights etc.

Dhanalaksmi and babu [14] (2008a): They created various fuzzy rules based on its membership function and use genetic algorithm to optimize the result and find out best rule.

Hoang X D et al. [15] (2009) Uses multiple detection engine along with fuzzy inference. The proposed methods was evaluated based on HMM model. The experimental analysis shows high detection rate and very low false alarm rate along with its training and testing time.

Shanmugam B et al. [16] (2009b) has proposed improved intrusion detection system using Fuzzy Logic for Detecting Anomaly and Misuse type of Attacks. Parameters detection rate and false positive rate are used for evaluation. The performance of the proposed method shows that the detection rate is comparatively higher than all other systems. The false positive rate is also low in comparison to the values obtain from other models.

Wang G et al. [17] (2010) has proposed a new method for intrusion detection using Artificial Neural Networks along with fuzzy clustering.

Mabu S et al. [18] (2011) an intrusion detection model based on Fuzzy Class association rule mining using genetic network programming. Experimental results on the proposed method using KDD Cup and DARPA98 databases shows that it provides competitively high detection rates compared with other machine learning techniques.

Arif Jamal Malik, et al [19] (2011a) proposed a new concept of hybrid partial swarm optimization with random forest algorithm to reduce feature attribute and to classify accuracy than others with approximately 95%.

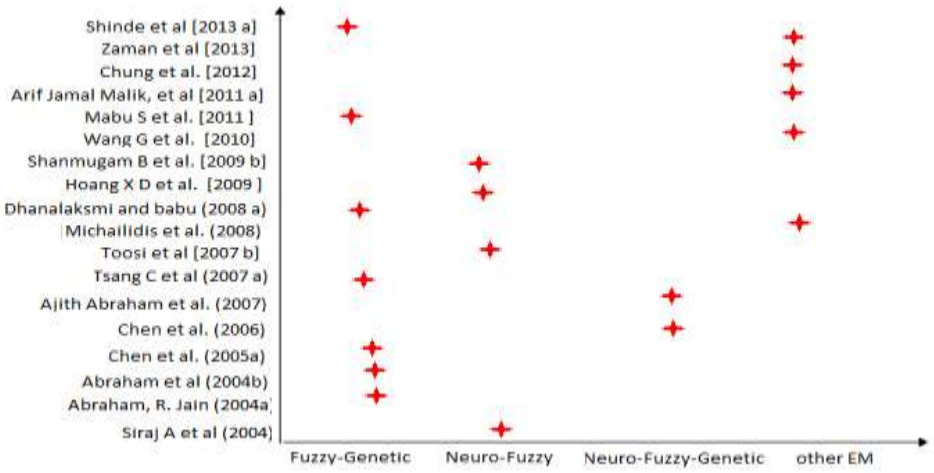
Chung et al. [20] (2012) has proposed a hybrid network intrusion detection system using simplified swarm optimization (SSO). The testing on the proposed system shows that the proposed hybrid system can achieve higher classification accuracy than others with 93.3% and it can be one of the competitive classifier for the intrusion detection system.

Zaman et al [21] (2013) has proposed a new concept for feature selection based on various soft computing methodologies such as PSO, GA and DE for reducing attribute in KDD dataset to detect intrusion. The classification accuracy, FPR, training time and testing time are classified using SVM and NN method and found that DE reduce more attribute other two approaches

Shinde et al [22] (2013a) has proposed a new hybrid concept of combining fuzzy GNP based on probabilistic classification. The paper explains a novel fuzzy genetic network programming (GNP) and probabilistic classification for detecting network intrusions. Proposed method can flexibly applied to both misuse and anomaly detection.

V DISCUSSION

This paper provides a depth study on intrusion detection in the soft computing techniques. It concludes that approximately many researcher focused on anomaly detection based on fuzzy genetic algorithm. But recently the researcher moves toward various evolutionary methods such as particle swarm optimization, ant colony optimization, and simplified swarm optimization. The optimization techniques are used to increase accuracy and to reduce false alarm rate that works more effectively than other methods. Most commonly used dataset are KDD cup 99 and DARPA 98 to show the proposed method efficiency. The below figure shows a comparison of various soft computing methods for intrusion detection.



.

Fig. 1: Comparison of various hybrid soft computing method

VI CONCLUSION

Intrusion detection plays a vital role in system security. This paper affords various soft computing methods in detecting intrusion. These methods are very impressive and interactive with many deviations. A wide-ranging direct comparison of all research approaches are not currently feasible However, not all of the authors used same deviations of the methods and the results of the test is also not known, but still some results stand out in each paper that are used for analytical purpose in intrusion detection. This paper concludes that the focus of the researchers moves towards various optimization techniques to obtain some near optimal solution. Most of the researcher focused on anomaly detection and use existing benchmark datasets for their experiments.

REFERENCES

1. Teresa F. Lunt: ―Ides: An intelligent system for detecting intruders, Computer security, threat and countermeasures 30-45 (1990).
2. Dorothy E. Denning: ―An intrusion-detection model.‖ In: IEEE Trans Software VOL. SE-13 NO. 2, 118–13 (1986).
3. http://en.wikipedia.org/wiki/Intrusion_detection_system.
4. Zadeh, L. ―A.: ―The Roles of soft computing and fuzzy logic in the conception, design and deployment of information/intelligent systems. Computational intelligence: soft computing and fuzzy-neuro integration with applications, vol 162. Springer, New York (1998).
5. Siraj A., Vaughn R. B., Bridges S. M., Intrusion Sensor Data Fusion in an Intelligent Intrusion Detection System Architecture, Proceedings of the 37th Hawaii International Conference on System Sciences. (2004).
6. A. Abraham, R. Jain, S. Sanyal, S.Y. Han: ―Scids a soft computing intrusion detection system.‖ In: 6th international workshop On distributed computing (IWDC 2004c). Springer, Berlin, pp 252– (2004).
7. K. Shah, N. Dave, S. Chavan, S. Mukherjee, A. Abraham, and S. Sanyal: ―Adaptive neuro - fuzzy intrusion detection system.‖ In: IEEE international conference on ITCC'04, Vol pp 70–74 (2004b).
8. Chen Y, Abraham A, and Yang J: ―Feature deduction and intrusion detection using flexible neural trees.‖ In: Second IEEE International Symposium on Neural Networks 2617-2634 (2005b).
9. W. H. Chen, S. H. Hsu, H.P Shen: ―Application of SVM and ANN for intrusion detection.‖ Computer Operating Res Volume 32, Issue 10, 2617–2634 (2005a).
10. A. Abraham, R. Jain, J. Thomas, S.Y. Han: D-scids: distributed soft computing intrusion detection system. J Network Computer Application 30:81–98(2007).
11. Tsang C., Kwong S., Wang H., Genetic-fuzzy rule mining approach and evaluation of feature selection techniques for anomaly intrusion detection, Pattern Recognition. 40 (2007) 2373 – 2391.
12. A. N. Toosi: ―Adaptive a new intrusion detection based on an evolutionary Soft Computing Model.‖ In Computer Communication Elsevier 2201–2212 (2007).
13. E. Michailidis, S. K. Katsikas, E. Georgopoulos: ―Intrusion detection using evolutionary neural networks.‖ In: Panhellenic conference on informatics (PCI 2008), pp 8–12(2008).
14. L. Tao, H. Yuan-bin, Q. Ai-ling, and C. Xin-Tan: ―Feature optimization based on artificial fish-swarm algorithm in intrusion detection.‖ In: 2009 international conference on networks, security, wireless communications and trusted computing, Hube, Wuhan, pp 542– 545(2009).

15. Hoang X. D., Hu J.,Bertok P., A program-based anomaly intrusion detection scheme using multiple detection engines and fuzzy inference , Journal of Network and Computer Applications. 32 (2009) 1219–1228.
16. Shanmugam B.,Idris N. B., Improved Intrusion Detection System using Fuzzy Logic for Detecting Anamoly and Misuse type of Attacks, 2009 International Conference of Soft Computing and Pattern Recognition.(2009).
17. Wang G.,Hao J., Ma J.,Huang L., A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering, Expert Systems with Applications 37 (2010) 6225–6232.
18. Shingo Mabu, *Member, IEEE*, Ci Chen, Nannan Lu, Kaoru Shimada, and Kotaro Hirasawa, *Member, IEEE*, An Intrusion-Detection Model Based on Fuzzy Class-Association-Rule Mining Using Genetic Network Programming, IEEE Transactions On Systems, Man, And Cybernetics—Part C: Applications And Reviews, VOL. 41, NO. 1, January 2011.
19. Arif Jamal Malik, Waseem Shahzad,Farrukh Aslam Khan , Network intrusion detection using hybrid binary PSO and random forests algorithm, published in Evolutionary Computation (CEC), 2011 IEEE Congress on New Orleans, LA, Pg.no 662 – 668 , June 2011. Doi: 10.1109/CEC.2011.5949682.
20. Yuk Ying Chung, Noorhaniza Wahid, A hybrid network intrusion detection system using simplified swarm optimization (SSO), Applied Soft Computing 12 Pg No:3014–3022, 2012.
21. Safaa Zaman, Mohammed El-Abed, Fakhri Karray, Features Selection Approaches for Intrusion Detection Systems based on Evolution Algorithms, *ICUIMC(IMCOM)'13*, Kota Kinabalu, Malaysia, ACM 978-1-4503-1958-4…. January 17–19, 2013.
22. S.B.Shinde, V.P.kshirsagar and M.K. Deshmukh " A hybrid approach for intrusion-detection based on fuzzy GNP and probabilistic classification ", *Proc. SPIE* 8768, International Conference on Graphic and Image Processing (ICGIP 2012), 87681Y (March 14, 2013); doi:10.1117/12.2010855; http://dx.doi.org/10.1117/12.2010855

Biographical Notes

Mrs. S. Revathi is presently pursuing Ph.D. in Computer Science from Government Arts College, Coimbatore, India.

Dr. A. Malathi is working as a Assistant professor in Computer Science Department, Government Arts College, Coimbatore, India.