International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 1 | Issue – 6

Real Time Intrusion Detection System using Computational Intelligence and Neural Network: A Review

Dr. Prabha Shreeraj Nair
Dean Research, Tulsiramji Gayakwade Patil College of Engineering and Technology, Nagpur

ABSTRACT

Today, Intrusion detection system using neural network is interested and measurable area for the researchers. The computational intelligence describe based on following parameters such as computational speed, adaptation, error resilience and fault tolerance. A good intrusion detection system must be satisfied adaptable as requirements. The objective of this paper, provide an outline of the research progress via computational intelligence and neural network over the intrusion detection. In this paper focused, existing research challenges, review analysis, research suggestion regarding Intrusion detection system.

Keywords: Intrusion detection; neural network; computational intelligence;

I. INTRODUCTION

Intrusion prevention methodology such as access control, firewalls or encryption, unable to completely protected the network during malwares and attacks. Thus, intrusion detection systems (IDS) address the solution of these securities over protection of system or widespread network.

In intrusion detection system, patterns of intrusion obtain on the basis of compare audit data to detection model. Outcomes obtain into two phase that is intrusion attempt or unsuccessful intrusion attempt, both are help for intrusion identities. Intrusion detection model[1] concentrate attention in 1987, at that time when researchers focused on practically implementation of these aspects. In 1990, a new approach has arrived that are combination of statistical aspects and expert system regarding detection of normal and abnormal behavior of automated system or manually transmission over network. Set of training data generated via machine learning approach and artificial intelligence. Generally, set of training data prepared with the help of following techniques that is classification, data clustering and rule based induction.

In intrusion detection problems, data is not trivial when process of automatically constructing models. There are challenges to define outline between normal and abnormal behavior during unbalance node and high traffic of network so as per requirement dynamically adaptation must be satisfies. As per requirement of high detection accuracy with respect to time, machine learning and artificial intelligence have limitation. However, in this circumstances computational intelligence approach play very important roll due to it is able to handle fault tolerance and adaption at the noisy information over the network.

The objective of this paper highlight challenges, review and suggestion regarding common mistakes done by researcher for intrusion detection models using computational intelligence (CI) and neural network.

II. RELATED WORK

A. Intrusion detection

The working strategy of intrusion detection system is that run time analysis or runtime monitoring over the system or network. Thus it is able to decide, whatever

events running on that are normal or abnormal with respect to system or network

[1] Organization of intrusion detection system as figure 1, here data /control flow indicated by solid lines and responses to intrusive activities indicated by dashed lines.

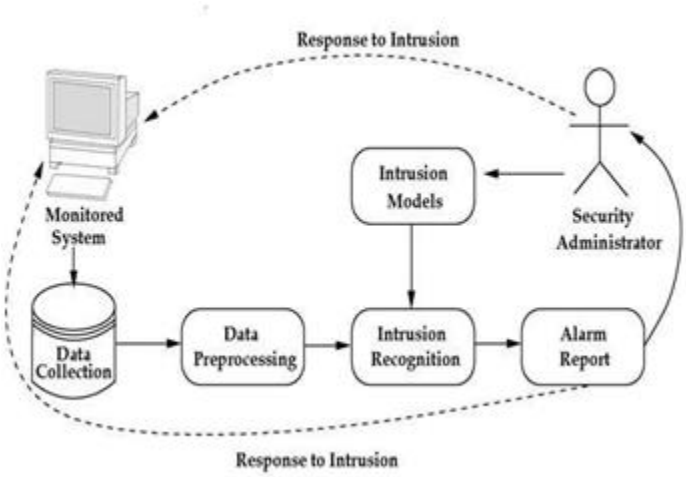

Fig 1: Organization of intrusion detection system

In intrusion detection system based on anomaly detection and misuse detection, its divided into two phases.

Misuse detection, working strategy is that outcomes of data compare to predefined intrusive behavior and based on this matching phenomena observed the intrusions with better accuracy. So due to this strength, its adopted into commercial projects. Sometime intrusions are unexpected means that unable to predict the behavior then misuse detection has unable to solve such issue that is limitation of misuse detection for example facing unknown intrusions. As a solution of this issue is that continually run time updated the knowledge database as per requirement of supervised learning algorithms.

It is challenging and costly task for prepared dataset when its run time change, its behavior or depends on type of intrusions. The alternate solution of this issue solve by Denning [5], using anomaly detection model.

In the anomaly detection, let us consider that abnormal behavior observed rarely and its symptoms or behavior different from normal behavior. Therefore, anomaly detection observed by monitoring the behavior models and compares it from normal behavior. Based on observation, anomaly detection divided into two categories static and dynamic [6]. In static anomaly detection indicates that behavior of intrusion never changes. The real time example is system call of operating systems.

In dynamic anomaly detection, check and extract the profile of end user on the basis of history or predict habit based on previous profile data corresponding to particular profile.

As a working strategy of anomaly detection, we can conclude that it is easily identify new types of intrusions and required only profiles data. The challenging task is that identify the outline normal and abnormal behavior. Secondary challenges are runtime changes of normal behavior to abnormal behavior. Thus, for better accuracy we have used some addition categories of intrusion detection system as soon in figure 2.

B. Computational intelligence

Computational Intelligence is logical approach [7]; here whatever agent we have design work as intelligent agents. It has ability to understand the situation or limitation of particular scenario and take the decision according to them for finite computation, it learn from experiences and flexible for integrity, fault tolerance and adaption.

According to Bezdek[8];

Any system is consider the computational intelligent [8]when it has capability pattern/features recognition at only numerical workload and observed pattern dummy for in terms of knowledge regarding artificial intelligence; and it has capability to manage following parameters such error rates, fault tolerance, numerical adaptively corresponding to human performance.

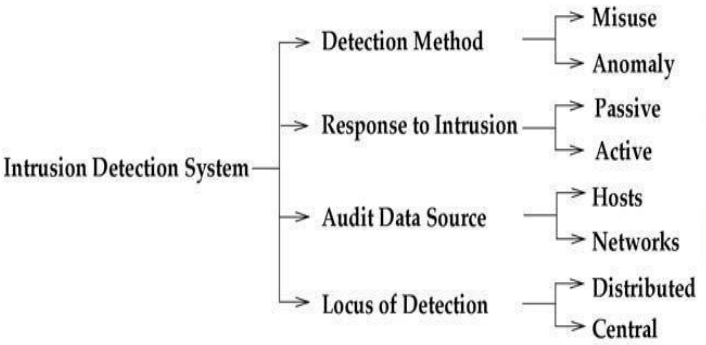

Fig 2: Characteristics of Intrusion detection systems over a network

Based on observed data, intrusion detection techniques categories into parts: anomaly detection and misuse detection. In misuse detection, working

strategy is that identifies and compared observed data with predefined behavior of intrusive. Thus effective outcomes obtain with low false alarm rate. Due to this strength and advantage, it's used in commercial projects. Behaviors of intrusion are unpredictable and may be change in run time then it's unable to handle by misuse detection. For example if we have found any unknown intrusion; that is limitation of misuse detection.

The address of solution for this issue into anomaly detection, in which updated the knowledge database as per run time requirement with the help of supervised learning algorithms. The task for run time updating the database may be costly and challenging at run time, in order to consider the better accuracy analysis of profile and predict behavior of end user[1].

III. ALGORITHMS

Address the solution of intrusion detection system, there are following aspects are possible as per dynamic requirement.

A. Artificial neural networks

Neurons are basic processing unit of artificial neural networks (ANN) that are fully connected basis on topology. ANN is update or enhanced learning by its experiences and generalized the outline of the system from noisy data, limited or incomplete data. It is successfully wide spectrum over datasets.

A.1 Supervised learning

Supervised learning is first simplest and arguable artificial neural network devise are feed forward neural networks. Supervised learning divided into two types: forward neural and multi layered feed forward.

Multilayered feed forward back propagation (MLFF-BP)[9,10] is capable to handle work at user behavior on the following aspects such as host address of login, command sets, difference between normal and abnormal behavior[10], so this techniques used into anomaly detection of intrusion system When automated intrusion detection system has arrived then researcher focused on predicts software behavior using sequences of system calls. According to Ghosh et al. observed that system call more stable compare to commands, in it proposed[12] approach apply the DARPA BSM98 dataset[11].

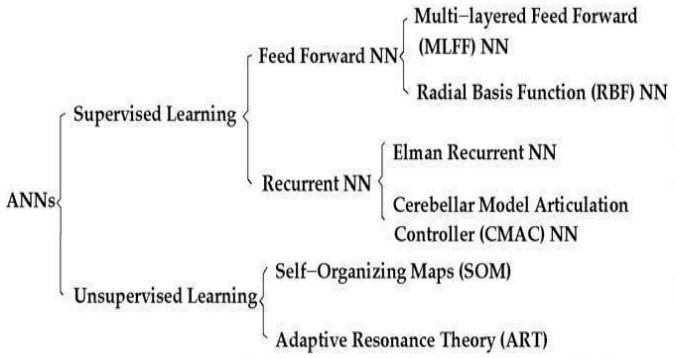

Fig 3: Categories of Artificial Neural Networks

A.2 Unsupervised learning

Unsupervised neural networks are two typical categories adaptive resonance theory and self-organizing maps. As the statistical clustering algorithms, it has group objects. Unsupervised learning is suitable for intrusion detection tasks for normal behavior.

A.2.1 Self-organizing maps

Kohonen maps or Self-organizing maps (SOM) is feed forward networks single-layer, outputs are clustered 2D or 3D grid [13]. Based on their similarity, we preserve topological relationships for the input data.

Self-organizing maps used anomaly detection for trained datasets. It able to detect viruses [14] over multiuser machine in 1990. After few time, some researchers [15,20] focused on Self-organizing maps for extract pattern or feature of general system events. Thus, self organizing map are used into misuse intrusion detection system.

A.2.2 Adaptive resonance theory (ART)

The adaptive resonance theory is capable of handle wide spread of neural network models in terms of pattern recognition, efficiency of unsupervised/ supervised learning. Unsupervised learning models associated with Fuzzy ART , ART-version.(version are 1,2,3) and supervised networks are Fuzzy ARTMAP and Gaussian ARTMAP.

IV. DATASETS AND PERFORMANCE EVALUATION TECHNIQUES

There are few misconception, we are observe during review process and try to addresses the solution with respect to standards datasets.

Generally, in the reviewed research work data are collected from three sources: log files, data packets, CPU/memory usage and system call sequences. We represent benchmarks regarding intrusion detection datasets as describe in Table 1. Researchers free to use these datasets either anomaly detection and misuse detection. We categories two benchmarks datasets that are the KDD99 and DARPA-Lincoln. MIT's Lincoln laboratory, collect the DARPA-Lincoln datasets, the implementation of intrusion detection techniques. In 1998, collection of datasets into two categories that are training data and test data during few weeks.

Table 1: Datasets for Intrusion detection system

Source of Data	Dataset name	Notation
Traffic into	TCP Dump File for DARPA in	
Network	1998[15]	DARPA98
	TCP Dump File for DARPA in 1999	
	[15]	DARPA99
	Datasets of KDD99 [17]	KDD99
	Datasets of 10% KDD99 [17]	KDD99-10
	Internet Exploration Shootout	IES
	Datasets [18]	
User behavior	Datasets of UNIX [19]	UNIXDS
System call	BSM File of DARPA in 1998[15]	BSM98
Sequences		
	BSM File of DARPA in 1999 [15]	BSM99
	Datasets of New Mexico [6]	UNM

A. Performance evaluation Strategy

The intrusion detection systems are effectiveness evaluation if it is able to produce correct predictions. In real time scenario when we are compared prediction to actual outcomes with respect to intrusion detection system, then obtain four possibility such as true negatives, true positive, false positive and false negatives called as confusion matrix. True negatives and true positives obtain respectively if successfully execute the events. False positives indicate general events corresponding to predict as attacks; false negatives are observe if wrong predicted for normal events. In this way, performance of intrusion detection system observes the confusion matrix value.

V. SUMMARY AND SUGGESTION

Here we have focused artificial neural networks and computational intelligence over intrusion detection. Therefore, various unsupervised and supervised artificial neural network are associated anomaly and misuse detection techniques.

Few researchers [21,22] focused on the contradictory approach of artificial neural networks. In this strategy, reduce the training time and cluster approach to address the solution retraining problem of artificial neural network if facing a new class of data; Hofmann et al. [22] proposed solution for black box nature of artificial neural network via if–then rules over trained artificial neural network For the purpose of improve detection accuracy; there are following practices useful in real time scenario at artificial neural network:

- ***Temporal locality property:***

It is useful property or parameters for normal or intrusive behavior regarding intrusion detection domain. Generally, time stamp of artificial neural network represented into two modes implicitly or explicitly. Conclude that under the mode of explicitly representation [23, 24] of time unable to produce accurate identify intrusions. Either we selected implicit mode of representing time, at that time required short-term memory. Due to better utilization of bandwidth vector concept is used over sliding windows. Another secondary strategy, evaluate time

difference between two events, leaky bucket algorithm, chaotic neurons, layer-window statistical preprocessors. Thus, temporal locality property play important role in design and analysis of artificial neural network detection technique.

➢ ***Network infrastructure*:**

Prediction of intrusions is difficult task and involvement of intrusion are continuously process. We are unable to predict attackers objective for example sometimes it's interested into protocol, operating system or application based attacks. So it's unable to insure that single neural network has successfully addresses the solution.

➢ ***Datasets and features:***

Neural networks have recognized corresponding to input datasets. The training datasets has limitation for unknown feature pattern extraction due to dependency of input datasets. We obtain complete training set [16,20] with respect to more network patterns. Based on selection of optimal feature sets affect the performance improvements. Sarasamma et al.[25] proposed different subsets of workload of features, for the purpose of searching fixed categories of attacks. According to Kayacik et al. [26] proposal, hierarchical self organizing maps framework over the KDD99 data, it has observe that six fundamental features of sufficient for recognizing a wide scope over denial of service attacks.

VI. CONCLUSION

It is observed that this research paper focused on analysis, review and summary with suggestion regarding existing challenges for intrusion detection system using computational intelligence and neural network. It's described misconception and suggestion regarding same. On the basis of identities for intrusion detection system, soft computing play important role in such a way, disadvantages superimpose and offer better solutions. However, computational intelligence and neural network addresses the solution for intrusion detection system.

REFERENCES

1. D.E. Denning, An intrusion detection model, IEEE Transactions on Software Engineering 13 (2) (1987) 222–232 (Special issue on Computer Security and Privacy).
2. H. Debar, M. Dacier, A. Wespi, Towards a taxonomy of intrusion-detection systems, Computer Networks 31 (8) (1999) 805–822.
3. S. Chebrolu, A. Abraham, J.P. Thomas, Feature deduction and ensemble design of intrusion detection systems, Computers & Security 24 (4) (2005) 295–307.
4. H. Debar, M. Dacier, A. Wespi, Towards a taxonomy of intrusion-detection systems, Computer Networks 31 (8) (1999) 805–822.
5. D.E. Denning, An intrusion detection model, IEEE Transactions on Software Engineering 13 (2) (1987) 222–232.
6. S. Chebrolu, A. Abraham, J.P. Thomas, Feature deduction and ensemble design of intrusion detection systems, Computers & Security 24 (4) (2005) 295–307.
7. D. Poole, A. Mackworth, R. Goebel, Computational Intelligence—A Logical Approach, Oxford University Press, Oxford, UK, 1998, ISBN-10:195102703.
8. J.C. Bezdek, What is Computational Intelligence? Computational Intelligence Imitating Life, IEEE Press, New York, 1994, pp. 1–12.
9. K. Tan, The application of neural networks to unix computer security, in: Proceedings of IEEE International Conference on Neural Networks, vol. 1, Perth, WA, Australia, November/December 1995, IEEE Press, 1995, pp. 476–481.
10. J. Ryan, M.J. Lin, R. Miikkulainen, Intrusion detection with neural networks, Advances in Neural Information Processing Systems 10 (1998) 943–949.
11. A.K. Ghosh, A. Schwartzbard, A study in using neural networks for anomaly and misuse detection, in: Proceedings of the 8th USENIX Security Symposium, vol. 8, Washington, DC, USA, 23–36 August, (1999), pp. 141–152.
12. A.K. Ghosh, J. Wanken, F. Charron, Detecting anomalous and unknown intrusions against programs, in: Proceedings of the 14th Annual Computer Security Appli-cations Conference (ACSAC'98), Phoenix, AZ, USA, 7–11 December 1998, IEEE Computer Society, 1998, pp. 259–267.

13. T. Kohonen, Self-organizing Maps, volume 30 of Springer Series in Information Sciences, 3rd edition, Springer, Berlin, 2001.

14. K. Fox, R. Henning, J. Reed, A neural network approach toward intrusion detec-tion, in: Proceedings of the 13th National Computer Security Conference, vol. 1, Washington, DC, USA, 1–4 October 1990, (1990), pp. 124–134.

15. The DARPA-Lincoln Dataset. Retrieved January 26, 2008, from http://www.ll.mit. edu/IST/ideval/data/data_index.html.

16. A. Abraham, R. Jain, Soft computing models for network intrusion detection systems, in: S.K. Halgamuge, L. Wang (Eds.), Classification and Clustering for Knowledge Discovery, volume 4 of Studies in Computational Intelligence, Springer, Berlin/ Heidelberg, 2005, , pp. 191–207, chapter 13.

17. The KDD99 Dataset. Retrieved January 26, 2008, from http://kdd.ics.uci.edu/ databases/kddcup99/task.html.

18. The Internet Exploration Shootout Dataset. Retrieved, 2008, from http://ivpr.cs.uml.edu/shootout/network.html.

19. The New Mexico Dataset. Retrieved January 26, 2008, from http://www.cs.unm. edu/~immsec/systemcalls.htm.

20. The Unix User Dataset. Retrieved January 26, 2008, from http://kdd.ics.uci.edu/ databases/UNIX_user_data/UNIX_user_data.html

21. E. Cheng, H. Jin, Z. Han, J. Sun, Network-based anomaly detection using an elman network, in: X. Lu, W. Zhao (Eds.), Networking and Mobile Computing, volume 3619 of Lecture Notes in Computer Science, Springer, Berlin/Heidelberg, 2005, 471–480.

22. A. Hofmann, C. Schmitz, B. Sick, Rule extraction from neural networks for intrusion detection in computer networks, in: IEEE International Conference on Systems, Man and Cybernetics, vol. 2, 5–8 October 2003, IEEE Press, 2003, pp. 1259–1265.

23. P. Lichodzijewski, A. Zincir-Heywood, M.I. Heywood, Host-based intrusion detection using self-organizing maps, in: The IEEE World Congress on Computa-tional Intelligence, International Joint Conference on Neural Networks (IJCNN'02), vol. 2, Honolulu, HI, USA, 12–17 May 2002, IEEE Press, 2002, pp. 1714–1719.

24. M. Amini, R. Jalili, H.R. Shahriari, RT-UNNID: a practical solution to real-time network-based intrusion detection using unsupervised neural networks, Com-puters & Security 25 (6) (2006) 459–468.

25. S.T. Sarasamma, Q.A. Zhu, J. Huff, Hierarchical kohonenen net for anomaly detection in network security, IEEE Transactions on Systems, Man and Cyber-netics - Part B 35 (2) (2005) 302–312.

26. H.G. Kayacik, A.N. Zincir-Heywood, M.I. Heywood, A hierarchical SOM-based intrusion detection system, Engineering Applications of Artificial Intelligence (2007) 439–451.

27. Jabez Ja, B.Muthukumarb, Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach, International Conference on Intelligent Computing, Communication & Convergence, Procedia Computer Science 48 (2015) 338 – 346.