RESEARCH ARTICLE OPEN ACCESS

A survey on RBF Neural Network for Intrusion Detection System

Henali Sheth*, Prof. Bhavin Shah**, Shruti Yagnik***

*(Department of Computer Engineering, L.J. Institute of Engineering & Technology, Ahmedabad, India. Email: hvs.sweety@gmail.com.)

** (Associate Professor, M.C.A Programme, L.J. Institute of Management studies, Ahmedabad, India. Email: bms_mca@yahoo.com)

*** (Department of Computer Engineering, L.J. Institute of Engineering & Technology, Ahmedabad, Gujarat, India. Email: shruya@gmail.com)

ABSTRACT

Network security is a hot burning issue nowadays. With the help of technology advancement intruders or hackers are adopting new methods to create different attacks in order to harm network security. Intrusion detection system (IDS) is a kind of security software which inspects all incoming and outgoing network traffic and it will generate alerts if any attack or unusual behavior is found in a network. Various approaches are used for IDS such as data mining, neural network, genetic and statistical approach. Among this Neural Network is more suitable approach for IDS. This paper describes RBF neural network approach for Intrusion detection system. RBF is a feed forward and supervise technique of neural network.RBF approach has good classification ability but its performance depends on its parameters. Based on survey we find that RBF approach has some short comings. In order to overcome this we need to do proper optimization of RBF parameters.

Keywords – Immune Radial Basis Function (IRBF), Intrusion Detection System (IDS), Multiple Granularities Immune Network (MGTN), Neural Network, Particle swarm optimization (PSO), Radial basis function (RBF).

I. INTRODUCTION

In this era of computer, use of Internet is increasing day-by-day. According to the Symantec Internet Security Threat Report 2014, 2013 was the year of Mega Breaches [22]. Security threats are increasing in order to harm network or system and compromise information security through malicious activities or through security policy violations. It has brought unprecedented chances and challenges to the society for security purpose. Traditional protection techniques such as user authentication, data encryption, avoiding programming errors and firewalls are generally unable to protect against malicious activity [17]. Intrusion detection system (IDS) is used to detect attacks which are not detected by traditional tools & techniques as mentioned above. In 1980 firstly Anderson developed such IDS which was able to detect the attack with more accuracy as compared to traditional security tools [1].

Various approaches are adopted to build IDS using different techniques like statistical models, Data Mining base Methods, Neural Network, Rule based systems, Genetic Algorithms, State transition based, and Expert based System as described in [5]. Out of these neural network based model have become a promising AI approach for IDS [3]. Among various Neural Network based approaches RBF is proven technique which has been already used in [3] [4] [5] [6] [7] [8] [9] [10] [11] and [12]. RBF neural network has some advantages like good approximation ability, better classification and fast learning speed over back propagation (BP) neural network. RBF will have a broad future in the research field of intrusion detection [5].

In this paper section II & section III describes IDS and types of attacks respectively. Section IV includes RBF approach. Then section V contains literature survey. Comparison and discussion is included in section VI. Section VII contains conclusion.

II. INTRUSION DETECTION SYSTEM

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations [2] [15] [18]. IDS detects attacks and generate alerts [2]. But Intrusion Prevention System (IPS) has feature of detection and prevention. IPS takes manual or auto action such as drop or block or terminates the connection [13]. Many organizations are using Intrusion Detection & Prevention System (IDPS) nowadays [13]. The simple structure of IDS is as shown in following Figure-1.

As per the Figure-1 all network traffic is captured and stored. Then data is given to preprocessing module. Afterwards data is normalized. And it is given to intrusion detection engine where detection and learning is done based on knowledge & behavior fetch from database. Then alerts are generated and reported to administrator or IPS or log auditing is done.

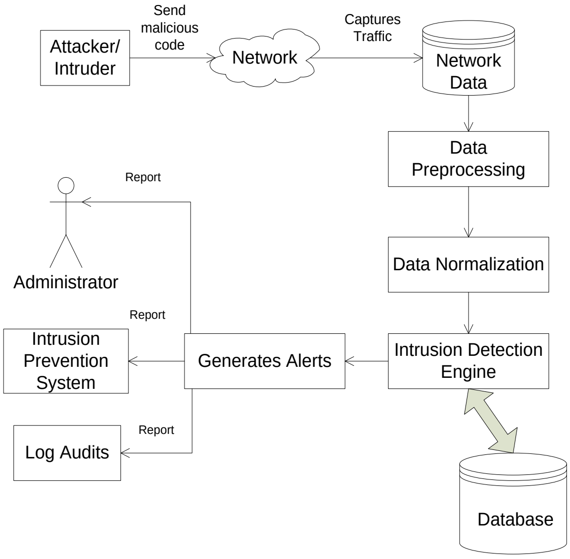

Figure:-1. The general view of intrusion-detection system.

On the basis of source of data, IDS can be classified into host-based and network-based [5] [14] [15]:

1) Host-based IDS: This detects attacks by inspecting a single host and collecting audit data from host audit trails [5] [14]. They are application specific, has detailed signature and better for detecting attacks from inside [18] [19].
2) Network-Based IDS: It analyzes network traffic and evaluates information capture from network connection [14]. NIDS is better for detecting attacks from outside [19].

Further, on the basis of the detection technique, IDS can be classified as misuse detection or anomaly detection. Misuse detection relies on patterns of known intrusions [19]. In anomaly detection unknown attacks or unusual behavior in network are inspected. It is very difficult to detect such unusual behavior which leads to high false rate [19].

III. Types of Attacks

There are different types of attacks in network as described in [5][25]. These attacks are categorized into following four main groups: 1) **Denial of Service (DOS):** This attack will deny legitimate user requests to a system e.g. flood. 2) **User-to-Root (U2R):** In this attack hacker starts off on the system with a normal user account and attempts to abuse vulnerabilities in the system in order to gain super user privileges e.g. perl, xterm 3) **Remote-to-Local (R2L):** In this attack, hacker gets unauthorized access from a remote machine e.g. guessing password. 4) **Probe attack**: It is a surveillance attack. In this hacker scan system or network and find its vulnerabilities e.g. port scanning.

IV. Radial basis Function (RBF)

RBF was first introduced in the solution of the real multivariable interpolation problem by Broomhead & Lowe (1988) and Moody & Darken (1989) [23] [24].It is a kind of local approximation neural network, which has very strong approximation ability, good classification ability and rapid learning speed [20]. Different applications of RBF are pattern classification, curve fitting, function approximation, time series prediction and control system.

RBF neural network is a feed forward network and it has simple structure [20]. The structure of RBF neural network is as shown in Figure-2 [24]. It has three layers known as input layer (x), hidden layer which includes radial basis function, and output layer (y) which is linear summation of hidden layer [16]. The neurons in the hidden layer commonly contain Gaussian transfer functions whose outputs are inversely proportional to the distance from the center of the neuron [4]. The connection weight (w) between hidden layer and output layer is adjusted. Input layer achieve non-linear mapping and output layer realize on linear mapping [20].

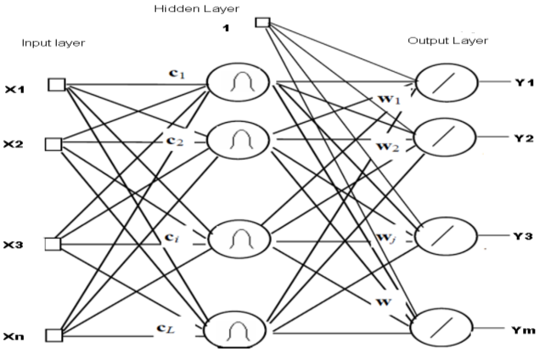

Figure:-2 The structure of RBF [24]

Training procedure of RBF network is divided into two phases: Unsupervised learning and Supervised Learning [8].During both the learning, the choice of the parameters has an important influence on the classification performance of RBF neural network. Following is the list of such parameters.

1. The number of neurons in the hidden layer.
2. The coordinates of the center of hidden-layer
3. The radius (spread) of each RBF function in each dimension.
4. The weights between hidden & output layer.

V. Literature Survey

In this section different research papers based on RBF approach for IDS which have been reviewed are included.

- An IDS based on RBF neural Network [6]

The objective of this paper is to shows how well RBF neural network can distinguish the known intrusion behavior and new intrusion behavior with high detection rate. Authors had implemented their model on KDD CUP 1999 dataset and also on real network traffic of Shanhua Company. Authors had compared their RBF implementation with BP Neural Network. During such comparison they found that RBF has better detection rate as compare to BP. During their implementation authors had recorded 97.6% as detection rate and 1.6% as false positive rate with 4s training time.

- RBF based Real time Hierarchical IDS [7]

Authors used hierarchical IDS which has Serial hierarchical IDS (SHIDS) and Parallel hierarchical IDS (PHIDS) layers. The objective of the model is to support real time traffic monitoring, detecting anomalous activity by modifying the internal structure.

As per the authors, initially SHIDS will have single layer and more layers will be added as new attack group has been given. Such structure suffers from single point of failure as the layers are arranged in a sequential manner. To overcome this, authors proposed PHIDS. During their implementation authors found that deciding the threshold value which is used to identify the anomaly, is difficult.

- NIDS method based on RBF neural network [8]

.Objective of this paper is to support rapid and effective intrusion detection. Authors have compared the RBF with BP Neural Network. During such comparison authors found that RBF has less training and testing error, less average iteration time, faster convergence rate. Still it suffers from high false alarm rate.

- Application of PSO-RBF Neural Network in Network Intrusion Detection [9]

Authors had combined RBFNN and Particle swarm optimization (PSO) algorithm in order to increase detection rate of NIDS.PSO algorithm is used to optimized RBF parameters. During their implementation authors had found that PSO-RBF performance is superior to conventional RBFNN. But PSO algorithm suffers from local minima, premature convergence and high false alarm rate.

- QPSO optimized RBF network for anomaly detection [10]

Author Yuan Liu has proposed a novel hybrid algorithm used with RBFNN for anomaly detection. This algorithm is combination of Quantum behave PSO (QPSO) and gradient descent which is used to train the RBFNN. During implementation author had compare QPSO-RBF, GD-RBF and QPSO-GD-RBF approaches. During such comparison author found that detection rate of QPSO-GD-RBF is 96.77% which is higher than others. But one short coming of this approach is that false positive rate is still high.

- IDS based on Adaptive RBF neural network [11]

Authors had implemented a new method such as multiple granularities immune network (MGIN) to design a classifier for intrusion. Authors had first use MGIN to find the candidate hidden neurons. Further they remove some redundant hidden neurons by employing preserving criterion.

Authors had compared this combine approach with BPNN. They found that BPNN has best result for detection rate and false positive than RBF. Authors also found that BP is difficult to use for high dimensional pattern classification problem and it does not converge well. During their implementation authors had also compared this new algorithm with traditional RBF. They found that this approach has better detection rate and low false positive rate than traditional RBF.

- Application study on Intrusion Detection System using IRBF [4] [12]

The objective of this paper is to improve convergence speed and precision of RBF neural network. For this authors had used RBF based on immune recognition algorithm (IRBF). Input data are regarded as antigens and antibodies are regarded as the hidden layer centers. Weights of output layer are determined by adopting the recursive least square method.

During their implementation authors had recorded 83.7% detection precision for all type of attack. Further author also found that IRBF has high precision, less computation time, faster convergence speed and good real time performance. But still false positive & false negative exists and IRBF is unable to detect all type of invasion.

VI. Comparison and Discussion

The objective of this paper is to find current challenges of RBF approach for Intrusion detection. Basic comparison is shown in Table 1. From that table following are the current challenges:1) Response time [7]. 2) High false alarm rate [4] [8] [9] [10] [11] [12].

1) Response time:

As per literature survey and comparison Table-1, one problem is that response time is high for SHIDS [7]. Response time is high, because SHIDS used sequential layered approach for classifying intrusion. To overcome this PHIDS is used as in[7].PHIDS used parallel layered approach so response time is reduced. In this approach parallel implementation is done so it will avoid single point failure problem. While SHIDS suffers from single point failure, this also increases response time.

2) High false alarm rate:

From comparison Table-1major current challenge is high false alarm rate. False alarm rate is high if there is no proper training of RBFNN. To overcome this problem proper parameter tuning is required. From our literature review we found that false alarm rate can be reduced by optimizing the following parameters.

- Number of neurons in hidden layer: If numbers of neurons in hidden layer are too high then RBFNN will have poor generalization and also suffers from over training. If numbers of neurons are insufficient then RBFNN cannot learn the data adequately. So it will lead to slow convergence. Therefore number of neurons in hidden layer will affect false alarm rate. To reduce false alarm rate number of neurons in hidden layer must be properly chosen. MGIN algorithm is used for hidden layer neuron selection [11].
- Location of centre and width spread: Location of center is important because if input is closer to center then it has better classification. So locating centers are important for better RBF performance which in turn reduce false alarm rate. K-nearest neighbor & clone selection algorithm is used for center selection [4] [8] [12]. Sometime centers are selected randomly. We need to select width parameter in order to properly distinguish between classes. So location of center and width must be properly chosen to reduce false alarm rate.
- Weight: It is used between hidden layer and output layer for linear summation. This weight is adjustable and so it affects false alarm rate. Recursive least mean square method is used to adjust weight [4] [12].

From above discussion it is clear that RBFNN performance depends on its parameters. Therefore proper optimization of RBF parameter is required. Various optimization algorithms are used such as PSO, QPSO and IRBF [4] [9] [10] [12].

VII. CONCLUSION

This paper concludes that RBF network can be used to detect anomaly detection and Misuse detection. If sequential layered approach such as SHIDS is used for intrusion detection then response time will increase. This problem is avoided by using parallel approach such as PHIDS. Moreover RBFNN performance depends on its parameters. Based on comparison and discussion proper optimization of RBF parameters is required in order to reduce false alarm rate.

DECLARATION

The content of this paper is written by Author 1(Henali Sheth) while Author 2(Prof. Bhavin shah) had guided the work and Author 3(Shruti yagnik) has reviewed this paper. Hence Author 1 is responsible for the content and issues related with plagiarism.

References

[1] J. P. Anderson, Computer Security Threat Monitoring and Surveillance. Technical Report, Fort Washington, PA (1980).

[2] Z.J. Tang et al. Intrusion detection. Tsinghua University Press. 2004, chap 2, pp 6-8.

[3] Yanwei, Fu, Zhu Yingying, and Yu Haiyang. "Study of neural network technologies in intrusion detection systems." *Wireless Communications, Networking and Mobile Computing, 2009. WiCom'09. 5th International Conference on. IEEE, 2009.*

[4] Yichun, Peng, Niu Yi, and Hu Qiwei. "Research on Intrusion Detection System Based on IRBF." *Computational Intelligence and Security (CIS), 2012 Eighth International Conference on. IEEE, 2012.*

[5] Devaraju, S., and S. Ramakrishnan. "Performance analysis of intrusion detection system using various neural network classifiers." *Recent Trends in Information Technology (ICRTIT), 2011 International Conference on. IEEE, 2011.*

[6] Yang, Zhimin, et al. "An intrusion detection system based on RBF neural network." *Computer Supported Cooperative Work in Design, 2005. Proceedings of the Ninth International Conference on. Vol. 2. IEEE, 2005.*

[7] Jiang, Ju, Chunlin Zhang, and M. Kamel. "RBF-based real-time hierarchical intrusion detection systems." *Neural Networks, 2003. Proceedings of the International Joint Conference on*. Vol. 2. IEEE, 2003.

[8] Tian, Jingwen, Meijuan Gao, and Fan Zhang. "Network intrusion detection method based on radial basic function neural network." *E-Business and Information System Security, 2009. EBISS'09. International Conference on*. IEEE, 2009.

[9] Chen, Zhifeng, and Peide Qian. "Application of PSO-RBF neural network in network intrusion detection." *Intelligent Information Technology Application, 2009. IITA 2009. Third International Symposium on*. Vol. 1. IEEE, 2009.

[10] Liu, Yuan. "Qpso-optimized rbf neural network for network anomaly detection."*Journal of Information & Computational Science* 8.9 (2011): 1479-1485.

[11] Zhong, Jiang, et al. "Intrusion detection based on adaptive RBF neural network."*Intelligent Systems Design and Applications, 2006. ISDA'06. Sixth International Conference on*. Vol. 2. IEEE, 2006.

[12] Peng, Yichun, et al. "Application Study on Intrusion Detection System Using IRBF." *Journal of Software* 9.1 (2014): 177-183.

[13] Ashoor, Asmaa Shaker, and Sharad Gore. "Difference between Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)." (2011).

[14] Ashoor, Asmaa Shaker, and Sharad Gore. "Importance of Intrusion Detection system (IDS)." *International Journal of Scientific and Engineering Research* 2.1 (2011): 1-4.

[15] Niu, Yi, and Yi Chun Peng. "Application of Radial Function Neural Network in Network Security." *Proceedings of the 2008 International Conference on Computational Intelligence and Security-Volume 01*. IEEE Computer Society, 2008.

[16] Liu, Yinfeng. "An improved RBF neural network method for information security evaluation." *TELKOMNIKA Indonesian Journal of Electrical Engineering* 12.4 (2014): 2936-2940.

[17] Govindarajan, M. "Hybrid Intrusion Detection Using Ensemble of Classification Methods." *International Journal of Computer Network & Information Security* 6.2 (2014).

[18] Debar, Herve. "An introduction to intrusion-detection systems." *Proceedings of Connect* 2002 (2000): 77.

[19] Chowdhary, Mahak, Shrutika Suri, and Mansi Bhutani. "Comparative Study of Intrusion Detection System." (2014).

[20] Chun-tao, Man, Wang Kun, and Zhang Li-yong. "A new training algorithm for RBF neural network based on PSO and simulation study." *Computer Science and Information Engineering, 2009 WRI World Congress on*. Vol. 4. IEEE, 2009.

[21] Er, Meng Joo, et al. "Face recognition with radial basis function (RBF) neural networks." *Neural Networks, IEEE Transactions on 13.3 (2002): 697-710.*

[22] Symantec Corporation, Internet Security Threat Report (ISTR), 2013 Trends, Volume 19, Published April 2014. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

[23] Broomhead, David S., and David Lowe. Radial basis functions, multi-variable functional interpolation and adaptive networks. No. RSRE-MEMO-4148. ROYAL SIGNALS AND RADAR ESTABLISHMENT MALVERN (UNITED KINGDOM), 1988.

[24] Ugur Halici. Artificial Neural Network. Chapter 9. Radial basis function Network .EE543 lecture notes. Metu EEE. Ankara 139.

[25] KDD dataset, 1999; http//kdd.ics.uci.edu/databases/-kddcup99/kddcup99.html.

Table 1: Comparison Table

Techniques Used in different papers	Objective	Dataset used for training & testing	Advantages	Disadvantage
Only RBF [6]	Finds if RBF can distinguish the known and unknown intrusion with high exactness.	KDD CUP 1999	-Better approximation than BP -good Classification -faster learning -training step fewer	- performance needed to be improved.
RBF for Hierarchical IDS(serial & parallel) [7]	Two hierarchical IDS are proposed based on RBF to monitor network traffic in real-time, train new classifier and modify their structure adaptively.	KDD CUP 1999	-better than BP -SHIDS use for monitoring real traffic -Structures update automatically. -PHIDS is better than SHIDS -PHIDS has less layers	-response time is more. -SHIDS has too many clusters and layers. SHIDS has problem of "single point failure" -In PHIDS it is difficult to choose suitable decision threshold to identify novel intrusion.
RBF and K-NN algorithm [8]	-RBF is used to detect intrusion behavior rapidly and effectively. -Advantages of RBF.	DARPA	-local approaching network so fast learning -fast convergence rate -higher stability -truly detect anomaly intrusion behavior	- requires predominance of RBF to enhance learning ability. -false rate is high
PSO-RBF [9]	To detect all kinds of intrusion efficiently and therefore, the novel combination method based on RBF & PSO is adapted to NIDS.	KDDCUP1999	-used to solve non-linear problem -used for optimization purpose. -superior than conventional RBF neural network	-high false alarm rate.
QPSO-RBF GD-RBF QPSO-GD-RBF [10]	QPSO-GD-RBF, a novel hybrid algorithm proposed for network anomaly detection.	KDDCUP 1999	-better optimization -global searching possible -high detection rate	-false positive rate is still high
RBF-MGIN [11]	This algorithm is used to reduce data & get the candidate hidden neurons & construct an original RBF.	KDDCUP 1999	-advantage of class label. -small network -generalized well -better classification	-detection rate is low than BP. -false positive is also high
IRBF [4] [12]	Hidden layer centers are selected and convergence speed and precision are improved.	KDDCUP 1999	-can distinguish between self and non self -less computation time -faster convergence -high precision -good real time performance. -ability of self learning and self adjusting. - can detect unknown intrusion.	-false positive and false negative still exists. - can't detect all invasion.