ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

# Improving the Performance of Adaptive Secured Backup Ad-hoc Routing protocol by Artificial Neural Networks in Wireless Ad-hoc Networks

[1]Vignesh.M, [2]Deepak Kumar.T,[3]Sakthivel.K,[4]Mahalingam.R, [5]Satheesh Kumar.S

[1-4]UG Students, [5]Assistant Professor

Department of CSE

Nandha Engineering College, Erode-52.

**Abstract**—The Proposed work is concerned with secured backup routing protocol, which is used to store secured backup routes from multiple routes available between the source and destination in Ad-hoc networks. Ad-hoc network users while on movement can use the network services efficiently and securely by using the proposed protocol. The Efficiency of the Secured Backup Routing Protocol can be improved by using Artificial Neural Networks. We simulate our protocol using NS2 and obtain the result that shows the packet drop ratio is very low and packets sent are high than the existing routing protocols.

**Keywords-Ad-hoc network,Back up Routing,Artificial Neural Networks.**

## I. INTRODUCTION

Routing is the act of moving information across the network from a source to a destination. It is also referred as the process of choosing a path over which the packets are sent.

Mobile Ad-hoc network sare self-organizing and self-configuring multi-hop wireless networks, where the structure of the network changes dynamically. This is mainly due to the mobility of the nodes. No design the networks utilize the same random access wireless channel, cooperating in intimate manner to engaging themselves in multi-hop forwarding. The node in the network not only acts as hosts but also as routers that route data to/ from other nodes in network. In infrastructure networks, within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes.

There are many existing routing protocols available for MANET and those can be categorized as table driven approach (proactive) and on demand routing protocols (reactive). Proactive routing protocols are based on continuous information refreshing in routing tables. Information on any change in the network is sent at constant time periods. The main goal is to maintain up-to-date information in routing tables thus enabling the route selection in a most excellent manner.Some of the representative protocols based on table driven logic are OLSR and Destination sequenced distance vector (DSDV)

Reactive routing protocols calculate optimal route on demand. When a route is calculated, it is stored and used until the destination is available or the path's time is out. The mostly used reactive protocols are DSR and AODV. In order to create a better solution, a hybrid solution gives the possibility to combine some of the advantages of proactive and reactive routing protocols. The routing protocol proposed here is a hybrid routing ones. As a reactive routing protocol, the proposed algorithm should find the optimal path on demand, based on up-to-date information.

## II. PROPOSED PROTOCOL

To improve the routes stability and to improve the trust on participating nodes, this paper present a secure backup routing protocol for mobile ad hoc network. The proposed protocol discovers multiple routes from source to destination in order to store a backup route to the destination node to be used in case of intruder attack and link or node failure which avoids the reroute discovery phase.

The nodes are been authenticated well in order to know that the participating nodes are not intruders to break the link and to find the optimal paths from the available multiple paths we use ANN algorithm in our protocol. Initially by using the concepts of AODV multipath routing protocol we find multiple paths available from source to destination. The architecture of our protocol is shown below in the Figure.2.1.

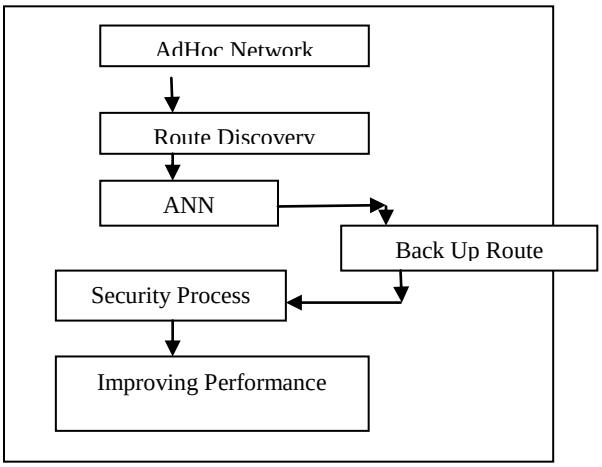


Figure 2.1Architecture of Secured Backup Routing Protocol based on Artificial Neural Networks.

*A.RouteDiscovery in Ad-hoc Networks*

There are three options related to route discovery for a Ad-hoc network

- SUPPRESS route discovery: The message is routed along the tree.
- ENABLE route discovery: The message is routed along an already discovered mesh route, if one exists; otherwise the Router initiates a route discovery.
- FORCE route discovery: If the Router has the route capacity, it will initiate a route discovery, even if a known route already exists.

The mechanism for route discovery between two End Devices involves the following steps:

1. A route discovery broadcast is sent by the parent Router of the source End Device. This broadcast contains the network address of the destination End Device.
2. All Routers eventually receive the broadcast, one of which is the parent of the destination End Device.
3. The parent Router of the destination node sends back a reply addressed to the parent Router of the source.
4. As the reply travels back through the network, the hop count and a signal quality measure for each hop are recorded. Each Router in the path can build a routing table entry containing the best path to the destination End Device.
5. Eventually, each Router in the path will have a routing table entry and the route from source to destination End Device is established. Note that the corresponding route from destination to source is not known – the route discovered is unidirectional.

*B. Back up Routing Scheme in Ad-hoc Networks*

In this section we discover a backup path from source to destination in case of primary path link failure or intruder attack . By using ANN algorithm we obtain the optimal path from source to destination, and in the same phase we find an alternate secure path to be used in link failure due to attacks.

The alternate path will be next best path when compared to the optimal path. By this method when a primary path fails we can recover the connection by utilizing the backup paths. This backup path routing contains three main functions: connectivity management, Backup path discovery phase and Backup path maintenance phase.

*C. Backup Path discovery phase*

The backup paths intersect with primary paths to establish a braided path structure. The primary path and backup path are established during the route discovery phase itself when we find optimal path by using ANN. The backup paths are physically closer to the primary paths.

*D. Backup Path maintenance*

The data packets are delivered via the primary path till the primary path is disconnected. When a node detects a link failure, it utilizes the backup path in place of primary path. This is done with the help of RERR message where when a node faces the link or node failure it will send a RERR message to the source node that that initiates the routing process. So the source node chooses the backup path from where the link has broken instead of finding a new route by reroute discovery process.

## III. ARTIFICIAL NEURAL NETWORKS

An Artificial Neural Network (ANN) is an information processing paradigm that is inspired by the way biological nervous systems, such as the brain, process information. An artificial neuron is a device with many inputs and one output. The neuron has two modes of operation; the training mode and the using mode. In the training mode, the neuron can be trained to fire (or not), for particular input patterns. In the using mode, when a taught input pattern is detected at the input, its associated output becomes the current output. If the input pattern does not belong in the taught list of input patterns, the firing rule is used to determine whether to fire or not.

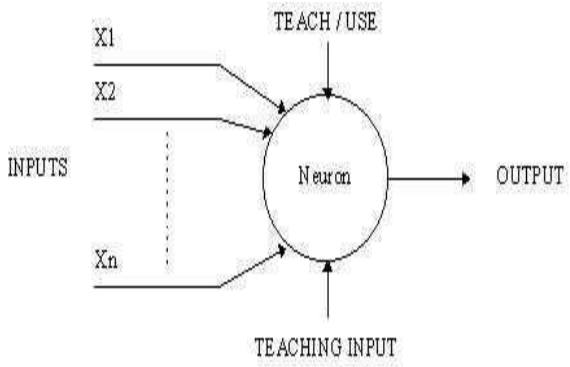


Figure 3.1 A simple neuron

Artificial Neural Networks consist of a number of **units** which are mini calculation devices. They take in **real-valued** input from multiple other nodes and they produce a single real valued output. By *real-valued* input and output we mean real numbers which are able to take any decimal value.

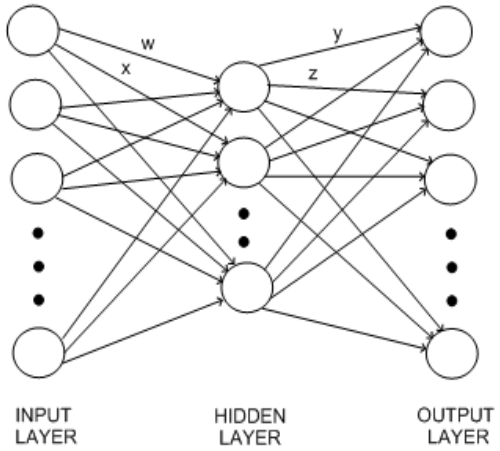


Figure 3.2 Layers of Artificial Neural Networks

Note that the w, x, y and z represent real valued weights and that all the edges in this graph have weights associated with them (but it was difficult to draw them all on). Note also that more complicated ANNs are certainly possible. In particular, many ANNs have multiple hidden layers, with the output from one hidden layer forming the input to another hidden layer. Also, ANNs with no hidden layer - where the input units are connected directly to the output units - are possible

***A. ANN implementation***

Scenarios have been created for Ad-hoc networks under attack and under safe conditions by using TCL (tool command language). Mat-lab 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 Ad-hoc networks, 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. 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 Perceptions 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 feed forward 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 Perceptions (MLP) design include specification of the number of hidden layers and the number of units in these layers.

## IV. SIMULATION WORK

In this section we evaluate and compare the performance of ordinary on demand routing algorithm for MANET with secure Backup routing protocol for MANET using ANN by using NS-2.

The simulation scenario consists of 100 nodes randomly distributed in 400m x400m square area. Maximum speed of nodes is varied in five different maximum moving speeds: 0/5/10/15/20 m per second.

We consider only the continuous mobility case. The transmission range of every node is 100m. There are 20 constant bit rate CBR traffic resource distributed over the network. The CBR data packets are 512 bytes, and the sending rate is 4packets per second. Simulations run for 300 seconds.

We use the following metrics to compare the performance of the three routing protocols:
1. Packet delivery ratio,
2. Throughput,
3. End-to-end delay,

### *A. Packet Delivery Ratio*

The packet delivery ratio is defined as the ratio between the packets that are received and the number of packets sent. This is one of the most used metrics for protocol comparison. In our simulations the proposed NN model exhibits the best performance, then the OSPF, as depicted in Figure 4.1

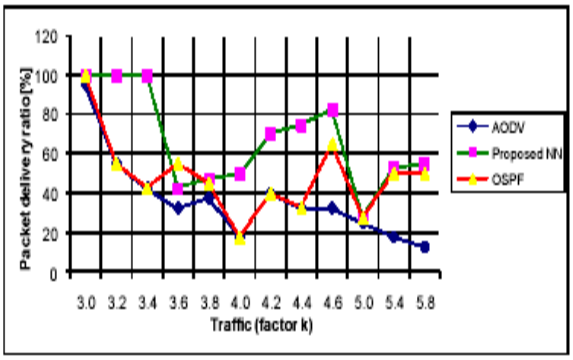


Figure 4.1Packet Delivery Ration performance

### *B. Throughput*

The throughput between two nodes is expressed as the number of bytes delivered per unit of time.
Formally:
*Throughput = Total bytes received/Total time*
The throughput (measured by bytes per seconds) we have calculated as a function of the traffic load (expressed as the number of equal-sized packets per second), for different routing protocols, and results are depicted in

Figure 4.2 The proposed NN algorithm gives significantly better results than AODV and OSPF. This is based on fact that the proposed algorithm is tailored for finding the optimal routes and thus increasing the number of packets which reach the destination.

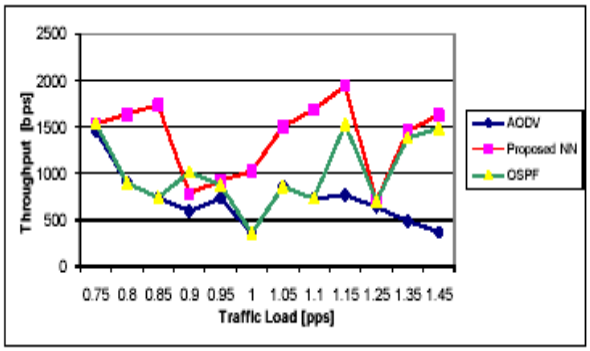


Figure 4.2 Throughput performance.

*C. End-to-End Delay*

The end-to-end packet delay is calculated as the time interval between the time instant when the packet is generated and is ready for the transmission, and the moment when it reached the destination node. Simulation results, depicted in Figure 4.3 show that the OSPF is better than the proposed NN method (for about 20%) while AODV is significantly worse, but note that we have the full benefits of neural networks can be achieved only through the hardware implementation, when the parallel work of all neurons is possible. Instead of that, we are using simulation, meaning our model was working in sequential mode which is unnatural for neural networks.

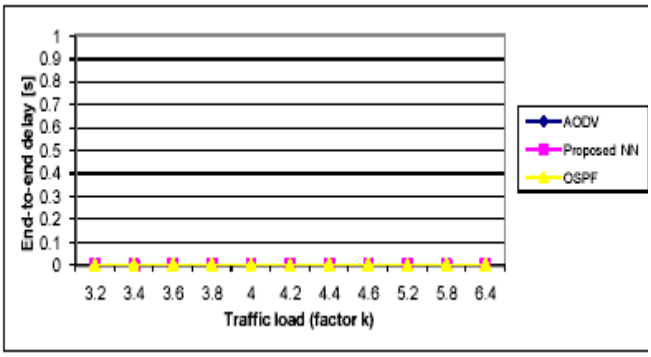


Figure 4.3 End-to-end Delay performances

## V. CONCLUSION

The Proposed protocol for Improving the Efficiency of Secured Backup Routing Protocol for Ad-hoc Networks using Artificial Neural Networks discovers a secured Backup route for communicating packet from source to destination through a Management key included in the route request packet. It addresses how to reconnect quickly when the transmission route fails and to retransmit the packets to the destination. We used several metrics for describing the performances of the routing algorithms. It is shown that the proposed routing protocol has better or the same performance in all metrics, even though the neural network is simulated by a digital computer.

## REFERENCES

1. G. Lavanya, C.Kumar and A. Rex Macedo Arokiaraj," Secured Back up Routing Protocol for Ad-hoc Network" International Journal of Computer Theory and Engineering, Vol. 2, No. 4, August, 2010,pp1793-8201.

2. Gihan Nagib and Wahied G. Ali,Network Routing Protocol usingGenetic Algorithms,International Journal of Electrical & Computer Sciences IJECS-IJENS Vol:10 No:02

3. Heni KAANICHE and Farouk KAMOUN,Mobility Prediction in Wireless Ad Hoc,Networks using Neural Networks,JOURNAL OF TELECOMMUNICATIONS, VOLUME 2, ISSUE 1, APRIL 2010

4. Joo-Han Song, Wong,V.W.S and Leung V.C.M, "Efficient on-demand routing for mobile ad-hoc wireless access networks", IEEE Journal on selected areas in Communications, August 2004, pp.1374-1383.

5. Chao-Chin Chou,David S.L .Wei, C-C.Jay Kuo and Kshirasagar Naik, "An efficient anonymous communication protocol for peer-to-peer applications over mobile ad-hoc networks" IEEE Journal on selected areas in communications, January 2007, pp.192- 203.

6. Khalil Shihab "A Backpropagation Neural Network for Computer Network Security", Journal of Computer Science, 2006,pp.710-715.

7. Papadimitratos, P and Haas, Z.J "Secure data communication in mobile ad-hoc networks", IEEE Journal on selected areas in communications, February 2006, pp.343 - 356.

8. Bo Zhu, Zhiguo Wan, Kankanhalli, M.S., Feng Bao and Deng, R.H. "Anonymous secure routing in mobile ad-hoc networks", 29th IEEE international conference on Local Computer Networks, December 2004, pp 102- 108.

.