International Journal of Engineering Sciences & Emerging Technologies, Mar. 2015.
ISSN: 22316604 Volume 7, Issue 5, pp: 743-752 ©IJESET

NEURAL NETWORK BASED INTRUSION DETECTION SYSTEM AGAINST VARIOUS ATTACKS IN MANET

Pratik Gite, Sanjay Thakur
Department of Computer Science and Engineering,
PAHER University, Udaipur, India

ABSTRACT

Data security and privacy is the primary need of any computer applications and networks. Therefore a number of techniques are recently developed for enhancing the security and trust on network in last few years. Among these applications Intrusion Detection System (IDS) is most essential network analysis and security tool. This paper provides the brief overview and different concepts of IDS and related techniques. As discussed in previous papers, Mobile Ad-hoc Network and its dynamic network topology, open environment and lack of centralized security infrastructure, MANET is very much vulnerable due to presence of malicious node patterns and certain types of attacks. To address these concerns in this chapter a neural network based Intrusion Detection System is proposed to detect various kinds of attacks and threats in MANET. Many security issues and certain attacks that are violating confidentiality, integrity, availability and non-repudiation of networks that can be caused of many intrusions which are increasing rapidly in Mobile Ad-hoc Network due to their Ad-hoc nature. In order to protect such types of attack patterns and malicious node patterns, Intrusion Detection Systems were designed. As per survey, various soft computing based techniques have been proposed for the IDS in last few decades but in this work, a neural network based IDS using back propagation training algorithm with key management techniques is proposed. These IDS systems are trained with normal network behaviour and attack behaviour information and then the system classify normal patterns and attacks patterns as per observation. The main aim of this paper is to provide detailed study of IDS and performance comparison of IDS based techniques with proposed techniques.

KEYWORDS: *Network Security, Intrusion Detection System, Artificial Neural Network, Back Propagation Neural Network, Key Management Technique, Performance Analysis of different IDS Classifier.*

I. INTRODUCTION

IDS systems are a sort of security filter designed using software or hardware configuration for protecting the network. As a result, intrusion detection system (IDS) examines all inbound and outbound network activity such as packet transactions, user activities and recognizes apprehensive patterns. These patterns are analysed using any network administrator defined rules, predefined constrain for network or utilizing machine learning algorithms. That may point towards an attack on network or system commenced by someone attempting to break into or compromise a system. There are several tactics to categorize IDS [1][5][6]:

Misuse detection vs. anomaly detection: In misuse detection, the IDS analyse the information it congregates and compares it to large databases of attack signatures. In effect, the IDS look for a definite attack that has already been documented. Similar to a virus detection system, misuse detection software is only as fine as the database of attack signatures that it used to evaluate packets against. In anomaly detection, the administrator of system identifies the baseline, or usual state of the networks traffic load, breakdown, protocol, and standard packet size. The most popular methods of signature detections are: the Expert System, the Genetic Algorithm and Pattern Matching method that

provides signature of attacks. The anomaly detector supervises segments of network in order to evaluate their position and then compare them to the normal baseline and look for anomalies. The method which is used to calculate user profile for anomaly detection systems are Expert Systems and Neural Network [1].

Network-based vs. host-based systems: In a network-based Intrusion Detection System, (NIDS), the individual packets flowing through a network are analysed. The NIDS can perceive malicious packets that are intended to be overlooked by firewalls simplistic filtering rules. In a host-based system, the IDS inspects at the activity on each individual computer or host. **Passive system vs. reactive system:** In a passive system, the IDS notice a latent security breach, register the information and signal an alert. In a reactive system, the IDS take action towards the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source.

However these both work network security, IDS is dissimilar from a firewall in term that the latter investigates intrusions in order to stop them from happening. The firewall regulates the access between networks so as to put off intrusion and doesn't report an internal network attack. IDS evaluate a suspected intrusion once it has taken place and signal an alarm. IDS also watch for attacks that originate from within a system [7].

Working with all varieties of system is much complex, time consuming and pricey work for us, thus in this critique we work with first kind of system and modify it to make the IDS more strong and getting trustworthy results. Additionally, in our dissertation we include the new pattern detection for newly found attack.

An Anomaly-Based Intrusion Detection System is a system to identify intrusions in computer and exploitation by means of supervising different activities and categorizing either as normal or abnormal. The classification is rooted on heuristics or rules, instead patterns or signatures, and will sense any type of misuse that falls out of usual system operation. This is as contrasting to signature based systems which can simply detect attacks for which a signature has formerly been created. In order to find out what attack traffic is, the system ought to be trained to recognize normal system activity. This can be achieved in several ways, most habitually with artificial intelligence kind of techniques. Systems using neural networks have been used to immense effect. An added method is to define what normal usage of the system comprises using a strict mathematical model, and design any deviation from the normal behaviour as an attack. This is identified as strict anomaly detection. According to this all method, the intrusion detection problem is a classification problem. After having these all methods, Specially Neural Networks have the ability to classify all normal patterns and malicious patterns, and thus can be used in other aspects of intrusion detection systems such as attack classification and alert validation. Consequently, neural network models have become a promising AI approach to improve the search for malicious patterns or misuse attempts in the network. Using neural network methods in IDS is also capable of identifying new attacks. The rest of the paper is organized in following manner: Section 2 describes Neural Network Based Approaches on Intrusion Detection Systems. Section 3 represents the Proposed IDS architecture with key management techniques, section 4 provides the future work of Neural Network based technology and finally section 5 conclude the whole paper.

II. RELATED WORK

With the rapid development of wireless networks and computer technology, the number of intrusions into computer network is also growing. So, the network security become more and more important to protects network information from the threats and variety of attacks. The reason is that each and every day, new automated and semi automated tools and techniques are easily appearing and these tools and techniques with variety of system vulnerability are easily available on the internet [1][4]. Behalf of these reasons, to implement and design effective Intrusion Detection Systems is the key challenge for many researchers in the field of security.

Intrusion detection concept was proposed by **James Anderson** in 1980's defined as an intrusion attempt or threat to be potential possibility of a deliberate unauthorized attempt to access information, manipulate or render a system unreliable or unusable [14]. Sights moved for using data mining in content of NIDS in the late of 1990's. Researchers also recognized that the need for existence of standardized dataset to train IDS tool. Minnesota Intrusion Detection System (MINDS) combines

signature based tool with data mining techniques. Signature based tool (Snort) are used for misuse detection & data mining for anomaly detection technique [15]. In this technique [15] **Jake Ryan et al** applied neural networks to detect intrusions. Neural network can be used to learn a print or user behaviour & identify each user. If it does not match then the system administrator can be alerted. A back propagation neural network called NNID was trained for this process.

Denning D.E et al [16] has developed a model for monitoring audit record for abnormal activities in the system. Sequential rules are used to capture a user's behaviour [26] over time. A rule base is used to store patterns of user's activities deviates significantly from those specified in the rules. High quality sequential patterns are automatically generated using inductive generalization & lower quality patterns are eliminated. An automated strategy for generation of fuzzy rules obtained from definite rules using frequent items. The developed system [21] achieved higher precision in identifying whether the records are normal or attack one.

Dewan M et al [17] presents an alert classification to reduce false positives in IDS using improved self adaptive Bayesian algorithm (ISABA). It is applied to the security domain of anomaly based network intrusion detection. **S.Sathyabama et al** [18] used clustering techniques to group user's behavior together depending on their similarity & to detect different behaviours and specified as outliers.

Amir Azimi Alasti et al [19] formalized SOM to classify IDS alerts to reduce false positive alerts. Alert filtering & cluster merging algorithms are used to improve the accuracy of the system.SOM is used to find correlations between alerts.

Alan Bivens et al [20] has developed NIDS using classifying self organizing maps for data clustering. MLP neural network is an efficient way of creating uniform, grouped input for detection when a dynamic number of inputs are present. An ensemble approach [27] helps to indirectly combine the synergistic & complementary features of the different learning paradigms without any complex hybridization. The ensemble approach outperforms both SVMs MARs & ANNs. SVMs outperform MARs & ANN in respect of Scalability, training time, running time & prediction accuracy. This paper [28] focuses on the dimensionality reduction using feature selection. The Rough set support vector machine (RSSVM) approach deploy Johnson's & genetic algorithm of rough set theory to find the reduct sets & sent to SVM to identify any type of new behavior either normal or attack one.

Aly Ei-Senary et al [26] has used data miner to integrate Apriori & Kuok's algorithms to produce fuzzy logic rules that captures features of interest in network traffic. **Taeshik Shon et al** [25] proposed an enhanced SVM approach framework for detecting & classifying the novel attacks in network traffic. The overall framework consist of an enhanced SVM- based anomaly detection engine & its supplement components such as packet profiling using SOFM, packet filtering using PTF, field selection using Genetic Algorithm & packet flow-based data preprocessing. SOFM clustering was used for normal profiling. The SVM approach provides false positive rate similar to that of real NIDSs. In this paper [19] genetic algorithm can be effectively used for formulation of decision rules in intrusion detection through the attacks which are more common can be detected more accurately.

Oswais.S et al [24] proposed genetic algorithm to tune the membership function which has been used by IDS. A survey was performed using approaches based on IDS, and on implementing of Gas on IDS. Machine learning classification algorithm for time series data was proposed by **Sean Davis et al. [23].** They declared that machine learning techniques were used to derive classifiers from set of labeled sequences to achieve adequate performance on the task without over fitting the training data. The intrusion detection system using data mining approaches was proposed by **Wenke Lee et al. [22].** They have suggested that the association rules and frequent episodes algorithms was used to compute the consistent patterns from audit data. This method provides the basi for feature selection and used to discover patterns of intrusions.

Norouzian M.R et al [21] **defined** Multi- Layer Perceptron (MLP) for implementing & designing the system to detect the attacks & classifying them in six groups with two hidden layers of neurons in the neural networks. Host based intrusion detection is used to trace system calls. This system [21] does not exactly need to know the program codes of each process. Normal & intrusive behavior are collected through system call & analysis is done through data mining & fuzzy technique. The clustering and genetic optimizing steps [14] were used to detect the intrude action with high detection rate & low false alarm rate.

III. IDS CLASSIFIER, NEURAL NETWORK AND RELATED TECHNIQUE

Classifiers are the terminology of data mining algorithms or machine learning algorithms. Data mining is a technique which offers to analyse the data and their patterns to distinguish the targeted data among new arrived data. This section provides the understanding of the different techniques of data mining that are utilized for classifying the patterns of KDD CUP datasets. Basically there are two kinds of techniques are available for data analysis supervised and unsupervised. In supervised learning technique the training samples includes the data attributes and their significant class labels. On the other hand in unsupervised learning the data contains only the attributes sets. Most of the IDS design the supervised learning concepts are utilized for pattern recognition; some of these frequently used technologies are SVM, Decision Trees, Bayesian Classifier, KNN, and Neural Network. This section introduces brief overview of neural network based techniques.

Neural network is biologically inspired machine learning technique which is used for pattern learning, classification, predictions and regression analysis. Therefore that is an essential learning method in data analysis and pattern discovery. Artificial neural networks are generally presented as systems of interconnected "neurons" which can compute values from inputs, and are capable of machine learning as well as pattern recognition thanks to their adaptive nature.

Neural networks are similar to biological neural networks in performing functions collectively and in parallel by the units, rather than there being a clear delineation of subtasks to which various units are assigned. The term "neural network" usually refers to models employed in statistics, cognitive psychology and artificial intelligence. Neural network models which emulate the central nervous system are part of theoretical neuroscience and computational neuroscience. The neural network basically composed with the three different layers of neurons first is known as input layer which is used to accept the input values from the data sources second layer is called the hidden layer that is used to process the information through the stored weights and input values. The final layer is known as the output layer that collects the outcomes of the neural network. That is efficient and accurate modelling of data for different intelligence applications.

The neural network can also be defined as an information processing system that is inspired by the way biological nervous systems, such as the brain, process information. It is composed of a large number of highly interconnected processing elements (PEs) working with each other to solve specific problems. The learning process is essentially an optimization process in which the parameters of the best set of connection coefficients (weights) for solving a problem are found and includes the following basic steps: Present the neural network with a number of inputs (vectors each representing a pattern), Check how closely the actual output generated for a specific input matches the desired output, Change the neural network parameters (weights) to better approximate the outputs. To improve the detection efficiency of IDS, Artificial Intelligence technology (such as neural networks, genetic algorithms, fuzzy technology, the theory of immunity) has been applied to intrusion detection system research. This paper mainly introduces five different types of Neural Network based methods being used in IDS: multilayer perceptions (MLP), radial basis function (RBF), self organizing feature map (SOFM), adaptive resonance, theory (ART) and principal component analysis (PCA).

1. MLP: A. Multilayer Perceptions are layered feed forward networks typically trained with static back propagation. These networks have found their way into countless applications requiring static pattern classification. For example, Ryan et al.[4] described an offline anomaly detection system called NNID “Neural Network Intrusion Detector” which utilized a back-propagation MLP neural network. The MLP was trained to identify users' profile and at the end of each log session, the MLP evaluated the users' commands for possible intrusions (offline). The authors described their research in a small computer network with 10 users. One hundred most important commands are used to describe a user's behavior. They used a three layer MLP where two are hidden layers. The MLP identified the user correctly in 22 cases out of 24. The main advantages of this method are that they are easy to use, and that they can approximate any input/output map. The key disadvantages are that they train slowly, and require lots of training data typically three times more training samples than network weights [1].

2. Radical Basis Function: Radial basis function (RBF) networks are nonlinear hybrid networks typically containing a single hidden layer of processing elements (PEs). This layer uses

Gaussian transform functions, rather than the standard sigmoid functions employed by MLPs. The centers and widths of the Gaussians are set by unsupervised learning rules, and supervised learning is applied to the output layer. These networks tend to learn much faster than MLPs. Zhimin Yang et al. [5] discuss the structure and function of intrusion detection system based on RBF. In the experiment of network simulation, continuous training of input normal samples and abnormal sample are used. The result of experiment proves that RBF network is better than BP network in its property of optimal approximation, classify ability and the rapidity of study, RBF can improve the detection performances of IDS. In [6], J. Zhong et al. proposed a new method to design classifier based on multiple granularities immune network. Firstly a multiple granularities immune network (MGIN) algorithm is employed to reduce the data and get the candidate hidden neurons and construct an original RBF network including all candidate neurons. Secondly, the removing redundant neurons procedure is used to get a smaller network. Experimental results on the real network datasets show that the new classifier has higher detection and lower false positive rate than traditional RBF classifier [1].

3. **Self-organizing feature map:** Self-organizing feature maps (SOFMs) transform the input of arbitrary dimension into a one or two dimensional discrete map subject to a topological (neighborhood preserving) constraint. The feature maps are computed using Kohonen unsupervised learning. The output of the SOFM can be used as input to a supervised classification neural network such as the MLP. This network's key advantage is the clustering produced by the SOFM which reduces the input space into representative features using a self-organizing process. Hence, the underlying structure of the input space is kept, while the dimensionality of the space is reduced. Heywood et al. [7][8]described an approach to dynamic intrusion detection using SOFM, and investigated a hierarchical SOFM architecture under two basic feature sets, one is limited to 6 basic features whereas the other contains all 41-features. The authors estimate that "hierarchically built unsupervised neural network approach is able to produce encouraging results". Horeis[9] described and concluded that the combination of RBF and SOFM is convenient to use as an intrusion detection model. They concluded that the 'evaluation of human integration" is necessary to reduce the classification error. Experimental results are promising and show that RBFSOFM achieves, compared to RBF, similar or even better results [1].

4. **Adaptive resonance theory:** The basic Adaptive resonance theory system is an unsupervised learning model, typically consisting of a comparison field and a recognition field composed of neurons, a vigilance parameter, and a reset module. The comparison field takes an input vector (a one-dimensional array of values) and transfers it to its best match in the recognition field. Its best match is the single neuron whose set of weights (weight vector) most closely matches the input vector. Because of most supervised neural network architectures requires retraining, in order to improve analyses capability due to changes in the input data, Adaptive Resonance Theory (ART) as a neural network with the adaptability of unsupervised training has been used in intrusion detection systems as well as efficient classification of the input data. In[10], the authors introduced an ART-based Intrusion Detector(UNNID) system, which employed ART network for clustering and classifying of network traffic in order to detect intrusive or attack traffic. UNNID has flexibility to change structure and parameters of ART neural networks for training and testing in different situations. KDD Cup's 99 dataset which covers four categories of attacks: Denial of Service (DoS) attacks, User-to-Root (U2R) attacks, Remote-to-Local (R2L) attacks, and Probing were trained and tested. The system uses a hybrid of misuse and anomaly detection approaches, so is capable of detecting known attack types as well as new attack types as anomalies [1].

5. **Principal component analysis:** Principal component analysis (PCA) networks combine unsupervised and supervised learning in the same topology. Principal component analysis is an unsupervised linear procedure that finds a set of uncorrelated features principal components, from the input. An MLP is supervised to perform the nonlinear classification from these components. It is well known that principal component analysis (PCA) is an essential technique in data compression and feature extraction, and it has been also applied to the field of ID [11][12]. In [13], a hierarchical ID model is presented based on the PCANN, which is suitable for adaptive online computing for both misuse detection and anomaly detection. Experimental results and comparative studies based on the 1998 DARPA evaluation datasets show the proposed model can classify the network connections with satisfying performance [1].

IV. PROPOSED IDS MODEL WITH BPN AND KEY MANAGEMENT TECHNIQUE

The working of the proposed security scheme is described in this section. Basically we are trying to prepare a data mining based intrusion detection system for wireless networks. In this approach the entire intrusion system design and modeling can be described in two major modules:

Training: training is process by which an implemented algorithm learns from the historical data. The learning of the algorithm can be an in supervised manner or in unsupervised manner. The supervised learning takes advantages over the unsupervised learning process. Thus for implementing the proposed methodology the supervised learning algorithm namely back propagation algorithm is used. That accepts the labeled data as input to the system and used for learning of the patterns hidden in training data.

Testing: During the testing the current network samples are utilized with the trained model of back propagation neural network. the input network samples are classified using the trained neural network classifier. For training and testing of the network the following organization of components are described as given in figure 1.

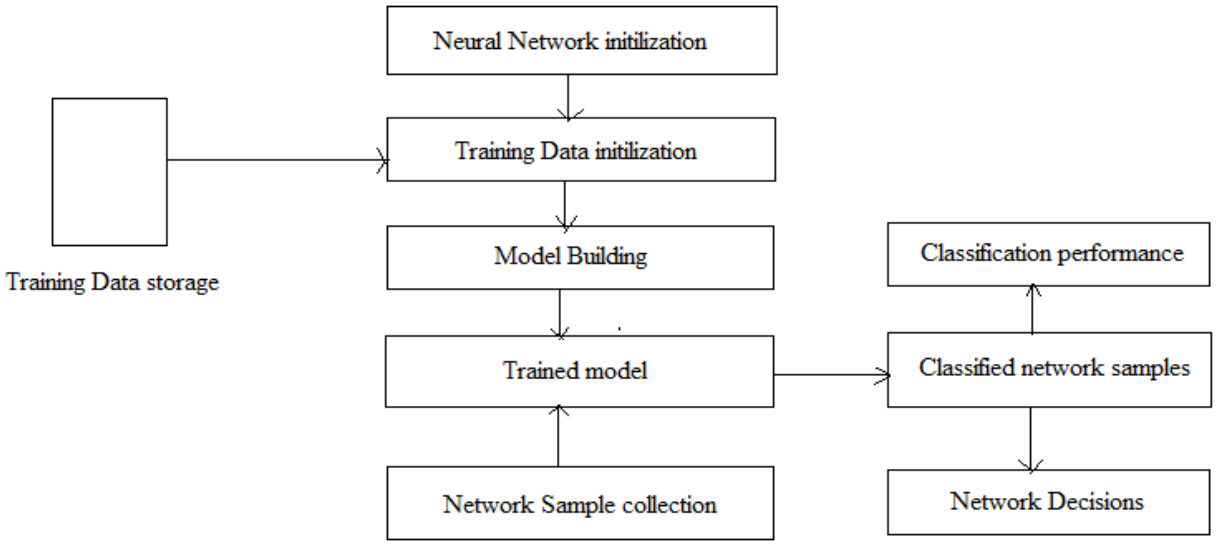

Figure 1 proposed system

The above given model is used for detection of intrusions in a network. Therefore a training data samples are collected first and labeled with the behavior of nodes. That data is stored in training ***data storage***. On the other hand the ***neural network is initialized*** with the different input attributes such as number of training cycles, number of input layer, number of hidden units and learning rate of model. Now the training data is initialized for training of data model. Using the input training samples the data is processed and the patterns are learned using the neural network algorithm. As the neural network is trained that is able to classify the patterns input to the neural network. Therefore for collecting the network samples the data collection unit is prepared which collect the data samples from entire network. That is produced as input samples to the neural network for classification. In classified patterns are identified and according to the classification outcomes the attacks are detected and the decision is made.

One additionally functionality is also developed for wireless network. After the classification that is distinguishable which nodes are legitimate and which one are malicious. The server node which performs the classification task is responsible for broadcast a cryptographic key for all the legitimate nodes. During the communication legitimate nodes are required to incorporate the security key with data chucks.

V. PERFORMANCE STUDY OF DIFFERENT CLASSIFIER

In order to adopt the efficient and accurate learner for intrusion detection system design, the comparison among three different classifiers namely KNN (K-nearest neighbour), BPN (back propagation neural network) and with a hybrid fuzzy and BPN algorithm is performed. The obtained performance parameters are explained as follows:

1. ACCURACY

The amount of correctly identified patterns among the input samples to classify is known as the classifier's accuracy. That can be computed using the following formula:

$$accuracy\ \% = \frac{total\ correctly\ classified\ data}{total\ amount\ of\ data\ to\ classify}$$

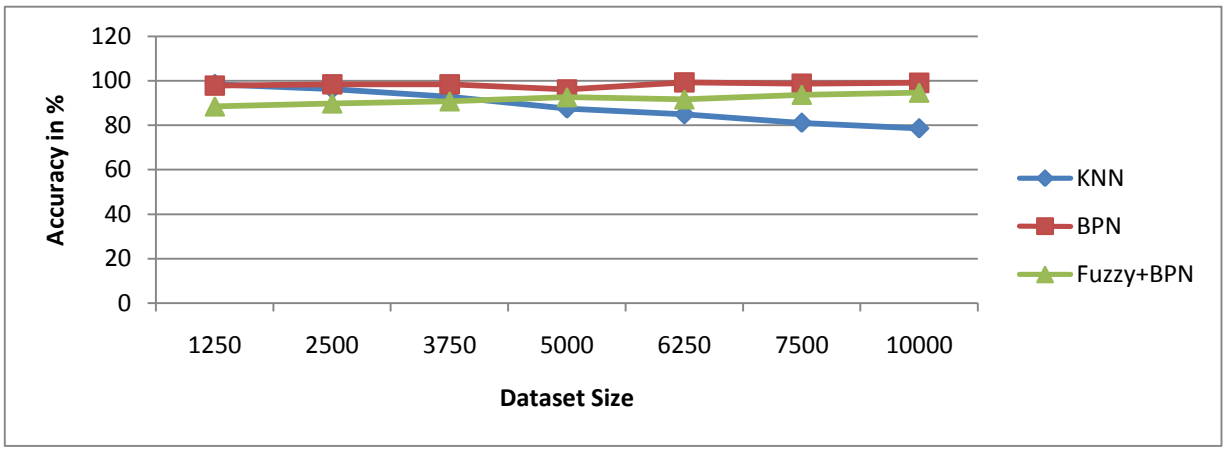

Figure 4.1 classification accuracy

The evaluated classification outcomes of the implemented classifiers for intrusion detection system development are simulated using figure 4.1. In this diagram the X axis includes the instances of data provided for classification and the Y axis represents the amount of data correctly recognized. According to the comparative outcomes the performance of BPN (back propagation neural network) is effectively higher as compared to other two classification schemes.

2 TIME COMPLEXITY

The amount of time required to analyze the given set of data is known as the time complexity or time consumption. The comparative performance in terms of time consumption is given using figure 4.2.

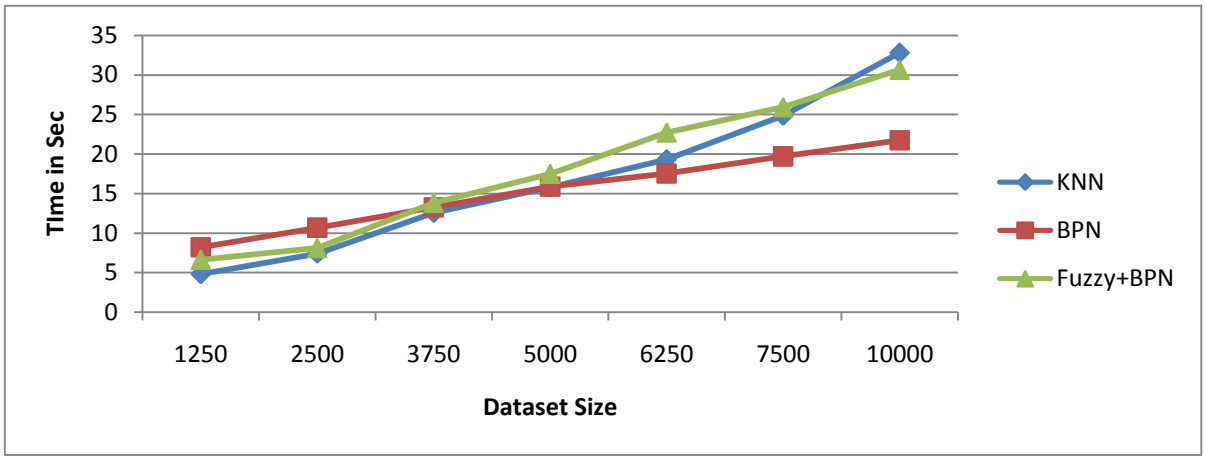

Figure 4.2 Time complexity

According to the obtained time complexity of the system that is found that the performance of the BPN in terms of time consumption during decision making is efficient as compared to the two different approaches available for data classification. In order to represent the performance of the classifier the X axis is denoted by the dataset instances and the Y axis shows the time consumed to classify the data.

3 SPACE COMPLEXITIES

The amount of main memory consumed for processing of the input dataset using the selected classification algorithm is termed here as space complexity. The comparative space complexity or memory consumption is given using figure 4.3.

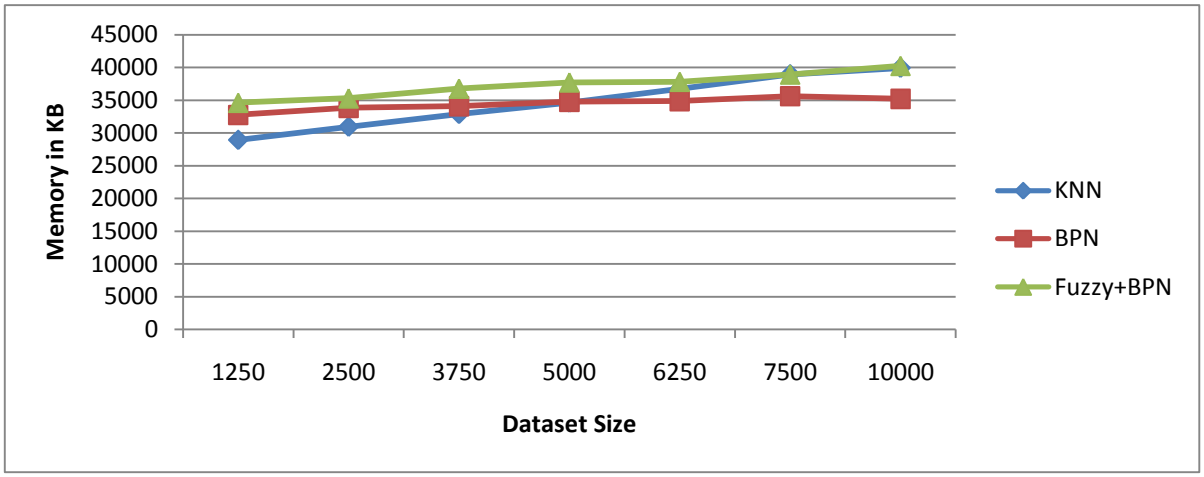

Figure 4.3 memory consumption

According to the given figure 4.3 the memory consumption of the BPN algorithm is much stable as compared to two other algorithms implemented. The space complexity of KNN algorithm is increases as the amount of data is increases additionally the fuzzy BPN is also increases. On the other hand the BPN memory consumption is not much fluctuating. Thus BPN is much adoptable as compared to the other two implemented algorithm.

VI. CONCLUSION

This paper provides the understanding and solution about the different attack analysis using a single system implementation. Therefore different kinds of intrusion detection systems are discussed in this

paper. In addition of the most frequently used algorithms for intrusion system design and network attack pattern classification methods are investigated based on the different previously suggested solutions. Among them three key techniques are distinguished namely back propagation neural network, k-nearest neighbour and the fuzzy neural network with BPN. To obtaining the most suitable network pattern classifier a performance study among these classification techniques are also provided in this paper. The performance analyses of these classifiers are performed under the accuracy, decision time and their space complexity. Among the selected three different classifiers the performance of the back propagation neural network found much optimum and stable for small and large set of data analysis. Thus this paper provides the efficient and accurate classification technique for wireless network's intrusion system design. In the recent years, the security attacks have become more and more widespread and difficult to detect in the network. So, the Intrusion Detection System is the main key area of research in the field of security.

ACKNOWLEDGEMENTS

It is a great privilege to acknowledge my gratitude and deep hearted thanks to my mentor and Supervisor Dr**. Sanjay Thakur,** Principal, Lord Krishna College and Technology, Indore, (M.P.), India. I am greatly thankful for his kind support and valuable guidance.

REFERENCES

[1] XiaoHang Yao, "A Network Intrusion Detection Approach Combined with Genetic Algorithm and Back Propagation Neural Network", 2010 International Conference on E-Health Networking, Digital Ecosystem and Technologies, PP. 402-405, 978-1-4244-5517-1/10/$26.00©*2010 IEEE.*

[2] Abhinav Jain, Sanjay Sharma and Mahendra Singh Sisodiya, "Network Intrusion Detection by using Supervised and Unsupervised Machine Learning Technique: A Survey", International Journal of Computer Technology and Electronics Engineering (IJCTEE), PP. 14-20, ISSN 2249-6343, Volume 1, Issue3.

[3] Manoranjan Pradhan, Sateesh Kumar Pradhan and Sudhir Kumar Sahu, "Anomaly Detection Using Artificial Neural Network", International Journal of Engineering Science and Engineering Technologies, April 2012, Volume 2, Issue 1, ISSN: 2231-6604, PP.-29-36©*IJESET.*

[4] Ryan J, Lin M, Miikkulainen R. Intrusion detection with neural networks. AI approaches to fraud Detection and risk management: papers from the 1997 AAAI workshop(Providence, Rhode Island), 1997. pp. 72-79.

[5] Z.M. Yang et al. "An intrusion detection system based on RBF neural network", cscwd, pp.873-875 Vol. 2, Proceedings of the Ninth International Conference on Computer Supported Cooperative Work in Design, 2005. Vo1.2, 2005.

[6] J. Zhong, Z.O. Li et al. Intrusion Detection Based on Adaptive RBF Neural Network. Proceedings of the Sixth International Conference on Intelligent Systems Design and Applications (ISDA'06) - Volume 02, 2006, pp. 1081- 1084.

[7] Z.J. Tang et al. Intrusion Detection. Tsinghua University Press, 2004, Chap.2, pp.6-8.

[8] Innella P, McMillan O. An introduction to intrusion detection systems. Tetrad Digital Integrity, LLC, last updated December 6, 200I, http://www.ecurityfocus.comlinfocus/ 1520.

[9] C. Stergiou, D. Siganos. Neural Networks. http://www.doc.ic.ac. ukI-ndisurprise 96/journal/vol41 cs 1 1/report.html.

[10] M. Heywood et al. "Dynamic intrusion detection using selforganizing maps". The annual Canadian information technology security symposium, May 2002.

[11] H.Ounes Kayacik et al., "A hierarchical SOM-based intrusion detection system Engineering Applications of Artificial Intelligence", 2007, PP. 439-451.

[12] Horeis T. Intrusion detection with neural networks-combination of self-organizing maps and radial basis function networks for human expert integration. Computational Intelligence Society, Research report. http://ieeecis.orgl_ fileslEAC Research 2003_ Report Horeis.pdf.

[13] M. Amini, R. Jalili. Network-Based Intrusion Detection Using Unsupervised Adaptive Resonance Theory (ART). http://nsc.sharif.edulresources/papers/amini-Network-BasedART.pdf.

[14] Anderson.J.P, "Computer Security Threat Monitoring & Surveilance", Technical Report, James P Anderson co., Fort Washington, Pennsylvania, 1980.

[15] Jake Ryan, Meng - Jang Lin, Risto Miikkulainen, "Intrusion Detection With Neural Networks", Advances in Neural Information Processing System 10, Cambridge, MA:MIT Press,1998,DOI:10.1.1.31.3570.

[16] Denning .D.E, "An Intrusion Detection Model", Transactions on Software Engineering, IEEE Communication Magazine, 1987,SE-13, PP-222-232,DOI:10.1109/TSE.1987.232894.

[17] Dewan Md, Farid, Mohammed Zahidur Rahman, "Anomaly Network Intrusion Detection Based on Improved Self Adaptive Bayesian Algorithm", Journal of Computers, Vol 5, pp-23-31, Jan 2010, DOI:10.4.304/jcp 5.1.

[18] Sathyabama.S, Irfan Ahmed.M.S, Saravanan.A,"Network Intrusion Detection Using Clustering: A Data Mining Approach", International Journal of Computer Application (0975-8887), Sep-2011, Vol: 30, No: 4, ISBN: 978-93-80864-87-5, DOI: 10.5120/3670-5071.

[19] Amir Azimi, Alasti, Ahrabi, Ahmad Habibizad Navin, Hadi Bahrbegi, "A New System for Clustering & Classification of Intrusion Detection System Alerts Using SOM", International Journal of Computer Science & Security, Vol: 4, Issue: 6, pp-589-597, 2011.

[20] Alan Bivens, Chandrika Palagiri, Rasheda Smith, Boleslaw Szymanski, "Network-Based Intrusion Detection Using Neural Networks", in Proceedings of the Intelligent Engineering Systems Through Artificial Neural Networks, St.Louis, ANNIE-2002, and Vol: 12, pp- 579-584, ASME Press, New York.

[21] Norouzian.M.R, Merati.S, "Classifying Attacks in a Network Intrusion Detection System Based on Artificial Neural Networks", in the Proceedings of 13th International Conference on Advanced Communication Technology(ICACT), 2011,ISBN:978-1-4244-8830-8,pp-868-873.

[22] Sadiq Ali Khan, "Rule-Based Network Intrusion Detection Using Genetic Algorithm", International Journal of Computer Applications, No: 8, Article: 6, 2011, DOI: 10.5120/2303-2914.

[23] Shilendra Kumar, Shrivastava ,Preeti Jain, "Effective Anomaly Based Intrusion Detection Using Rough Set Theory & Support Vector Machine(0975-8887), Vol:18,No:3, March 2011,DOI: 10.5120/2261-2906.

[24] Oswais.S, Snasel.V, Kromer.P, Abraham. A, "Survey: Using Genetic Algorithm Approach in Intrusion Detection Systems Techniques", in the Proceedings of 7th International Conference on Computer Information & Industrial Management Applications (CISIM), 2008, IEEE Communication Magazine,pp-300-307,ISBN:978-0-7695-318-7,DOI:10.1109/CISM.2008-49.

[25] Taeshik Shon, Jong Sub Moon, "A Hybrid Machine Learning Approach to Network Anomaly Detection", Information Sciences 2007, Vol: 177, Issue: 18, Publisher: USENIX Association, pp- 3799-3821, ISSN:00200255,DOI:10.1016/j.ins-2007.03.025.

[26] Aly Ei-Semary, Janica Edmonds, Jesus Gonzalez-Pino, Mauricio Papa, "Applying Data Mining of Fuzzy Association Rules to Network Intrusion Detection", in the Proceedings of Workshop on Information Assurance United States Military Academy 2006, IEEE Communication Magazine, West Point, NY,DOI:10.1109/IAW.2006/652083.

[27] Srinivas Mukkamala, Andrew H. Sung, Ajith Abraham, "Intrusion Detection Using an Ensemble of Intelligent Paradigms",Journal of Network & Computer Applications ,pp-1-15, 2004.

[28] Shilendra Kumar, Shrivastava ,Preeti Jain, "Effective Anomaly Based Intrusion Detection Using Rough Set Theory & Support Vector Machine(0975-8887), Vol:18,No:3, March 2011,DOI: 10.5120/2261-2906.

AUTHOR'S PROFILE

Sanjay Thakur has completed Doctor of Philosophy in Computer Science from Dr. Hari Singh Gour Central University, Sagar (M.P.) under the guidance of Prof. Diwakar Shukla. Presently Dr. Thakur is serving as a Principal in Lord Krishna College of Technology (LKCT), Indore, M.P. and having over 12 years experience of teaching to U.G. and P.G. classes. He has participated in a number of workshops/seminars/conferences at national and international level. He has published more than 40 research papers as author and co-author. He has guided some M.Tech. students for their dissertation and guiding some Ph.D. theses in Computer Science and Engineering. He is an editorial board member and reviewer of some Journals and Associations. His research interest areas are Stochastic Modelling, Computer Network and Wireless Network.

Pratik Gite has received B.E. (C.S.E.) from Malwa Institute of Technology, Indore in year 2009 and M.E. (C.S.E.) from Medi-Caps Institute of Technology, Indore in year 2011. He is a research scholar in Computer Science and Engineering Department of Pacific Academy of Higher Education and Research University, Udaipur (R.J.). He has published 10 papers in various international and national conferences. His areas of interests are Mobile Ad-hoc Network, Software Testing, Software Engineering and Computer Network.