Improving the Performance of Dynamic Source Routing Protocol by Optimization of Neural Networks

Rajesh Gargi, Yogesh Chaba, R.B.Patel

Abstract: *Dynamic Source Routing protocol is one of the most promising among on demand category of protocols for MANETs. Demands of network performance conflict with the demands of mobile networks . To enhance the QoS in a protocol like DSR we used ANN which helps to preserve the resources of the MANET leading to improvement in performance of DSR. While routing the data, If a legitimate node is mistaken as rogue node then also the QoS suffers and if a rogue node is not detected then also it can consume the resources of the network and deteriorate the QoS . In this work a neural network has been further optimized to improve its accuracy by varying the number of layers in it. A typical wireless network scenario of DSR has been simulated in NS2 and then a rogue node has been introduced to mimic attack. The parameters from the trace files have been used to train a neural network simulated in Matlab and its effectiveness has been improved to make the detection of intrusion more accurate. Although previous work has been reported in the area of application of neural networks for intrusion detection but there is a scope of improvement in this technique by varying the number of layers of ANN, making it more effective and improving the QoS of MANET.*

Key words : *Artificial Neural Networks, MANET, QoS.*

1. INTRODUCTION

MANET stands for mobile ad-hoc network. It configures it self and does not have any infrastructure and hence it is an attractive option for connecting devices quickly and spontaneous. MANET is an autonomous system of mobile nodes connected by wireless links in which each device is free to move independently in any direction, and will therefore change its links to other devices frequently. Each node operates not only as an end system, but also as a router to forward packets. The absence of any fixed infrastructure makes them easy to deploy, at the same time however, due to the absence of any fixed infrastructure, it becomes difficult to make use of the existing routing techniques for network services, and this poses a number of challenges in ensuring the security of the communication, something that is not easily done as many of the demands of network security conflict with the demands of mobile networks, mainly due to the nature of the mobile devices like low power consumption and low processing load.

Significant examples of MANETs include establishing survivable, efficient and dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. They may be used as hybrid infrastructure extensions and in fixed infrastructure operations. They allow low-cost, low complexity dynamic adjustments to provide coverage regions and range extensions away from the more fixed infrastructure backbone networks. Suggested areas of use will include establishing efficient communication networks for mobile workers in desolate regions or in disaster areas where existing networks have been destroyed or do not exist. To communicate in an efficient way proper routing protocols are needed. They have to contend with the effects of radio communication, such as noise, fading, and interference as the nodes communicate over wireless links. Bandwidth of MANET is lesser than that of a wired network. The use of efficient handover protocols and auto configuration of arriving nodes is needed.

The routing protocols are application specific, depending upon the size of the network and the frequency of the change in topology. The two types of protocols are based on the link-state (LS) routing algorithm and Based on the distance-vector (DV) routing-algorithm. Both of these algorithms try to find the shortest path from the source node to the destination node. The main difference is that in LS based routing a global network topology is maintained in every node of the network. In DV based routing the nodes only maintain information of and exchange information with their adjacency nodes. The general categories of MANET routing protocols are Proactive routing protocols and Reactive routing protocols. There is also a new class of routing protocols known as the hybrid routing protocols, which tries to encompass the advantages of both the proactive and reactive routing protocols.

For maintaining a reliable and secure ad-hoc network environment five major security goals that need to be addressed are Confidentiality (Protection of any information from being exposed to unintended entities), Availability (Services should be available whenever required), Authentication (Assurance that an entity of concern or the origin of a communication is what it claims to be or from), Integrity (Message being transmitted is never altered) and Non-repudiation (Ensures that sending and receiving parties can never deny ever sending or receiving the message).

Today’s routing algorithms are not able to thwart common security threats. Most of the existing ad hoc routing protocols do not accommodate any security and are highly vulnerable to attacks. Broadly there are two major categories of attacks when considering any network: external and internal. Internal attacks are more severe and their detection and correction is difficult. Passive Attack obtains the vital routing information but does not disrupt the operation of the protocol. Such attacks are usually difficult to detect and hence, defending against such attacks is complicated. An Active Attack injects arbitrary packets and tries to disrupt the operation of the protocol in order to limit availability, gain authentication, or attract packets destined to other nodes. The attacks based on modification disturb the operations of an ad-hoc network by announcing better routes (to reach other nodes or just a specific one) than the ones presently existing. Some other types of attacks are: Impersonation attack, Attack by Fabrication of Information etc. There is a difference between Malicious and selfish nodes. Both these nodes cause intentional non-cooperation. Selfish nodes want to save power while the malicious nodes are interested in attacking the network.

Prevention mechanisms, by themselves cannot ensure complete cooperation among nodes in the network. Detection on the other hand specifics solutions that attempt to identify clues of any malicious activity in the network and take punitive actions against such nodes. A node may misbehave by agreeing to forward packets and then failing to do so, because it is overloaded, selfish or malicious. The three types of prevention are Using symmetric cryptography, Using asymmetric cryptography and Using one-way hash chains. Detection on the other hand specifics solutions that attempt to identify clues of any malicious activity in the network and take punitive actions against such nodes.

Position aided routing protocols use geographical information to make forwarding decisions, resulting in a significant reduction in the number of routing messages. Secure Position Aided Ad hoc Routing (SPAAR) is a routing protocol designed to use protected position information to improve security, efficiency, and performance in MANET routing. SPAAR requires that each device can determine its own location. GPS receivers are relatively inexpensive and lightweight, so it is reasonable to assume that all devices in our network are equipped with one. Due to the resource limitations imposed in an ad hoc environment, reactive on demand routing approaches like AODV are preferred to the proactive routing protocols in order to conserve the resources of the nodes. Then security features were incorporated into those protocols (such as SAODV) which use asymmetric cryptography for authentication to address security issues.

Intrusion response is dependent upon the type of intrusion, the type of network protocols and the confidence in the veracity of the audit trace data. The response might range from resetting the communication channels between nodes or identifying the compromised nodes and precluding them from the network. Mobile ad-hoc networks have properties that increase their vulnerability to attacks. Unreliable wireless links are vulnerable to jamming and by their inherent broadcast nature facilitate eavesdropping. Constraints in bandwidth, computing power, and battery power in mobile devices can lead to application-specific trade-offs between security and resource consumption of the device. Mobility/Dynamics make it hard to detect behavior anomalies such as advertising bogus routes, because routes in this environment change frequently. Latency is inherently increased in wireless multi-hop networks, rendering message exchange for security more expensive. Multiple paths are likely to be available. This property offers an advantage over infrastructure-based local area networks that can be exploited by diversity coding.

A prevention-only strategy will only work if the prevention mechanisms are perfect; otherwise, someone will find out how to get around them. Most of the attacks and vulnerabilities have been the result of bypassing prevention mechanisms. In view of this reality, detection and response are essential. Even though prevention works as the first line of defense, it is not sufficient in addressing all the security threats. Hence we suggest an integrated layered framework which adopts the prevention techniques for the first level and detection techniques can be used at the second level complementing the protection techniques.

There are many open research challenges, because by definition mobile ad-hoc networks are self-organized and have no infrastructure and central authorities. Examples include self-organized key management, cooperation incentives, group-membership and access control, authentication and identity persistence, and trust management.

2. LITERATURE SURVEY

Moradi et al in their work on implementation of neural networks for intrusion detection in MANET have described that an intruder node injects a large amount of junk packets into the network and causes a denial in the services of the attacked node. Using a simulated MANET environment, ANNs modeling for detecting the DOS attack is investigated and it is showed that model can detect nodes under Dos attack effectively [1]. Hamad et al in their work on Neural Network's k-means Distance-Based Nodes-Clustering for Enhanced RDMAR Protocol in a MANET have described k-means as distance-based nodes clustering technique proposed enhance the performance of RDMAR protocol in a Mobile Ad-hoc NETwork (MANET) [2]. Saeed et al have worked on Modeling MANET Utilizing Artificial Intelligence to model MANET routing for three different routing protocols: dynamic source routing (DSR), ad hoc on-demand distance vector (AODV) and optimized link state routing (OLSR) and compare them with the traditional mathematical equation models. The results show that artificial intelligent (AI) models are more accurate and presenting to MANET than traditional mathematical equations [3].

Shah et al in their paper on the development and simulation of Artificial Neural Network Based Decision on Parametric Values for Performance Optimization of Reactive Routing Protocol for MANET Using Qualnet have described MANET as a collection of wireless nodes like mobile, laptops, palmtops etc. and a soft computing technique Artificial Neural Network based reactive AODV routing protocol is proposed to determine the frequency of hello interval to improve the performance of the network [4]. Mitrokotsa et al have worked on Intrusion Detection with Neural Networks and Watermarking Techniques for MANET using a novel combined watermarking embedded method. The performance of the proposed model is evaluated under different traffic conditions, mobility patterns and visualization metrics, showing its high efficiency [5]. Imana et al have developed Proactive reputation-based defense for MANETs using radial basis function neural networks. The RBF-NN predictors developed in this research to implement the proactive defense system resulted in an overall performance of 98.7% correct prediction with a 10-step predictor, and for comparison purposes, 98.1% with a 15-step predictor [6].

Guangjie et al have proposed a Novel Fault Diagnosis System for MANET Based on Hybrid GA-BP Algorithm and the performance of this system is excellent [7]. Min-Hua et al have worked on Cluster-based Cooperative Back Propagation Network Approach for Intrusion Detection in MANET. The effectiveness of the proposed scheme is illustrated by means of extensive simulations using NS-2 simulator. Specifically, the comparison between BPN and finite state machine (FSM) is given [8]. Masillamani et al in their paper entitled “Intelligent MANET" have implemented neuro-genetic intelligence for quick route rebuilding in MANET for improving the performance of the network [9]. Moursy et al have proposed Empirical model-based adaptive control of MANET describing the proposed self-controller, its design issues, and provide a preliminary case study to demonstrate the effectiveness and tradeoffs of two potential empirical-modeling techniques: regression and artificial neural networks [10].

Saeed et al have proposed Intelligent MANET Routing System which acquires the network's performance and then selects the optimum routing protocol that gives the best performance according to network context, such as: number and mobility of nodes. This module suggests the optimum network context for that situation [11] Saeed et al have developed IMAN: An Intelligent MANET routing system. Representative MANET scenarios, with different number of nodes and mobility schemes, were tested by means of simulations. Findings indicated considerable reduction in packets delay and data load when IMAN was utilized [12]. Danyang et al have worked on Reliable Routing Strategy for MANET based on SGC which can reduce the end-to-end delay and enhance the stability and raise the efficiency of communication by exerting the function of each node in MANET [13]. Hamrioui et al in their work on Improvement of the backoff algorithm for better MAC - TCP protocols interactions in MANET have studied the interactions between medium access control (MAC) and Transfer Control Protocol (TCP) protocols based on a dynamic adaptation of its maximal limit according to the number of nodes and their mobility and has shown the incidences of IB-MAC on MANET performance [14]. Chenn et al in their work on Zone Routing Protocol for Bluetooth MANET with Online Adaptive Zone Radius have proposed a routing protocol that utilizes the characteristics of Bluetooth technology is proposed for Bluetooth-based mobile ad hoc networks [15].

Kojima et al have proposed a Transition Reduction Method for FSM of MANET Routing Protocol with Blacklist by treating both input and output as sets. The proposed method redefines a given FSM to an FSM in which the number of states and the number transitions are drastically reduced [16]. Saxena et al in their Framework towards developing stability heuristic for cluster computation in MANETs have described that Hierarchical routing schemes in an ad-hoc environment outperform the flat routing schemes [17]. Saeed et al have proposed an Intelligent MANET Routing Protocol Selector which is adaptable to the variations in the network environment by predicting four important parameters that indicate the changes in the network context [18]. Ziane et al have evaluated Performance of an Adaptive State Dependent Mean Delay Routing Algorithm for MANET. To reduce the overhead generated by AMDR protocol, authors propose the use of a new MPR selection algorithm called flooding optimization algorithm (FOA) based on mean delay [19].

Urrea et al have worked on Estimating behavior of a GA-based topology control for self-spreading nodes in MANETs and shows that FGA converges toward significantly higher area coverage as it evolves [20]. Neelakandan et al have proposed Trust based optimal routing in MANET's and has proposed a secure, trusted, optimal scheme for routing in MANETs [21]. Kun et al have proposed a secure authentication scheme for integration of cellular networks and MANETs. Performance results by simulation reveal that this scheme is practical according to provided magnitude [22]. Wong et al have proposed a way of Managing interoperation in multi-organization MANETs by dynamic gateway assignment and has reported that cooperation is the key factor to produce optimal outcomes - a simple algorithm with tight cooperation among MANETs gives much better outcomes than a smart algorithm with loose cooperation [23]. Nacher et al have conducted a case study on Quantifying traffic anonymity in MANETs and deduced that it is relatively easy to identify what the sources are, especially those with the highest transmission rates. In contrast, authors show that inferences relative to recipients are minimal, meaning that recipient anonymity is easier to safeguard [24].

3. SIMULATION WORK DONE

Ns2 has been used as the simulation tool for evaluating the performance of DSR protocol. Scenarios have been created for MANETS under attack and under safe conditions by using TCL(tool command language). Matlab has been used to simulate ANN using the inputs from Ns2. Attempt has been made to Enhance the Accuracy of Detection of attack on MANET using Artificial Neural Networks. The Parameters from Ns2 act as inputs to the neural network. Given an input, which constitutes the measured values for the parameters of the MANET, the neural network is expected to identify if the accuracy has been achieved or not. This is achieved by presenting previously recorded parameters to a neural network and then tuning it to produce the desired target outputs. This process is called neural network training. The samples have been divided into training, validation and test sets. The training set is used to teach the network. Training continues as long as the network continues improving on the validation set. The test set provides a completely independent measure of network accuracy. The trained neural network has been tested with the testing samples. The network response has been compared against the desired target response to build the classification matrix which provides a comprehensive picture of a system performance.

The training data set includes a number of cases, each containing values for a range of input and output variables. Handling non-numeric data is more difficult. The most common form of non-numeric data consists of nominal-value variables such as Outcome : accurate / accurate Nominal-valued variables can be represented numerically. However, neural networks do not tend to perform well with nominal variables that have a large number of possible values. Other kinds of non-numeric data must either be converted to numeric form, or discarded. Dates and times, can be converted to an offset value from a starting date/time.

The number of cases required for neural network training frequently presents difficulties. There are some heuristic guidelines, which relate the number of cases needed to the size of the network (the simplest of these says that there should be ten times as many cases as connections in the network). Actually, the number needed is also related to the (unknown) complexity of the underlying function which the network is trying to model, and to the variance of the additive noise. As the number of variables increases, the number of cases required increases nonlinearly, so that with even a fairly small number of variables (perhaps fifty or less) a huge number of cases are required. This problem is known as the curse of dimensionality. For most practical problem domains, the number of cases required will be hundreds or thousands. For very complex problems more may be required, but it would be a rare (even trivial) problem which required less than a hundred cases. If the data is sparser than this, enough information to train a network is not there, and the best that can be done is probably to fit a linear model. If there is a larger, but still restricted, data set, one can compensate to some extent by forming an ensemble of networks, each trained using a different resampling of the available data, and then average across the predictions of the networks in the ensemble.

All neural networks take numeric input and produce numeric output. The transfer function of a unit is typically chosen so that it can accept input in any range, and produces output in a strictly limited range. For example of a sigmoid - S-shaped - function, the output is in the range (0,1), and the input is sensitive in a range not much larger than (-1,+1). The function is also smooth and easily differentiable, facts that are critical in allowing the network training algorithms to operate. Numeric values have to be scaled into a range that is appropriate for the network.

Multilayer Perceptrons is the type of network in which the units each perform a biased weighted sum of their inputs and pass this activation level through a transfer function to produce their output, and the units are arranged in a layered feedforward topology. The network thus has a simple interpretation as a form of input-output model, with the weights and thresholds (biases) the free parameters of the model. Such networks can model functions of almost arbitrary complexity, with the number of layers, and the number of units in each layer, determining the function complexity. Important issues in Multilayer Perceptrons (MLP) design include specification of the number of hidden layers and the number of units in these layers.

Unary encoding has been used in this simulation to perform symbol translation. The first six columns of data will represent the MANET characteristics. The last column represents whether the detection of attack is accurate or not. This data will be randomly generated. The next step will be to preprocess the data into a form that can be used with a neural network. The next step is to create a neural network that will learn to identify if the accuracy has been achieved or not.

4. SIMULATION & RESULTS

The results are in the form of graphs of performance vs number of epochs by changing the number of layers.

The first graph plots the percentage accuracy achieved when one layer was used to construct the artificial neural network

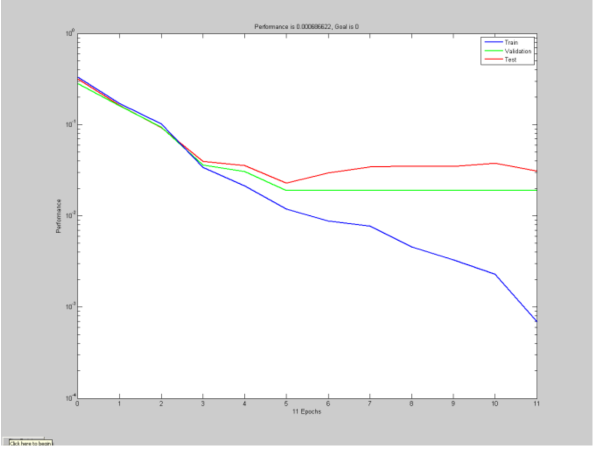


Fig 1 accuracy vs epochs using 1 layer ANN

It can be seen from the graph that ANN characteristics were TRAINLM-calcjx, Epoch 0/100, MSE 2.29141/0, Gradient 5.01065/1e-010

TRAINLM-calcjx, Epoch 17/100, MSE 0.001359/0, Gradient 0.00514123/1e-010

TRAINLM, Validation stop.

Total testing samples: 113

cm =70 6
2 35

cm_p = 61.9469 5.3097
1.7699 30.9735

Percentage Correct Intrusion Detection : 92.920354%

Percentage Incorrect Intrusion Detection : 7.079646%

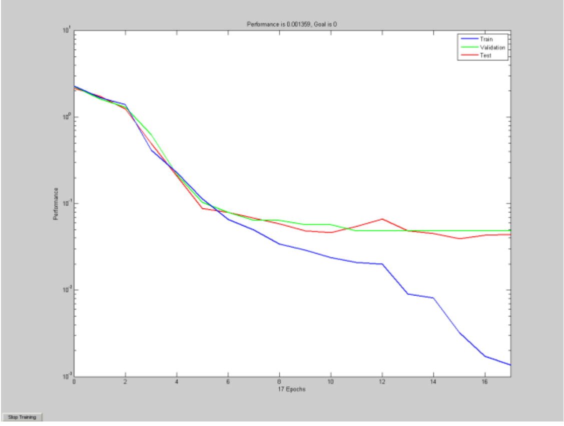


Fig 2 accuracy vs epochs using 2 layer ANN

It can be seen from the graph that ANN characteristics were TRAINLM-calcjx, Epoch 0/100, MSE 1.84577/0, Gradient 4.5495/1e-010

TRAINLM-calcjx, Epoch 13/100, MSE 0.00320523/0, Gradient 0.0078773/1e-010

TRAINLM, Validation stop.

Total testing samples: 113

cm = 74 0
2 37

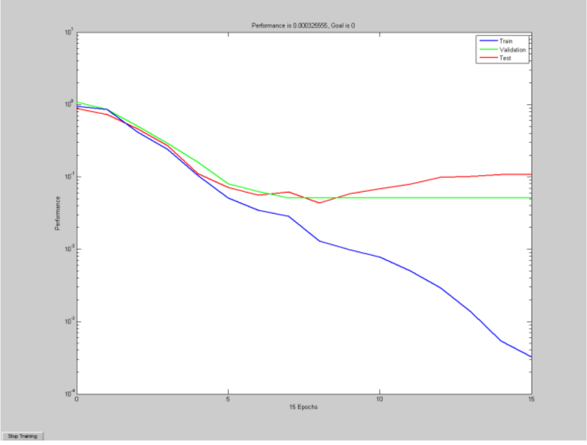
cm_p = 65.4867 0
1.7699 32.7434

Percentage Correct Intrusion Detection : 98.230088%

Percentage Incorrect Intrusion Detection : 1.769912%

Following graph plots the percentage accuracy achieved when 3 layers were used to construct the artificial neural network

Fig 3 accuracy vs epochs using 3 layer ANN



It can be seen from the graph that ANN characteristics were TRAINLM-calcjx, Epoch 0/100, MSE 0.331589/0, Gradient 1.24963/1e-010

TRAINLM-calcjx, Epoch 11/100, MSE 0.000686622/0, Gradient 0.0433198/1e-010

Total testing samples: 113

cm =
66 2
0 45

cm_p =
58.4071 1.7699
0 39.8230

Percentage Correct Intrusion Detection : 98.230088%

Percentage Incorrect Intrusion Detection : 1.769912%

Following graph plots the percentage accuracy achieved when 4 layers were used to construct the artificial neural network

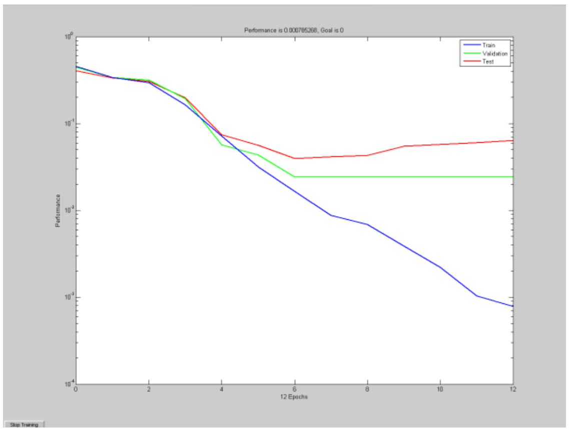


Fig 4 accuracy vs epochs using 4 layer ANN

It can be seen from the graph that ANN characteristics were TRAINLM-calcjx, Epoch 0/100, MSE 0.454978/0, Gradient 2.07929/1e-010

TRAINLM-calcjx, Epoch 12/100, MSE 0.000785268/0, Gradient 0.00297586/1e-010

```
   Total testing samples: 113
   cm =
      67     4
       1    41
   cm_p =
     59.2920    3.5398
      0.8850   36.2832
```

Percentage Correct Intrusion Detection : 95.575221%

Percentage Incorrect Intrusion Detection : 4.424779%

Following graph plots the percentage accuracy achieved when 5 layers were used to construct the artificial neural network

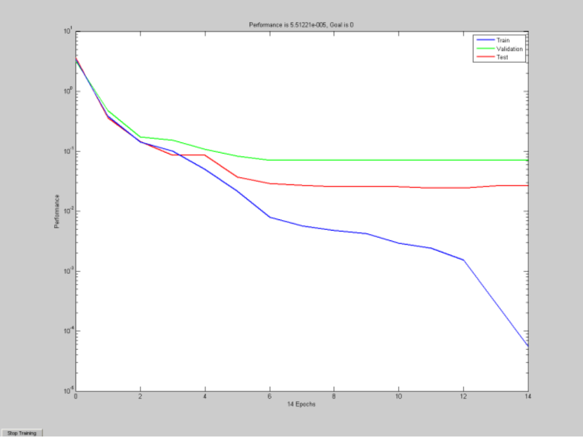


Fig 5 accuracy vs epochs using 5 layer ANN

It can be seen from the graph that ANN characteristics were

TRAINLM-calcjx, Epoch 0/100, MSE 0.953917/0, Gradient 2.67875/1e-010

TRAINLM-calcjx, Epoch 15/100, MSE 0.000325555/0, Gradient 0.000963222/1e-010

TRAINLM, Validation stop.

```
   Total testing samples: 113
   cm =
       71     1
        4    37
   cm_p =
     62.8319    0.8850
      3.5398   32.7434
```

Percentage Correct Intrusion Detection : 95.575221%

Percentage Incorrect Intrusion Detection : 4.424779%

Following graph plots the percentage accuracy achieved when 6 layers were used to construct the artificial neural network

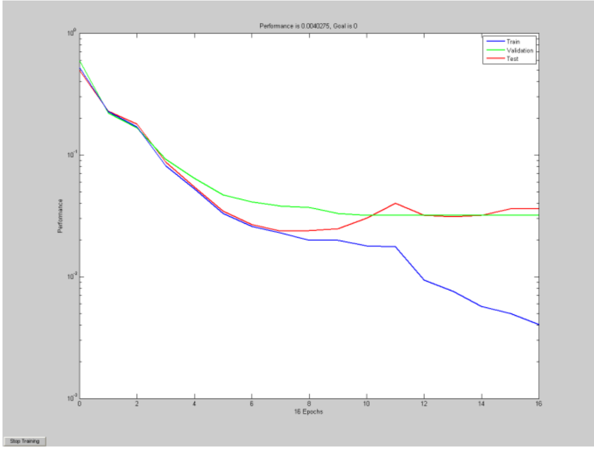


Fig 6 accuracy vs epochs using 6 layer ANN

It can be seen from the graph that ANN characteristics were TRAINLM-calcjx, Epoch 0/100, MSE 0.522056/0, Gradient 1.83581/1e-010

TRAINLM-calcjx, Epoch 16/100, MSE 0.0040275/0, Gradient 0.0865535/1e-010

TRAINLM, Validation stop.

```
   Total testing samples: 113

   cm = 75     2
         1    35
   cm_p = 66.3717    1.7699
           0.8850   30.9735
```

Percentage Correct Detection : 97.345133%

Percentage Incorrect : 2.654867%

Following graph plots the percentage accuracy achieved when 7 layers were used to construct the artificial neural network

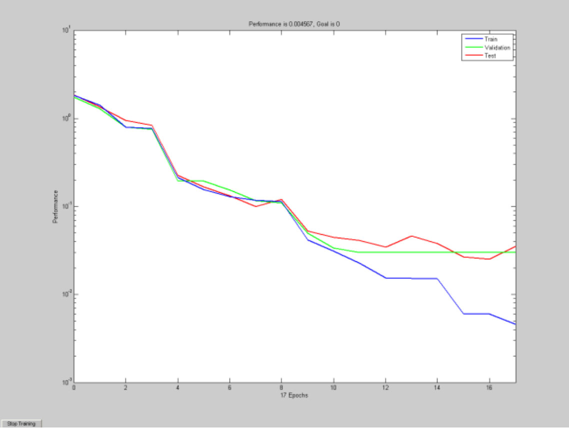


Fig 7 accuracy vs epochs using 7 layer ANN

It can be seen from the graph that ANN characteristics were TRAINLM-calcjx, Epoch 0/100, MSE 1.83033/0, Gradient 6.50093/1e-010

TRAINLM-calcjx, Epoch 17/100, MSE 0.004567/0, Gradient 0.00942413/1e-010

TRAINLM, Validation stop.

Total testing samples: 113

```
cm = 66    3
      3   41
cm_p   58.4071    2.6549
        2.6549   36.2832
```

Percentage Correct Intrusion Detection : 94.690265%

Percentage Incorrect Intrusion Detection : 5.309735%

Following graph plots the percentage accuracy achieved when 8 layers were used to construct the artificial neural network

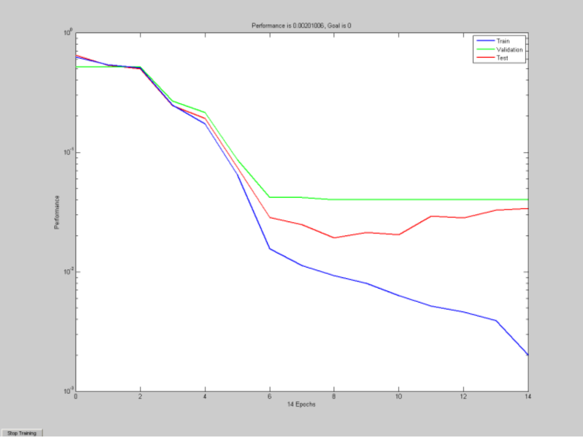


Fig 8 accuracy vs epochs using 8 layer ANN

It can be seen from the graph that ANN characteristics were TRAINLM-calcjx, Epoch 0/100, MSE 0.62786/0, Gradient 1.64507/1e-010

TRAINLM-calcjx, Epoch 14/100, MSE 0.00201006/0, Gradient 0.086174/1e-010

TRAINLM, Validation stop.

Total testing samples: 113

```
cm =
   68    1
    0   44
cm_p =
  60.1770    0.8850
        0   38.9381
```

Percentage Correct Intrusion Detection : 99.115044%

Percentage Incorrect Intrusion Detection : 0.884956%

Following graph plots the percentage accuracy achieved when 9 layers were used to construct the artificial neural network

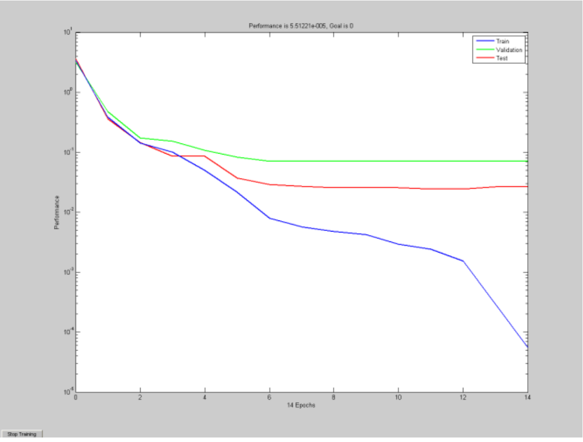


Fig 9 accuracy vs epochs using 9 layer ANN

It can be seen from the graph that ANN characteristics were TRAINLM-calcjx, Epoch 0/100, MSE 0.877436/0, Gradient 3.07186/1e-010

TRAINLM-calcjx, Epoch 14/100, MSE 4.93003e-005/0, Gradient 0.000833949/1e-010

TRAINLM, Validation stop.

Total testing samples: 113

```
cm =
   69    7
    4   33
cm_p =
  61.0619    6.1947
   3.5398   29.2035
```

Percentage Correct Intrusion Detection : 90.265487%

Percentage Incorrect : 9.734513%

Following graph plots the percentage accuracy achieved by varying the number of layers used to construct the artificial neural network. It can be seen that best result was obtained when 9 layers were used to construct the neural network.

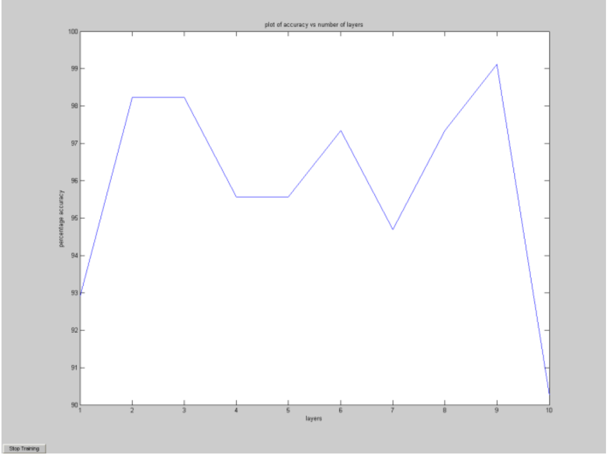


Fig 10 accuracy vs number of layers

The plot below shows the throughput with rogue node present

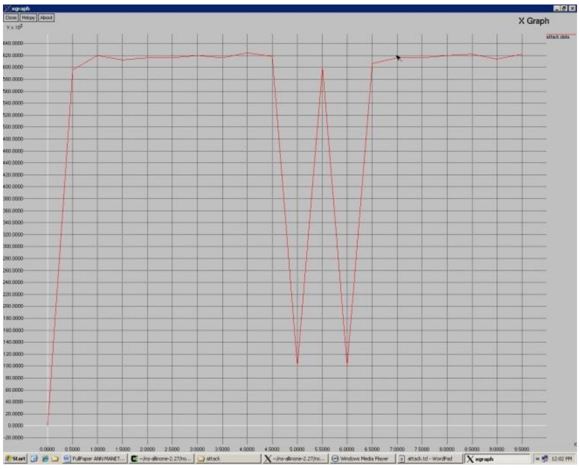


Fig 11 throughput in the presence of rogue node

The plot below shows the throughput with rogue node detected with accuracy

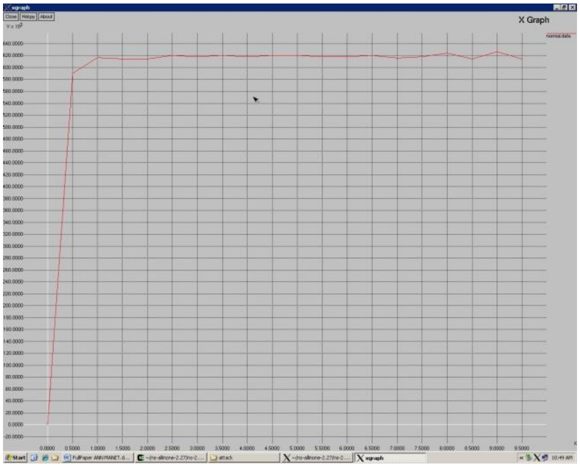


Fig 12 throughput after accurate detection of rogue node

CONCLUSION

In a protocol like Dynamic Source Routing the Technique used in this paper can significantly improve the throughput and it can further be concluded from this work that ANN with 9 layers is ideally suitable for predicting intrusion and it can achieve 98 % accuracy. As the simulation results show to increase the number of layers further may not improve the throughput .

Since the simulation results demonstrate increased precision by using this technique, thus from this work it can be concluded that intrusion can be predicted reasonably with the help of artificial neural network. Reasonable accuracy has been achieved by using ANN with optimized no of layers. When the output of ANN is applied to a typical simulation of DSR protocol it improved the throughput.

REFERENCES

[1]. Moradi, Z.; Teshnehlab, M.; Rahmani, A.M.; , "Implementation of neural networks for intrusion detection in manet," Emerging Trends in Electrical and Computer Technology (ICETECT), 2011 International Conference on , vol., no., pp.1102-1106, 23-24 March 2011

[2]. Hamad, O.F.; Mi-Young Kang; Jin-Han Jeon; Ji-Seung Nam; , "Neural Network's k-means Distance-Based Nodes-Clustering for Enhanced RDMAR Protocol in a MANET," Signal Processing and Information Technology, 2008. ISSPIT 2008. IEEE International Symposium on , vol., no., pp.192-197, 16-19 Dec. 2008

[3]. Saeed, N.H.; Abbod, M.F.; Al-Raweshidy, H.S.; , "Modeling MANET Utilizing Artificial Intelligent," Computer Modeling and Simulation, 2008. EMS '08. Second UKSIM European Symposium on , vol., no., pp.117-122, 8-10 Sept. 2008

[4]. Shah, S.K.; Vishwakarma, D.D.; , "Development and Simulation of Artificial Neural Network Based Decision on Parametric Values for Performance Optimization of Reactive Routing Protocol for MANET Using Qualnet," Computational Intelligence and Communication Networks (CICN), 2010 International Conference on , vol., no., pp.167-171, 26-28 Nov. 2010

[5]. Mitrokotsa, Aikaterini; Komninos, Nikos; Douligeris, Christos; , "Intrusion Detection with Neural Networks and Watermarking Techniques for MANET," Pervasive Services, IEEE International Conference on , vol., no., pp.118-127, 15-20 July 2007

[6]. Imana, E.Y.; Ham, F.M.; Allen, W.; Ford, R.; , "Proactive reputation-based defense for MANETs using radial basis function neural networks," Neural Networks (IJCNN), The 2010 International Joint Conference on , vol., no., pp.1-6, 18-23 July 2010

[7]. Guangjie Huang; Wei Guo; Jian Su; , "A Novel Fault Diagnosis System for MANET Based on Hybrid GA-BP Algorithm," Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on , vol., no., pp.1-4, 12-14 Oct. 2008

[8]. Min-Hua Shao; Ji-Bin Lin; Yi-Ping Lee; , "Cluster-based Cooperative Back Propagation Network Approach for Intrusion Detection in MANET," Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on , vol., no., pp.1627-1632, June 29 2010-July 1 2010

[9]. Masillamani, M.R.; Jamalipour, A.; Uma, G.V.; , "Intelligent MANET," Intelligent and Advanced Systems, 2007. ICIAS 2007. International Conference on , vol., no., pp.408-413, 25-28 Nov. 2007

[10]. Moursy, A.; Ajbar, I.; Perkins, D.; Bayoumi, M.; , "Empirical model-based adaptive control of MANETs," INFOCOM Workshops 2008, IEEE , vol., no., pp.1-6, 13-18 April 2008

[11]. Saeed, N.H.; Abbod, M.F.; Al-Raweshidy, H.S.; , "Intelligent MANET Routing System," Advanced Information Networking and Applications - Workshops, 2008. AINAW 2008. 22nd International Conference on , vol., no., pp.1260-1265, 25-28 March 2008

[12]. Saeed, N.H.; Abbod, M.F.; Al-Raweshidy, H.S.; , "IMAN: An Intelligent MANET routing system," Telecommunications (ICT), 2010 IEEE 17th International Conference on , vol., no., pp.401-404, 4-7 April 2010

[13]. Danyang Qin; Xuejun Sha; Yubin Xu; , "A Reliable Routing Strategy for MANET Based on SGC," Computational Sciences and Optimization, 2009. CSO 2009. International Joint Conference on , vol.1, no., pp.536-540, 24-26 April 2009

[14]. Hamrioui, S.; Lalam, M.; , "IB-MAC: Improvement of the backoff algorithm for better MAC - TCP protocols interactions in MANET," Programming and Systems (ISPS), 2011 10th International Symposium on , vol., no., pp.9-16, 25-27 April 2011

[15]. Chenn-Jung Huang; Liang-Chun Chen; Yao-Chuan Lin; Yi-Ta Chuang; Wei Kuang Lai; Sheng-Yu Hsiao; , "A Zone Routing Protocol for Bluetooth MANET with Online Adaptive Zone Radius," Information, Communications and Signal Processing, 2005 Fifth International Conference, pp.579-583.

[16]. Kojima, H.; Ohta, T.; Kakuda, Y.; , "A Transition Reduction Method for FSM of MANET Routing Protocol with Blacklist," Autonomous Decentralized Systems (ISADS), 2011 10th International Symposium on , vol., no., pp.611-616, 23-27 March 2011

[17]. Saxena, G.; Singhal, A.; , "Framework towards developing a stability heuristic for cluster computation in MANETs," Intelligent Computing and Intelligent Systems (ICIS), 2010 IEEE International Conference on , vol.2, no., pp.502-506, 29-31 Oct. 2010

[18]. Saeed, N. H.; Abbod, M. F.; Sulaiman, T. H.; Al-Raweshidy, H. S.; Kurdi, H.; , "Intelligent MANET Routing Protocol Selector," Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST '08. The Second International Conference on , vol., no., pp.389-394, 16-19 Sept. 2008

[19]. Ziane, S.; Mellouk, A.; , "Performance Evaluation of an Adaptive State Dependent Mean Delay Routing Algorithm for MANET," Wireless Communications and Mobile Computing Conference, 2008. IWCMC '08. International , vol., no., pp.348-353, 6-8 Aug. 2008

[20]. Urrea, E.; Şahin, C.S.; Uyar, M.U.; Conner, M.; Bertoli, G.; Pizzo, C.; , "Estimating behavior of a GA-based topology control for self-spreading nodes in MANETs," MILITARY COMMUNICATIONS CONFERENCE, 2010 - MILCOM 2010 , vol., no., pp.1405-1410, Oct. 31 2010-Nov. 3 2010

[21]. Neelakandan, S.; Anand, J.G.; , "Trust based optimal routing in MANET's," Emerging Trends in Electrical and Computer Technology (ICETECT), 2011 International Conference on , vol., no., pp.1150-1156, 23-24 March 2011

[22]. Kun Wang; Meng Wu; Pengrui Xia; Shendong Xie; Weifeng Lu; Subin Shen; , "A secure authentication scheme for integration of cellular networks and MANETs," Neural Networks and Signal Processing, 2008 International Conference on , vol., no., pp.315-319, 7-11 June 2008

[23]. Wong, S.H.Y.; Chi-Kin Chau; Kang-Won Lee; , "Managing interoperation in multi-organization MANETs by dynamic gateway assignment," Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on , vol., no., pp.129-136, 23-27 May 2011

[24]. Nacher, Marga; Calafate, Carlos T.; Cano Escriba, Juan Carlos; Manzoni, Pietro; , "Quantifying traffic anonymity in MANETs: A case study," Ubiquitous and Future Networks (ICUFN), 2010 Second International Conference on , vol., no., pp.171-176, 16-18 June 2010

Dr Yogesh Chaba received the B.E. degree in Computer Sc. & Engg with DISTINCTION from Marathwada University, Aurangabad in year 1993. He obtained his MS degree in Software Systems from BITS Pilani and PhD degree from Guru Jambheshwar University of Science & Technology, HISAR. He is working as Associate Professor in Deptt of Computer Sc. & Engg, Guru Jambheshwar University of Science & Technology, HISAR. He worked as Chairman, Deptt of Computer Sc. & Engg, Guru Jambheshwar University of Science & Technology, HISAR for three years. His Research areas are Computer Networks and mobile communication. He has published more then 75 papers in national and international journals and conferences of repute including IEEE, Springer and Science Direct Journals. He is Principal Investigator of two major research projects funded by All India Council for Technical Education and University Grants Commission, INDIA in the area of Network Security and Ubiquitous. He is also Deputy Coordinator of SAP project funded by University Grant Commission. He has vast international exposure as he has visited different universities and research institutions in USA, UK and China for academic assignments. He is also recipient of "Young Scientist Award" by International Academy of Physical Sciences for year 2002

Dr. R. B. Patel ,Dean ,Faculty of Information Technology & Computer Science ,Deenbandhu Chhotu Ram University of Science & Technology, Murthal. He received PhD from IIT Roorkee in Computer Science & Engineering, PDF from Highest Institute of Education, Science & Technology (HIEST), Athens, Greece, MS (Software Systems) from BITS, Pilani and B. E. in Computer Engineering from M. M. M. Engineering College, Gorakhpur, UP.He has two patents , numerous best paper awards and more than 100 publications to his credit. He is member of bodies like IEEE, ISTE.

Rajesh Gargi received the B.Tech. degree from Regional Engineering College , Kurukshetra. He obtained his M.Tech degree in Computer Sc. & Engg from Guru Jambheshwar University of Science & Technology, Hisar and perusing PhD from the same University. He is working as Associate Professor in Computer Sc. & Engg, Department at Indus Institute of Engineering and Technology Kinana,Jind. His Research areas are Computer Networks and Mobile Communication. He has published more than 10 papers in national, international journals and conferences of repute.