Analysis of Hybrid Soft Computing Techniques for Intrusion Detection on Network

Alka Chaudhary[1], Anil Kumar[2], V.N.Tiwari[3]

[1]*Ph.D Scholar CSE,* [2]*CSE, Manipal University jaipur,*

[1]*alkachaudhary0207@gmail.com,*[2]*anil.kumar@jaipur.manipal.edu*

[3]*ECE, Manipal University, Jaipur*

[3]*vivekanand.tiwari@jaipur.manipal.edu*

Abstract --- **Intrusion detection is an action towards security of a network when a system or network is being used inappropriately or without authorization. The use of Soft Computing Approaches in intrusion detection is an Appealing concept for two reasons: firstly, the Soft Computing Approaches achieve tractability, robustness, low solution cost, and better report with reality. Secondly, current techniques used in network security from intrusion are not able to cope with the dynamic and increasingly complex nature of network and their security. It is hoped that Soft Computing inspired approaches in this area will be able to meet this challenge. Here we analyze the approaches including the examination of efforts in hybrid system of SC such as neuro-fuzzy, fuzzy-genetic, neuro-genetic, and neuro-fuzzy-genetic used the development of the systems and outcome their implementation. It provides an introduction and review of the key developments within this field, in addition to making suggestions for future research.**

Keywords: **Soft Computing (CS), Intrusion detection systems (IDS), Hybrid Soft Computing Techniques.**

*****

I. INTRODUCTION

The nature of network is going to more complex rapidly from few decades. so that we can see a fundamental evolution in the nature and requirement of network security. The most primary issue with network is determining the difference between normal and abnormal activities. There are many techniques available for Prevention of network from intrusion such as encryption, firewalls and intrusion detection system. The Promising solution is coming out in the form of Soft Computing. The Soft Computing techniques can detect and challenge for harmful and previously unseen intruders. The rest of this paper is organized as follows: Section 2 and 3 introduce the area of IDS and Soft Computing with motivation and related work. In Section 4 Analyze the implementation of Soft Computing inspired IDSs and System implementation detail. In Section 5 indicates conclusion and future area of study.

II. INTRUSION DETECTION SYSTEM

The first intrusion detection system was called intrusion detection expert system (IDES) which was developed at 1980s [1]. Intrusion detection became more active when techniques for an intrusion detection system were proposed by Denning [2]. Intrusion detection is a security technology that attempt to identify those who are trying to break into and misuse a system without authorization and those who have legitimate access to the system but are abusing their privileges. An Intrusion detection system dynamically monitors a system and user actions in the system to detect intrusion [3]. Cohen noted that the determination of virus was undecidable and he also concluded that ―This leaves us with imprecise techniques [4]. There are four types of intrusion detection methods: Threshold, anomaly, rule based and model based [5].Rule based detection is same as misuse detection. Threshold detection is simply summary statistics. We can get the higher level of abstraction by Model based intrusion detection system. For other type of detection we can also use Model based detection. Me. L. used a genetic to manipulate vectors based on event counts and said the problem was NP complete [6]. In the credit to misuse detection, Lee and Heinbuch Today, all most practical IDS are signature based. The performance of these misuse base detection system is limited by the signature database. Many known attacks can be easily modified to present many different signatures. Completely new attacks cannot be present in the database. In source to anomaly detection, Lee and Heinbuch marked these systems were posed by two difficulties, one practical and other theoretical. The practical difficulty is that nominal usage has high variability and changes over time. Furthermore these on systems are unable to detect intrusion against multiple targets of the network. Hybrid systems which based host and network elements can offer the best protection and many systems are also under development which will protect against intrusion from multiple sources in the network [7].

III. SOFT COMPUTING

The term Soft Computing was first purposed by Zadeh [8] for constructing new generation computationally intelligent hybrid systems which is consisting of fuzzy logic (FC), artificial neural network (ANN), probabilistic reasoning (PR) and Genetic Computing (GC). Soft Computing Aimed that the intelligent systems, which can provide human like expertness such as specific knowledge for a particular domain, uncertain reasoning, and adaptation a time varying environment. All these features of Soft Computing are important for solving practical computing problems. Conventional AI techniques which only deal with precision, certainty but in contrast with soft computing is to exploit the tolerance for imprecision, uncertainty and partial truth, low solution cost, , achieve tractability, robustness, and better report with reality.SC is hybrid system such as neuro-fuzzy, neuro-genetic, fuzzy-genetic, and neuro-fuzzy- genetic. These hybrid system have been by for the most popular when building IDSs Such as Banissone denoted Hybrid Soft Computing System. He breaks SC in knowledge driven reasoning system such as probabilistic and fuzzy Computing and Optimization Approaches such as neuro and evolutionary computing [9]. Garcia and Copeland reported that SC tools were beginning to be used in intrusion first time the term Soft Computing was appearing in a paper about intrusion detection [10]. Bridges and Vaughn discussed a prototype IDS using combination of fuzzy data and genetic algorithm (GA) on networks [11]. Mukkamala et al. presented distributed intrusion detection sys-tem for detect and prevent attacks that would be invisible to any single system. The state of the art of the evolution of intrusion detection systems [12].Copeland and Garcia detected Real- time anomaly using Soft Computing techniques [13]. Shah et al. adopted neuro-fuzzy for intrusion detection system [14]. Abraham and Jain presented Soft Computing models for network intrusion detection system [15]. Abraham et al. purposed A Soft Computing intrusion detection system [16]. Chen et al. Suggested Application of SVM an ANN for intrusion detection [17]. Chen et al. used flexible neural network trees for feature deduction and intrusion detection [18]. Katar combined multiple techniques for intrusion detection [19].

Chen el al. estimated of distribution algorithm for optimization of neural Network and intrusion detection system [20]. A Abraham et al. purposed distributed soft computing intrusion detection system [21]. Toosi adopted a new approach for intrusion detection based on an evolutionary Soft Computing model [22]. Chou and Yen followed fuzzy C- Means (FCM) clustering [23]. Michailidis et al. [24] purposed an intrusion detection system using evolutionary neural networks. Dhanalaksmi and Baba applied combination of soft

Computing techniques for intrusion detection [25]. S Kaur explained Soft Computing in Intrusion detection [26]. M. Govindarajan et al. developed intrusion detection using neural based hybrid classification methods [27].

IV. Brief Summary of SC based Approaches

Soft Computing Approaches is played a prominent role in the field of intrusion detection. In this section describes general SC methods in order with illustrative papers of how these methods have been implemented as IDSs.

Copland and Garcia (2000): They Explored a combined strategy, starting with a SOM to group TCP Flags, followed by a Learning Vector Quantizer (LVQ), a type of ANN, to characterised connection types, followed by a network handshake-watching fuzzy inference system (FIS) which was fine tuned with a genetic Algorithm (GA) with the end goal of detecting anomalies on network traffic.
Bridges and Vaughn (2000): They discussed a prototype IDS using fuzzy data mining and genetic algorithm (GA) on network or audit data.GA fine tuned the fuzzy sets by adjusting the two parameters which defined functions in the fuzzy systems: where membership started and where member was I.

Biermann et al. (2001): They make a comparison between IDS Approaches. Those approaches whether it was anomaly or misuse detection, the origin of data, the accuracy, the completeness and the amount of the data where it detects these types of attacks: known, unknown, Dos, malicious use, break in and penetration of security.
A. Abraham, R. Jain (2004a): They investigated fuzzy rule-based classifiers, decision trees, support vector machines, linear genetic programming and an ensemble method to model fast and efficient intrusion detection systems. Empirical results clearly showed that soft computing approach could play a major role for intrusion detection.

Shah et al. (2004b): They compared an evolving fuzzy neural network (FNN) with ANN using snort for the training. EFuNN was preferred because accuracy was comparable to that of ANN but training was in second while the AAN training time was in minutes.
Abraham et al. (2004c): They proposed a light weight Soft Computing IDS (SIDS). It's started with a DT reduce features that were fed into an ensemble of another DT, Linear genetic programming (LGP) and a Fuzzy Classifier. This was expanded into a Distributed SCIDS (D-SCIDS).
Chen et al. (2005a): They proposed a flexible neural tree (FNT) using the DARPA Dataset in which the node structure was first optimized by genetic programming (GA) and then the node weight and function parameters were fine tuned with PSO. If did not result in a satisfactory solution, Then the GP and PSO processes were repeated.

Chen et al. (2005b): They compared a hybrid FNT with PSO and Evolutionary algorithms with a hybrid ANN-PSO using
the DARPA Datasets.

Chen et al. (2006): They studied two hybrids using the DARPA sets. The first one hybrid was neural an ANN which was trained by estimation of distributed algorithm, an evolutionary Method the second one was an ANN which was

Katar (2006): Purposed an ensemble of Naïve Bayes, ANN trained by PSO and C4.5DT on three separate sets of data input from the DARPA Dataset with the multiple fusion methods of Bayes Average, Recognition, Substitution, and Rejection rates (RSR).

Chen et al. (2006): They compared an estimation of distribution algorithm (EDA) ANN with a PSO ANN, and a DT using the DARPA Dataset.
Ajith Abraham et al. (2007): They implemented DIDS using co-operative intelligent agents distribute across the network(s).In this paper evaluates three fuzzy rule – based classifiers to detect intrusion in a network and Results are compared with other machine learning techniques like decision trees, support vector machines and linear genetic programming.

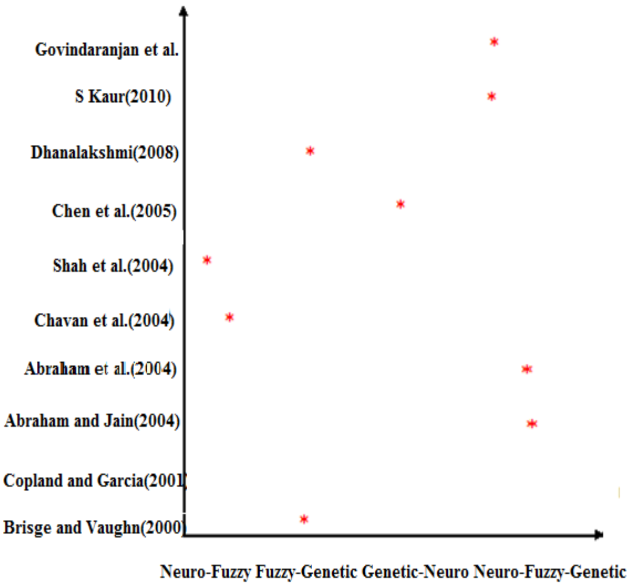

Fig. - Hybrid Soft Computing Approaches from literature

Michailidis et al. (2008): They had given an excellent description of evolutionary neural networks. He also proposed an ANN trained with PSO. They noted that evolutionary Algorithm (EA) can perform various (A tasks, including weight training, architecture design, learning rule Adaption, input feature selection and connection weight initialization.

Dhanalaksmi and babu (2008): They created fuzzy sets from the input network packet data, defined membership functions for fuzzy variables, and then applied a genetic algorithm to identify the best rules. **Dasgupta and Nino (2009)**: in this paper artificial neural network refer to a multilayer perception. A SOM is used technically also a type of ANN. An ANN is typically is classifier in a graph structure which stimulate biological neural networks. The knowledge engineers determine the structure of the ANN, which is then trained, usually with supervision. A human expert then decides if a follow up to an alert is appropriate to see if an intrusion has actually occurred. .

M. Govindarajan et al. (2011): They Purposed hybrid architecture involving ensemble and base classifiers for intrusion detection systems. The analysis of results shows that the performance of the purposed method is superior to that of single usage of existing classification methods such as multilayer perceptron and radial basis function.

V. Conclusion and Future Work

A All detection methods based Intrusion detection system such as rule based and Anomaly based is needed but not sufficient in detecting the wide variety of intrusion which are possible. Soft Computing offers very impressive and interactive methods or Approaches for intrusion detection with many variation and sub variation. A comprehensive direct comparison of the methods or approaches based on available research is not currently feasible. However, not all of the authors used same variations of the methods. For example, many different types of ANN were evaluated. The statistical relevance of the results of these tests is also not known. Although, some results stand out. As per Suggestion for future research is recommended a paradigm of a track meet with many parallel strategies needed against many different challenges. Attack scenarios are constantly changing and the best defense is a recommended. This is a wide area for future intrusion detection research.

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] Bo Sun and Lawrence Osborne: “Intrusion detection techniques in
mobile ad hoc and wireless sensor network.” In: IEEE Wireless
Communications, 1536-1284 (2007).

[4] Fred Cohen: “Computer viruses: theory and experiments. Computers and Security archive,” Volume *6* Issue *1*, 22–35 (1987).

[5] K. Ilgun, R. A. Kemmerer, and P. A. Porras: “State transition analysis: a rule-based intrusion detection approach.” In: IEEE Trans Software Eng VOL. SE-21 No.3, 181– 199(1995).

[6] Ludovic Me, Gassata: “A genetic algorithm as an alternative tool for security audit trails analysis.” In: Recent advances in intrusion detection (RAID’98) (1998).

[7] S.C. Lee, D.V. Heinbuch: “Training a neural network based intrusion detector to recognize novel attacks.” In: IEEE Trans Syst Man Cybernet A, 31: 294-299(2001).

[8] Zadeh, L. “A.: “The Roles of soft computing and fuzzy logic in the conception, design and deployment of information/intelligent systems.” In: Kaynak, O., Zadeh, L.A., Turksen, B., Rudas, IJ (eds) Computational intelligence: soft computing and fuzzy-neuro integration with applications, vol 162. Springer, New York (1998).

[9] P. P. Bonissone: “Hybrid soft computing systems: Where are we going?”http://www.cs.berkeley.edu/nikraves/bisc/present/Fall0/Pre).sent/Fall0/Pieroecai2000v4.pdf (5/7/08) (2000).

[10] R. C. Garcia, J.A. Copeland: “Soft computing tools to detect and characterize anomalous network behavior.” In: IEEE Southeast conference 475-478 (2000).

[11] S.M. Bridges, R.B. Vaughn: “Fuzzy data mining and genetic algorithms applied to intrusion detection.” In: National information systems security conference, vol. 1. 16–19 October, pp 13–26 (2000).

[12] A. Lazarevic, V. Kumar, and J. Srivastava: Intrusion detection: A Survey. In Kumar V, Srivastava, J, Lazarevic A (eds) Managing Cyber threats, Springer, New York, PP 19 – 78 (2005).

[13] J. A. Copeland, R. C. Garcia: “Real-time anomaly detection using soft computing techniques.” In: IEEE Southeast Conference 105 - 108 (2001).

[14] A. Abraham, R. Jain: “Soft computing models for network intrusion detection systems.” http://arxiv.org/ftp/cs/papers/0405/0405046.pdf. Accessed 15 May 2008 (2004a).

[15] 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).

[16] 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).

[17] W. H. Chen, S. H. Hsu, H.P Shen: “Application of SVM and ANN for intrusion detection.” Comput Oper Res Vol-ume 32, Issue 10, 2617–2634 (2005a).

[18] 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). [20] C. Katar: Combining multiple techniques for intrusion detection. Int J Comput Sci Network Security 208–218 (2006).

[19] C. Katar: “Combining multiple techniques for intrusion detection.” Int J Comput Sci Network Security 208–218 (2006).

[20] Y. Chen, Y. Zhang, A. Abraham: “Estimation of distribution algorithm for optimization of neural networks for intrusion detection system.” In: Rutkowski L, Tadeusiewicz R, Zadeh LA, Zurada J (eds) “Artificial intelligence and soft computing”— ICAISC 2006. Springer, New York (2006).

[21] A. Abraham, R. Jain, J. Thomas, S.Y. Han: D-scids: distributed soft computing intrusion detection system. J Network Computer Appl 30:81–98(2007).

[22] A. N. Toosi: “Adaptive a new intrusion detection based on an evolutionary Soft Computing Model.” In Computer Communication Elsevier 2201–2212 (2007).

[23] T. S. Chou, K. K. Yen: “Fuzzy belief k-nearest neighbour’s anomaly detection of user to root and remote to local at-tacks.” In: The 2007 IEEE workshop on information assurance, United States Military Academy, West Point, NY, pp 207–213(2007).

[24] E. Michailidis, S. K. Katsikas, E. Georgopoulos: “Intrusion detection using evolutionary neural networks.” In: Panhellenic conference on informatics (PCI 2008), pp 8–12(2008).

[25] 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).

[26] C. Langin, S. Rahimi: “Soft Computing in intrusion detection: The State of the Art” in Ambient Intell Human Compute 1:133-145 DOI 10.1007/s12652-010-0012-4(2010).

[28] M. Govindaranjan, R. M. Chandrasekaran: Intrusion detection using neural based hybrid classification methods. In: Computer networks Volume 55, Issue 8, 1662- 1671 (2011).

[27] M. Govindaranjan, R. M. Chandrasekaran: “Intrusion detection using neural based hybrid classification methods.” In: Computer networks Volume 55, Issue 8, 1662- 1671 (2011).